الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير

قسم : علوم التسيير

أطروحة مقدمة لنيل شهادة دكتوراه العلوم

فرع علوم التسيير ، تخصص الادارة الاستراتيجية و الذكاء الاقتصادي

بعنوان :

مستوى أمن المعلومات في المؤسسة الجزائرية و مدى تأثره بطبيعة التهديدات و طبيعة الحماية المطبقة

من إعداد المترشحة : فيلالي أسماء

نوقشت و أجيزت علنا بتاريخ : 2019/06/20

أمام اللجنة المكونة من السادة:

أ.د تشوار خير الدين	أستاذ التعليم العالي	جامعة تلمسان	رئيسا
أ.د بوشيخي عائشة	أستاذ التعليم العالي	جامعة تلمسان	مشرفا
أ.د بن منصور عبد الله	أستاذ التعليم العال	جامعة تلمسان	ممتحنا
أ.د أونان بومدين	أستاذ التعليم العالي	جامعة سيدي بلعباس	ممتحنا
أ.د بوزيان عثمان	أستاذ التعليم العالي	جامعة سعيدة	ممتحنا
د. بلحسن محمد	أستاذ محاضر "أ"	المركز الجامعي بمغنية	ممتحنا

السنة الجامعية :2019/2018

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي و البحث العلمي
Université Abou Bekr Belkaid Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

كلية العلوم الاقتصادية و العلوم التجارية و علوم التسيير

قسم علوم التسيير

أطروحة مقدمة لنيل شهادة دكتوراه علوم

فرع علوم التسيير ، تخصص الادارة الاستراتيجية و الذكاء الاقتصادي

بعنوان :

مستوى أمن المعلومات في المؤسسة الجزائرية و مدى تأثره بطبيعة التهديدات و طبيعة الحماية المطبقة

من إعداد المترشحة : فيلالي أسماء

نوقشت و أجيزت علنا بتاريخ : 2019/06/20

أمام اللجنة المكونة من السادة:

أ.د تشوار خير الدين	أستاذ التعليم العالي	جامعة تلمسان	رئيسا
أ.د بوشيخي عائشة	أستاذ التعليم العالي	جامعة تلمسان	مشرفا
أ.د بن منصور عبد الله	أستاذ التعليم العال	جامعة تلمسان	ممتحنا
أ.د أونان بومدين	أستاذ التعليم العالي	جامعة سيدي بلعباس	ممتحنا
أ.د بوزيان عثمان	أستاذ التعليم العالي	جامعة سعيدة	ممتحنا
د. بلحسن محمد	أستاذ محاضر "أ"	المركز الجامعي بمغنية	ممتحنا

السنة الجامعية :2019/2018


بسم الله الرحمن الرحيم


وقل رب زدني علما

الاهداء

إلى الوالدين الكريمين حفظهما الله و أدام صحتهما

إلى أختي " ابتسام " و أخواي "أمين " و " أيمن"

إلى ولداي " فراس " و " محمد ياسين"

إلى كل أفراد الأسرة كبيرا وصغيرا

إلى كل زملاء الدراسة

إلى كل من لم يدخر جهدا في مساعدتي

إلى كل طلبة العلم

أهدي هذا العمل المتواضع

شكر و تقدير

بسم الله الرحمن الرحيم و الصلاة و السلام على أشرف المرسلين سيدنا محمد عليه أفضل الصلاة و التسليم

الحمد لله الذ ي لا ينسى من ذكر اسمه ، الحمد لله الذي لا ينسى من شكره على نعمه و فضله ، الحمد لله الذي بنعمته تتم الصالحات ، الحمد لله الذي وفقنا على مواصلة الدرب ، و أعاننا على اتمام هذا العمل ، و ألهمنا الصبر و الارادة ، فلك الحمد و لك الشكر

أتقدم بخالص الشكر و التقدير للأستاذة الدكتورة : " **بوشيخي عائشة** " جامعة تلمسان لتفضلها بالاشراف على هذه الأطروحة ، و لما قدمته لي من عون صادق و ارشاد أمين و توجيه سديد، إذ لم تبخل علي بالنصائح و التوجيهات العلمية و المنهجية رغم انشغالاتها.

كما أتقدم بخالص الشكر و الامتنان و التقدير للأستاذ الدكتور "**شليل عبد اللطيف**" جامعة تلمسان على تشجيعه المستمر و دعمه الذي لا يقدر بثمن و مجهوداته في دعم هذا العمل طالبة من الله عز وجل أن يجعل كل ذلك في ميزان حسناته.

أتقدم بالشكر الجزيل على كل من ساعدني على اتمام هذا العمل و أخص بالذكر الأستاذ " **صوار يوسف** " جامعة سعيدة ، و مسؤول أمن المعلومات بالمؤسسة الوطنية للأشغال البترولية الكيرى بالرغاية اللذان لم يتوانا في تقديم المساعدة.

كما لا يفوتني في هذا المقام أن أتوجه بالشكر الجزيل لأعضاء لجنة المناقشة الموقرة لتفضلهم بقبول مناقشة هذه الأطروحة و على ملاحظاتهم القيمة التي سيكون لها الفضل في اثراء هذا العمل

قائمة المحتويات

فهرس الجداول

فهرس الأشكال

قائمة الرموز

الرمز	شرحه بالفرنسية أو الانجليزية	شرحه بالعربية
AASSI	L'**A**ssociation **A**lgérienne de la **S**écurité des **S**ystèmes d'**I**nformation	الجمعية الجزائرية لأمن نظم المعلومات
AFNOR	l'**A**ssociation **F**rançaise de **Nor**malisation	الجمعية الفرنسية للقياس
ANSI	The **A**merican **N**ational **S**tandards **I**nstitute	المعهد الوطني الأمريكي للقياس
ARIST	**A**gence **R**égionale pour l'**I**nformation **S**tratégique et **T**echnologique	الوكالة الاقليمية للمعلومة الاستراتيجية و التكنولوجية
ASSI	**A**gent de la **s**écurité des **S**ystèmes d'**I**nformation	عون أمن نظم المعلومات
BSI	**B**ritish **S**tandards **I**nstitution	المنظمة البريطانية للقياس
CEI	**C**ommission **E**lectrotechnique **I**nternationale	اللجنة الكهرتقنية الدولية
CEN	**C**omité **E**uropéen de **N**ormalisation	اللجنة الأروبية للقياس
CERT	**C**omputer **E**mergency **R**eponse **T**eams	فرق استجابة الكمبيوتر في حالات الطوارئ
CISM	**C**ertified **I**nformation **S**ecurity **M**anager	شهادة مدير معتمد لأمن المعلومات
CISSP	**C**ertified **I**nformation **S**ystem **S**ecurity **P**rofessional	شهادة محترف أمن نظم المعلومات
CLUSIF	**CLU**b de la **S**écurité de l'**I**nformation **F**rançais	نادي أمن المعلومات الفرنسي
CPI	**C**our **P**énale **I**nternationale	المحكمة الجنائية الدولية
DCSSI	**D**irection **C**entrale de la **S**écurité des **S**ystèmes d'**I**nformation	المديرية المركزية لأمن نظم المعلومات
DMZ	**DeMi**litarized **Z**one	منطقة منزوعة السلاح
FBI	**F**ederal **B**ureau of **I**nvestigation	مكتب التحقيق الفدرالي
IDS	**I**ntrusion **D**etection **S**ystems	أنظمة كشف التدخل
IP	**I**nternet **P**rotocol	عنوان الجهاز
ISACA	**I**nformation **S**ystems Audit and **C**ontrol **A**ssociation	جمعية مراقبة و تدقيق نظم المعلومات
ISO	**I**nternational **O**rganisation of **S**tandardization	المنظمة العالمية للقياس
NIST	**N**ational **I**nstitue of **S**tandards and **T**echnology	المعهد الوطني للمعايير والتكنولوجيا

OIT	**O**rganisation **I**nternational de **T**ravail	المنظمة العالمية للعمل
OMPI	**O**rganisation **M**ondiale de la **P**ropriété **I**ntellectuelle	المنظمة العالمية للملكية الفكرية
OSSI	**O**fficier de la **S**écurité des **S**ystèmes d'**I**nformation	ضابط أمن نظم المعلومات
PDCA	**P**lan,**D**o,**C**heck,**A**ct	دورة ديمنغ للتحسين المستمر
ROSI	**R**eturn On **S**ecurity **I**nvestment	العائد على الاستثمار في الأمن
RPO	**R**ecovery **P**oint **O**bjective	نقطة إعادة البناء
RSSI	**R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation	مسؤول أمن نظم المعلومات
RTO	**R**ecovery **T**ime **O**bjective	الوقت الأقصى المقبول لعدم الاتاحة
SEI	**S**oftware **E**ngineering **I**nstitue	معهد هندسة البرمجيات
TCP	**T**ransmission **C**ontrol **P**rotocol	بروتوكول التنقل
TI	**T**echnologie de l'Information	تكنولوجيا المعلومات
TIC	**T**echnologie de l'**I**nformation et de la **C**ommunication	تكنولوجيا المعلومات و الاتصال
VPN	**V**irtuel **P**rivate **N**etwork	الشبكة الافتراضية الخاصة
WIPO	**W**orld **I**ntellectual **P**roperty **O**rganisation	المنظمة العالمية للملكية الفكرية

المقدمة العامة

تمهيد

الاشكالية

الفرضيات

مبررات اختيار الموضوع

أهمية الدراسة

أهداف الدراسة

منهج البحث

الدراسات السابقة

حدود الدراسة

صعوبات الدراسة

تمهيد

لقد شهد هذا العصر انفجار معلوماتي هائل جعل المؤسسات مهما كان حجمها معرضة لمنافسة معقدة و متزايدة ، فالتغيرات العالمية و الثورة التكنولوجية الحديثة ، و الدخول في عصر العولمة و الانترنت جعل المؤسسة في مواجهة حادة مع المخاطر الناجمة عن التغير المستمر لبيئتها ،وتهديدات جديدة في ساحة الأعمال ، و لهذا فإنها دائما بحاجة إلى المعلومة المفيدة من أجل استغلالها في الوقت المناسب ، بل هي بحاجة أكثر إلى حماية هذه المعلومات خاصة الإستراتيجية منها و الحساسة ، وهذا ما يستدعي تكثيف الجهود وتسخير كل الوسائل المتاحة و الممكنة من أجل تعزيز أمن المؤسسة.

و أمن معلومات المؤسسة هو تحقيق حماية لكل الممتلكات المادية منها كالأجهزة و البنايات ، و غير المادية كصورة المؤسسة و أنظمتها المعلوماتية و بالأخص المعلومات الإستراتيجية و الحساسة ، و التي تعتبر ثروة حقيقية في ظل اقتصاد المعرفة ، فالتهديدات قد تطال إما توفر المعلومة أو سلامتها أو سريتها و أمنها ، و الحفاظ على سرية المعلومات ليس بالأمر الهين بل هو أمر أصبح يتعب الإدارة العليا للمؤسسات خاصة مع وجود شبكات الانترنت التي أحدثت تغييرات جذرية في كيفية نقل المعلومة ، هذه الشبكات أصبحت معرضة للاختراق و الوصول إلى بيانات المؤسسة بطرق غير شرعية ، هذا بالإضافة إلى أمن و سرية المعلومة داخل المؤسسة و صلاحية الوصول إلى نوع معين من البيانات من قبل مستويات معينة.

و عليه فان المؤسسة التي تسعى لتحقيق مستوى معين من الحماية عليها انتهاج منهج واضح في هذا المجال ، و رسم سياسة و استراتيجية خاصة بكيفية تطبيق هذا الأمن على مستواها ، فاليوم لم يعد كافيا شراء أحدث برامج الحماية من أجل حماية الأنظمة و المعلومات ، بل أصبح محتما على المؤسسات أن تنظر لهذا المفهوم كمنهج عمل يومي و دائم ، يحمل في طياته عدة أوجه ، فمن جهة عليها تأمين المؤسسة تأمينا ماديا يمنع أي دخول مادي غير مرخص للمؤسسة خصوصا المناطق الحساسة فيها كالقاعات التي تضم الأجهزة المعلوماتية ، و من جهة أخرى عليها مواكبة العصر في كل ما يتعلق بالحماية الفنية و البرمجية للأجهزة المعلوماتية من برامج حماية و منع الدخول و كلمات مرور...، و لكن أهم و أكبر مجهود يمكن أن تقوم به أي مؤسسة في مجال أمن المعلومات هو تطوير العامل البشري في هذا المجال ، فكل أنواع الحماية المذكورة سابقا لا تجدي نفعا دون رأس مال بشري واع و محسس بشكل كافي ، فالحلقة الأقوى في تطبيق الأمن هو الفرد الذي أثبتت كل الدراسات أنه سبب أغلب الهجمات و التهديدات التي تتعرض لها المؤسسات و الأنظمة ، و لهذا فعلى كل مؤسسة أن تغير نظرتها حول أمن المعلومات

من المنظور الضيق المحصور في الماديات إلى المنظور الواسع و الشامل ، و تبادر بإنشاء سياسات أمن معلومات ترسم الطريق لكيفية التطبيق الصحيحة له.

و بما أن المؤسسة الجزائرية اليوم تنشط في ظل اقتصاد مفتوح ، لا يمكنها أن تبقى في منأى عن كل التطورات الحاصلة في بيئة الأعمال ، و لكي تضمن بقاءها و استمراريتها عليها الأخذ بعين الاعتبار كل المفاهيم الجديدة الموجودة في الساحة و كل التغيرات الحاصلة في البيئة ، و التحصين ضد أي خطر أو تهديد لإرثها المعلوماتي الذي يعتبر اليوم الثروة الحقيقية لأي مؤسسة أو دولة ، و بالتالي عليها إتقان طرق الحماية من أي تدخل غير مشروع ، و تحقيق أمن المعلومات الذي يضمن لها الاستمرارية.

و على ضوء ما تقدم يمكننا طرح **الاشكالية** التالية :

❖ ما هو مستوى أمن المعلومات في المؤسسة الجزائرية ؟و ما مدى تأثره بالتهديدات الواقعة و طبيعة الحماية المطبقة؟

و على ضوء هذه الإشكالية يمكن طرح التساؤلات التالية:

- ما المقصود بأمن المعلومات؟
- ما هي التهديدات التي تفرضها البيئة المحيطة ؟
- ما هي طرق و سبل الحماية التي تعتمدها المؤسسة لتحقيق أمن المعلومات؟
- ما هو مستوى أمن المعلومات في المؤسسة الجزائرية ؟ و ما هي الطرق المتبعة في تحقيقه؟
- ما مدى تأثر مستوى أمن المعلومات في المؤسسة الجزائرية بطبيعة التهديدات الواقعة؟
- ما مدى تأثر مستوى أمن المعلومات في المؤسسة الجزائرية بطبيعة الحماية المطبقة؟

❖ فرضيات الدراسة:

للإجابة على هذه الإشكالية و التساؤلات قمنا بوضع الفرضيات التالية:

الفرضية الرئيسية الأولى : تؤثر طبيعة التهديدات على مستوى أمن المعلومات في المؤسسة الجزائرية :
و على ضوء هذه الفرضية تتفرع ثلاث فرضيات فرعية :

الفرضية الفرعية الأولى : تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية.

الفرضية الفرعية الثانية : تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية .

الفرضية الفرعية الثالثة : تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية.

الفرضية الرئيسية الثانية :تؤثر طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسة الجزائرية :

و يتفرع عن هذه الفرضية أربع فرضيات فرعية :

الفرضية الفرعية الأولى : تؤثر طبيعة الحماية المادية المطبقة على مستوى أمن المعلومات في المؤسسة الجزائرية.

الفرضية الفرعية الثانية : تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسة الجزائرية.

الفرضية الفرعية الثالثة : تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسة الجزائرية.

الفرضية الفرعية الرابعة : تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسة الجزائرية.

❖ مبررات اختيار الموضوع:

إن الأسباب التي دفعتنا إلى اختيار هذا الموضوع ما يلي:

- أول سبب في اختيار هذا الموضوع هو محاولة للتعمق أكثر في موضوع الماجستير " الذكاء الاقتصادي " ، حيث أن الذكاء يرتكز على ركيزتين أساسيتين : اليقظة الاستراتيجية و الأمن ، و نظرا لكثرة الدراسات المعالجة لموضوع اليقظة ، حاولنا دراسة الركيزة الثانية " الأمن "و التي هي في الحقيقة أهم من سابقتها.
- الأهمية الكبيرة للموضوع ، و التي اكتسبها من خلال الانفجار الكبير الذي يشهده عالم المعلومات ، و انتقال الاقتصاد العالمي من اقتصاد الكم إلى اقتصاد النوع.
- نظرا للانفتاح المعلوماتي ، الذي بقدر ما هو نعمة هو نقمة بسبب الخطر الكبير الذي يسببه على خصوصية المؤسسة و إمكانية المساس بمعلوماتها السرية ، أصبح أمن المعلومات ضرورة.
- محدودية الاهتمام بتطبيقات أمن المعلومات في المؤسسات الجزائرية.
- ضرورة ضمان حد أدنى من أمن المعلومات على مستوى كل مؤسسة.

- قلة الدراسات التي عالجت الموضوع على مستوى العينة المدروسة خاصة باللغة العربية ، إذ لم نجد أي بحث علمي تناول الموضوع على مستوى المؤسسات الجزائرية.
- بحكم التخصص الأكاديمي.

❖ **أهمية الدراسة:**

تكمن أهمية الموضوع في تفصيل كيفية تحقيق الأمن داخل المؤسسة و الطرق التي يمكن الاعتماد عليها في ذلك و أيضا تبيين الأسس و المعايير التي من خلالها يمكن للمؤسسة اختيار المعيار المناسب لها، و إعطاء نظرة عن موقع المؤسسة الجزائرية في هذا المجال، و طبيعة التهديدات التي تتعرض لها نظم معلوماتها، و الطرق المتبعة في مواجهتها، و مدى تأثر مستوى الأمن بذلك، فالمؤسسات الجزائرية متأخرة نوعا ما في مجال التعامل مع المعلومات باعتبارها مازالت في بداية الانفتاح و التطور، و لكن إن لم تركب الموج العالمي الاقتصادي بسرعة و تواكب كل تطور و كل جديد فإنها ستنهار لا محال، إذ أنه أصبح ضروريا على كل مؤسسة ضمان على الأقل حد أدنى من الأمن.

❖ **أهداف الدراسة:**

- إعطاء فكرة أوضح و أعمق عن موضوع أمن المعلومات و آلياته و طرق تطبيقه.
- الكشف عن النقائص التي تعاني منها المؤسسات الجزائرية في مجال أمن المعلومات.
- معرفة مستوى أمن المعلومات على مستوى المؤسسات الجزائرية ، و مدى تأثره بطبيعة التهديدات التي يتعرض لها ، و مدى تأثره أيضا بمستوى الحماية المطبقة من طرف المؤسسة.
- إعطاء آراء جديدة أو توضيح آراء موجودة يما يخص أمن المعلومات و أهميته في الحفاظ على استمرارية المؤسسة.
- تحديد موقع المؤسسة الجزائرية من التطورات الحاصلة في مجال أمن المعلومات.

❖ **منهج البحث :**

اعتمد هذا البحث على منهجية تتوافق مع طبيعته و المتمثلة في :

- **الجانب النظري** : تم اعتماد أسلوب المسح المكتبي حيث تم الاطلاع على العديد من المراجع المتعلقة بأمن المعلومات باللغة العربية و الفرنسية و بعض المراجع باللغة الانجليزية و تمثلت في الكتب و المقالات و الدراسات النظرية و الميدانية إضافة إلى البحوث العلمية المتمثلة في أطروحات الدكتوراه و رسائل الماجستير ، مع الاطلاع على بعض المواقع على الانترنت .

- **الجانب التطبيقي** : تم الاعتماد في هذا الجانب على الدراسة الميدانية من خلال تصميم استمارة وجهت لعينة من المؤسسات الجزائرية ، و استخدام المنهج الوصفي التحليلي لتحليل النتائج المتحصل عليها باعتباره الأسلوب العلمي المناسب للدراسات الميدانية إضافة إلى المقابلات الشخصية.

❖ الدراسات السابقة :

باعتبار أن البحث العلمي هو عملية تراكمية مستمرة ، فان الانطلاقة الصحيحة لأي بحث تكون على أساس البدء مما انتهي إليه الآخرون ، و يتحقق ذلك بالإطلاع على مختلف الدراسات السابقة التي تطرقت للموضوع ، إذ يساعدنا ذلك في معرفة النتائج التي توصلت إليها كل دراسة ، و في هذا البحث حاولت الباحثة التعرض لمختلف الدراسات حول موضوع أمن المعلومات و التهديدات الأمنية و طرق تسييرها ، فمنها الأجنبية و العربية و منها الوطنية ، و من بين الدراسات على سبيل المثال لا الحصر نذكر:

الدراسات الوطنية :

1- دراسة شركة " ألجيريا ديجيتال تراندس" للتوجيهات الرقمية (2018)

قامت شركة " **ألجيريا ديجيتال تراندس**" للتوجيهات الرقمية بالتعاون مع مؤسسة " رابيد7" الرائد العالمي في قطاع ادارة المخاطر بدراسة احصائية شملت أكثر من 1000 مؤسسة جزائرية ، و مس التحقيق مديري و تقنيي المعلومات و مديري أمن المعلومات و كذا مديري الشركات الكبرى و المؤسسات الجزائرية حول تطور الهجمات الالكترونية و استخدام التدابير الأمنية ، حيث تم عرض نتائجها خلال الجلسة الافتتاحية للطبعة السادسة للقمة الافريقية للأمن السيبراني التي احتضنتها مدينة وهران افريل 2018 ، و خلصت الدراسة إلى جملة النتائج التالية :

- الشركات الجزائرية لا تزال بعيدة عن المقاييس المفترضة في مجال استخدام التدابير الامنية التي تتضاعف مع التحول الرقمي .
- أثبتت الدراسة أن 47 % من المؤسسات الجزائرية موضوع الدراسة اعترفت بانعدام أي حماية لنظامها من الهجمات الالكترونية ، و لا تملك أي معرفة بالقوانين المتعلقة بالأمن المعلوماتي ما يجعلها عرضة للقرصنة و الهجمات الالكترونية.
- 16 % من المؤسسات لا تملك نظم أمن الكتروني و 12 % لا تعرف النظم الأمنية للمعلومات ، و 17 % لازالت تفكر في انشاء نظم حماية.

- 52 % من المؤسسات صرحت أنها لا تملك سياسة لحماية المنظومات المعلوماتية ، و لا موظفين متخصصين و مؤهلين في مجال تقنيات الاعلام و الاتصال ، مع سهولة الولوج إلى أنظمة معلومات المؤسسات.
- 27 % من المؤسسات صرحت أنها عانت مدى 12 شهرا الماضية نوعا من الهجمات المعلوماتية من الفيروسات أو عمليات التصيد الالكتروني ، في حين 12 % عانت فقدان أو تلف البيانات بسبب خطأ بشري.
- 57 % من المنظمات تصرح أنها لا تستضيف بياناتها لدى سرفرات جزائرية.

2- دراسة رابحي عزيزة (2018)

بعنوان : الأسرار المعلوماتية و حمايتها الجزائية

تهدف هذه الدراسة إلى التعرف على السلوكيات المجرمة الماسة بالأسرار المعلوماتية و كيفية اثباتها خاصة إذا كانت عابرة للحدود ، و يشمل نطاق هذا البحث دراسة الجرائم الماسة بالسرية المعلوماتية التي تقع بواسطة النظام المعلوماتي و على النظام المعلوماتي نفسه ، و شملت الدراسة النظام المعلوماتي للحاسب الآلي دون الهواتف الذكية نظرا للتشابه بينهما ، و باعتبار أن الأنظمة المعلوماتية الغالبة على مستوى الحياة العامة و الخاصة هي أنظمة الحاسب ، و خلصت الدراسة إلى مجموعة من النتائج نذكر أهمها :

- وفق المشرع الجزائري حينما نص على الجريمة المعلوماتية و سماها جرائم الاعتداء على نظام المعالجة الآلية للمعطيات لأنه باعتبار أن محل الجرائم المعلوماتية هو المعلومات لا يمكن اعتبار أن تكون المعالجة الآلية بواسطة النظام المعلوماتي للحاسب الآلي فقط ، بينما أيضا أي جهاز آخر في حكمه .
- لابد على المشرع الجزائري إضافة بعض النصوص لسد الفراغ في إطار التجريم في مجال السرية المعلوماتية : إضافة نص تجريم قرصنة المعلومات مع استثناء البرامج لتجريمها بقانون حماية الملكية الفكرية و الأدبية ، التجسس المعلوماتي يختلف عن الدخول غير المصرح به للنظام المعلوماتي بمعنى الدخول غبر المصرح به جريمة و البقاء جريمة أخرى في حين الدخول بهدف التصنت و التجسس جريمة من نوع آخر و الفرق بينهما هو السلوك المترتب بعد الدخول ، لهذا لابد على المشرع إضافة نص صريح يتعلق بالتجسس المعلوماتي يجرم بشكل مباشر اعتراض البيانات المعالجة آليا.
- تختلف جريمة التجسس المعلوماتي عن جريمة السرقة المعلوماتية ، فالأولى الحصول على المعلومات السرية عن طريق اعتراض البيانات المنتقلة أما الثانية فتتعلق بالمعلومات المخزنة.
- التصنت المنصوص عليه في المادة 303 من قانون العقوبات الجزائري ينطبق على التجسس المعلوماتي ، و إنما كان من باب أولى النص عليه بموجب نص مستحدث على أساس أن المشرع الجزائري صادق على الاتفاقية العربية.

3- دراسة Kaspersky Lab (2017) :

Kaspersky Lab الرائد العالمي في أمن أنظمة المعلومات أعلن نتائج دراسة وطنية متعلقة بالتصرفات و المواقف المحفوفة بالمخاطر للأمن المعلوماتي للمؤسسات و المنظمات في الجزائر ، هذه الدراسة محققة من قبل مكتب الدراسة و الخبرة CEI حلفاوي ، و هي الاولى من نوعها ، و خلصت الدراسة إلى مجموعة من النتائج :

- 19% " من المهنيين المسؤولين لا يستعملون الحماية المعلوماتية ، ما يظهر مستوى مرتفع نسبيا من الضعف المعلوماتي للمؤسسات و المنظمات الجزائرية.
- 40 % من المجيبين يصرحون أن مؤسساتهم أصيبت بتهديدات معلوماتية : الفيروسات (85 % من المجيبين) ، البرامج الضارة (58 %) ، البرامج التجسسية (29%) و هي أكثر التهديدات تكررا.
- 68 % من المهنيين المسؤولين قد وضعوا تحاميل غير معروفة على حواسبهم و 19 % يفتحون ملفات مرافقة في رسائل مجهولة.
- 72 % من المهنيين يستعملون شبكات التواصل الاجتماعي في العمل و 43 % من المجيبين لا يغيرون كلمات المرور ، ما يفاقم مخاطر التدخل و التجسس.
- 54 % من المجيبين يصرحون بعدم معرفة استخدام أدوات الحماية المعلوماتية ، ما يمثل مستوى ضعيف من التحسيس و التكوين لمختلف طرق الحماية المعلوماتية.
- 56% من المهنيين المستجوبين هم مدركين بالهجمات الالكترونية الحديثة ، ما يدفع 87 % من المجيبين على القول أنهم متيقظين ضد الهجمات الالكترونية.
- 89 % من المهنيين المستجوبين قالوا أنهم مقتنعين أن تواجد هذه التهديدات يتطلب حماية معلوماتية.

4- دراسة بوربابة صورية (2016)[1]

بعنوان : قواعد الأمن المعلوماتي – دراسة مقارنة –

تنحصر مشكلة هذه الدراسة في تحديد **ما هي الحماية المطلوبة لتحقيق الأمن المعلوماتي ؟ و ما هو نطاق الجرائم التي تهدد نطاق الأمن المعلوماتي ؟** و تهدف هذه الدراسة إلى التعرف على قواعد الأمن المعلوماتي في ظل المواكبة التقنية و القانونية و أنظمة حمايتها عبر مختلف المستويات ، و إبراز الحماية التقنية و القانونية الجزائية في مسائل بعض الجرائم المعلوماتية ، و خلصت الدراسة إلى جملة من النتائج نذكر أهمها :

[1] **بوربابة صورية** ، قواعد الأمن المعلوماتي – دراسة مقارنة – ، رسالة دكتوراه ، كلية الحقوق و العلوم السياسية ، جامعة الجيلالي اليابس – بلعباس–، 2016.

- الأمن المعلوماتي الفني و القانوني هو الوسيلة المتاحة حاليا لبعث الثقة و تأمين التعامل عبر وسائل الاتصال الحديثة ، و أن الاجرام الالكتروني أو المعلوماتي يجب أن يحظى بتنظيم تشريعي واسع بين جميع الدول باعتباره اجرام عابر للحدود.
- رغم أن الدول العربية و منها الجزائر قد حاكت الدول الاوروبية في اصدار تشريعات لتنظيم الجرائم المعلوماتية إلا أن الواقع كشف عن عدم توفر امكانات ممارسة هذا النشاط سواء المادية أو الفنية أو الكوادر البشرية.
- النصوص التشريعية سواء الموضوعية أو الاجرائية التي جاء بها المشرع الجزائري من التعديلات الأخيرة للقوانين العقابية أظهرت عدم كفايتها لمواجهة مهددات قواعد الأمن المعلوماتي .
- مواجهة رجال القضاء و المحققين لبعض الصعوبات أثناء القيام بإجراءات التحقيق و الاستدلال للكشف عن الجرائم المعلوماتية و يرجع ذلك لعدم توفر الخبرة الكافية من جهة و لحداثة هذه الاجراءات و تعقد الظاهرة الاجرامية من جهة أخرى.

5- دراسة قدايفة أمينة (جامعة بومرداس) (2016)

بعنوان : استراتيجية أمن المعلومات

تم معالجة الموضوع تحت ضوء الاشكالية التالية : **كيف يمكن تبني استراتيجية أمنية ضرورية لحماية أمن المعلومات في المنظمة؟**، و تهدف هذه الدراسة إلى التأكيد على أن أهمية أمن المعلومات للمنظمات هي حاجة ضرورية ، و خلصت الدراسة إلى النتائج التالية :

- تواجه المنظمات مخاطر أمنية من مصادر كثيرة ، منها الأخطاء البشرية ، البيئية ، الجرائم المحوسبة ، لذا وجب وضع استراتيجية أمنية فعالة لمواجهتها.
- عند بناء استراتيجية أمنية يجب تحديد الاجابة عن التساؤلات الثلاثة التالية : ماذا أريد أن أحمي ؟ من ماذا أحمي المعلومات ؟ كيف أحمي المعلومات؟.
- ان أمن المعلومات يحتاج إلى استراتيجية قوية ، بهدف حماية البنية التحتية و مواجهة التهديدات.
- الاستراتيجية تتطلب متابعة و مراجعة بشكل دوري للتأكد من ملائمتها للتغيرات.

6- دراسة قارة ملاك (جامعة قسنطينة) (2016)

بعنوان : الجريمة المعلوماتية في القطاع البنكي و أساليب مكافحتها – إشارة لحالة الجزائر–

تتمحور اشكالية هذا البحث حول التساؤل التالي : **ما هي أهم أنواع الجرائم المعلوماتية المستخدمة في القطاع البنكي الجزائري ؟ و ما هي الطرق المستخدمة في مكافحتها ؟** حيث تهدف هذه الدراسة إلى تسليط

الضوء على أهم أنواع الجرائم المعلوماتية التي تمس القطاع البنكي الجزائري ، و أهم الطرق و الأساليب المستخدمة في مكافحتها ، و خلصت الدراسة إلى أن تنامي ظاهرة الجريمة المعلوماتية في الجزائر بصفة عامة و القطاع البنكي بصفة خاصة يعود إلى :

- نقص تأهيل إطارات القطاع البنكي ، فحسب التقارير المختلفة فان تعاملات البنوك الجزائرية مازالت تقليدية و هذا ما يجعلها متخلفة.
- القوانين المتعلقة بالحد من هذه الجرائم تعاني من نقائص ، فمثلا ما تنص عليه المادة 303 مكرر من قانون العقوبات بالحبس من 3 أشهر إلى 3 سنوات ، و الغرامة بين 50 ألف و 30 ألف دينار جزائري غير كافية لردع أصحاب هذه الجرائم.

و من جملة التوصيات و الاقتراحات التي خرجت بها الدراسة مايلي :

- ضرورة استعمال برمجيات تركيب لحماية أجهزة المعلوماتية و البيانات الخاصة و السرية من التجسس للأفراد و المؤسسات ، و هي تعتبر برامج وقائية ،كما هو الشأن بالنسبة لأرقام الحسابات البنكية و البطاقات الائتمانية.
- التشديد في القوانين و التشريعات المتعلقة بالحد من الجريمة.

ضرورة إجراء دورات تكوينية عالية التقنيات لموظفي القطاع البنكي قصد التعرف على أساليب الجرائم المعلوماتية الحديثة في القطاع البنكي.

7- تحقيق الجمعية الجزائرية لأمن نظم المعلومات (AASSI) (2015)

تم عمل تحقيق من قبل الجمعية الجزائرية لأمن نظم المعلومات على مجموع المؤسسات و المنشآت الجزائرية حول أنظمة المعلومات و أسفر التحقيق عن النتائج التالية :

- 1 % من المؤسسات و المنشآت يستعمل معيار أمن نظم المعلومات مثل ايزو 27001.
- 7.5 % ليس لديهم اجراءات الامتثال لتكنولوجيا المعلومات .
- 10/1 ليس لديهم مخطط استئناف النشاط.
- 1 % من المؤسسات يصرحون أن لديهم سياسة تسيير الثغرات.

و حسب تصريح مهدي زكريا رئيس الجمعية فان :

- لا يمكن أن نتحدث عن تعاليم أو عقيدة الأمن المعلوماتي عند مقرري تكنولوجيا الاعلام الجزائريين.
- أكثر الهجمات سببها قلة المعرفة التقنية و استغلال الثغرات المعروفة المرتبطة غالبا بسذاجة الضحية مثل هجمات احتيال الشخصية.

- هجمات رفض الخدمة DoS من الصعب اكتشافها في الجزائر ، و لكن ما هو أكيد أن مجموع المختصين في الأمن يقولون أن الجزائر تواجه كل سنة عدة مئات من هجمات رفض الخدمة تشوش على وسائل التواصل للبلد.

8- دراسة يحياوي إلهام و بن بوزة الصديق (2014)[2]

بعنوان : أهمية و دور تطبيق المواصفة القياسية الايزو 27001:2005 في مراكز نظم المعلومات الجغرافية – دراسة حالة بعض الدول العربية –

تهدف هذه الدراسة إلى ابراز **مساهمة الايزو 27001:2005 في إدارة و حماية أمن المعلومات بمراكز نظم المعلومات الجغرافية في بعض الدول العربية** ، و ذلك من خلال التعريف بالمواصفة الدولية الايزو 27001:2005 و تسليط الضوء على نظم المعلومات الجغرافية. و لقد توصلت الدراسة إلى أهمية تنفيذ هذه المواصفة ، فهي تسمح بتلبية مطالب المؤسسة من خلال وضع نظام ادارة و حماية المعلومات و التأكيد على عمل هذا النظام في ظل هذه المواصفة ، فهو صالح لكافة المؤسسات مثل مراكز نظم المعلومات الجغرافية ، كما يمكن اعتبارها مدخلا للتحسين المستمر لنظام ادارة المعلومات ، كما تمثل عملية تبني مواصفة الايزو 27001:2005 خطوة مثالية لبناء أمن فاعل لادارة المعلومات في المنظمة ، حيث تتحصل المنظمة التي تطبق هذه المواصفة على مجموعة من المميزات منها الصدق و المصداقية و زيادة ثقة الزبائن و أصحاب العلاقة كما أنها تؤكد على أن المنظمة تطبق جميع القوانين النافذة و التعليمات.

9- دراسة الشريف بوفاس و فاطمة الزهراء طلحي (2014)[3]

بعنوان : نحو بناء نظم لادارة حماية المعلومات ايزو 27001 في المؤسسات الجزائرية

تكمن مشكلة الدراسة في **دراسة الإطار النظري لأمن المعلومات و المواصفة القياسية ايزو 27001:2005**، و تهدف هذه الدراسة إلى توضيح المواصفة الدولية ايزو 27001 و تبيان دورها في إتاحة الفرص و القدرات و القابليات أكثر في التعامل مع المعلومات و البيانات التي تتسم بالتزايد و التعقد الكبيرين في منظمات الأعمال الانتاجية و الخدمية ، مع محاولة اسقاطها على واقع الحال و امكانية الاستفادة منها في بناء نظم لادارة و حماية المعلومات في المؤسسات الجزائرية ، و خلصت الدراسة إلى مجموعة من النتائج منها :

[2] **يحياوي إلهام و بن بوزة الصديق** ، أهمية و دور تطبيق المواصفة القياسية الايزو 27001:2005 في مراكز نظم المعلومات الجغرافية – دراسة حالة بعض الدول العربية – ، مجلة الاجتهاد للدراسات القانونية و الاقتصادية – المركز الجامعي لتمنغاست –العدد 5 ، 2014.

[3] **الشريف بوفاس و فاطمة الزهراء طلحي** ، نحو بناء نظم لادارة حماية المعلومات ايزو 27001 في المؤسسات الجزائرية ، المؤتمر الدولي للذكاء الاقتصادي حول : اليقظة الاستراتيجية و نظم المعلومات في المؤسسة الاقتصادية ، جامعة باجي مختار عنابة ، 2014.

- يعتبر المعيار العالمي الايزو 27001 من المعايير العالمية المتميزة إن لم يكن الوحيد المعتمد والذي يتميز بمرونته بحيث يتوافق مع جميع المنظمات حكومية كانت أو خاصة ، بحيث تقوم المؤسسة بدراسة المخاطر المتعلقة بمعلوماتها وفهمها ومن ثم بناء نظام أمن معلومات متكامل يقلل المخاطر وقابل للتطوير بناء على منهجية واضحة وموثقة.
- نستطيع القول أن المشرع الجزائري اليوم بدأ في مرحلة التركيز في مجال حقوق المؤلف في انتظار التركيز أكثر للتماشي مع متطلبات العصر الرقمي.
- إن جميع المنظمات والشركات الحكومية والخاصة لها معلومات مهمة تحاول الحفاظ عليها ، لذلك فإن تطبيق المعيار العالمي لأمن المعلومات يعتبر أمرا ضروريا لمساعدة المنظمة على تحقيق أمن المعلومات.
- نقترح على المؤسسات في الجزائر ضرورة التركيز على المفاهيم الحديثة التي تسلط الضوء على كل ما له علاقة بدورة حياة المعلومات ، والمواصفة (ISO 27001) و ضرورة الربط الواقعي بينهما ، إذ أن هذا الربط سيوفر وسائل فاعلة وناجحة للتعامل مع المعلومات ، فضلا عن أن حصول المنظمات على شهادة ISO في هذا المجال سوف يمكنها من الحصول على ميزة تنافسية ، وإكسابها الطابع العالمي من خلال حصولها على شهادة دولية.

-يجب بذل جهود اكبر من المعهد الوطني للتقييس فيما يخص تحديد الاحتياجات الوطنية في مجال التقييس، و من ابرزها اليوم المواصفة القياسية العالمية لأمن و حماية المعلومات.

الدراسات العربية :

1- دراسة رؤى يونس (2017)[4] :

بعنوان : دراسة واقع ادارة أمن نظم المعلومات في المؤسسات السورية

تهدف هذه الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في وزارة الاتصالات و التقانة و الجهات المرتبطة بها ، و استخدمت الباحثة في دراستها المنهج الوصفي التحليلي ، و خلصت الدراسة إلى النتائج التالية :

- الادارات العليا للوزارة و الجهات المرتبطة بها تدرك أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الجهات سياسات معمول بها و مطبقة على أسس واضحة .
- تتوفر البنى التحتية لنظم المعلومات في المؤسسات بدرجة متوسطة.
- تقوم المؤسسات بإجراء عمليات النسخ الاحتياطي الاعتيادي المجدول و الطارئ.

[4] **رؤى يونس** ، دراسة واقع ادارة أمن نظم المعلومات في المؤسسات السورية ، مجلة جامعة البعث ، المجلد 39 ، العدد 31 ، 2017.

2- دراسة نهاد عبد اللطيف و د. خلود هادي الربيعي (2013) [5]:

بعنوان : أمن و سرية المعلومات و أثرها على الأداء التنافسي

عالجت هذه الدراسة اشكالية **مدى تأثير أمن و سرية المعلومات على الأداء التنافسي لشركات التأمين** ، و طبقت هذه الدراسة في شركة التامين العراقية العامة وشركة الحمراء للتامين الأهلية كنموذج عن شركات التامين في العراق ، وباختبار عينة من المدراء والموظفين العاملين في الشركتين بعدد 70 موظفا وقد استخدمت استمارة الاستبانه كوسيلة لجمع البيانات ، واستخدمت تلك البيانات في اختبار فرضية البحث (وجود سرية و أمن المعلومات يؤثر ايجابيا على الأداء التنافسي) ولغرض اختبار الفرضيات استخدمت مجموعة من الوسائل الإحصائية التي توصلت إلى نتائج معينة كانت من أهمها وجود علاقة ارتباط وتأثير بين أمن وسرية المعلومات والأداء التنافسي لشركات التامين قيد البحث . و عليه أكدت النتائج صحة الفرضية . وقدمت الباحثان مجموعة من التوصيات إلى الشركتين استنادا إلى النتائج التي تم التوصل إليها وكان أبرزها ضرورة قيام إدارة الشركات باتخاذ كافة التدابير الضرورية و القيام بالممارسات العملية اللازمة لنشر وأعمام ثقافة أمن وسرية المعلومات في مختلف المستويات الإدارية عن طريق إعداد البرامج التدريبية.

3- دراسة أيمن محمد فارس الدنف (2013)[6]

بعنوان : واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة و سبل تطويرها

تم معالجة الموضوع بطرح الاشكالية التالية : **ما هو واقع إدارة أمن نظم المعلومات بالكليات التقنية بغزة ؟ و ما هي سبل تطويرها ؟** و استخدم الباحث المنهج الوصفي التحليلي ، و تكون مجتمع الدراسة من العاملين على نظم المعلومات في الكليات التقنية و جمعت أدوات الدراسة بين الاستبانة و المقابلة ، و خلصت الدراسة إلى مجموعة من النتائج أهمها :

- تتوفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة.
- تدرك الادارات العليا للكليات التقنية أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها و مطبقة على أسس واضحة.

---

[5] **نهاد عبد اللطيف عبد الكريم** ، خلود هادي الربيعي ، أمن و سرية المعلومات و أثرها على الأداء التنافسي – دراسة تطبيقية في شركتي التأمين العراقية العامة و الحمراء للتأمين الأهلية ، مجلة دراسات محاسبية و مالية ، المجلد الثامن ، العدد 23 ، 2013.

[6] **أيمن محمد فارس الدنف** ، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة و سبل تطويرها ، رسالة ماجستير ، الجامعة الاسلامية – غزة- كلية التجارة ، 2013

- توجد فروقات ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة .

4- دراسة ندى اسماعيل جبوري (2011)[7]

بعنوان : حماية أمن أنظمة المعلومات – دراسة حالة في مصرف الرافدين/فرع شارع فلسطين

تسعى هذه الدراسة إلى تحليل مؤشرات أمنية أنظمة المعلومات لمنع المخاطر و الاختراقات المحتملة من خلال اعتماد المقياس المعياري : نظام تسجيل المخاطر (CVSS) ، حيث أجريت هذه الدراسة بمصرف الرافدين/فرع شارع فلسطين بالعراق و ذلك باستخدام قائمة الفحص و المعايشة الميدانية ، و كان مشكل هذا البحث ملخصا في التساؤلات التالية :

- هل يمكن تطبيق نظام التنبيه عند التعرض للمخاطر المحتملة (CVSS).؟
- هل يمكن الاستفادة من تطبيق قياسات منع الاختراق و المحافظة على السرية في استخدام أنظمة المعلومات؟
- ما هي طبيعة العلاقات بين مؤشرات المقياس من اجل تحسين و تطبيق نظام أمني للمصرف؟

من خلال هذه التساؤلات كان الهدف من هذه الدراسة هو عرض و تحليل واقع و مؤشرات المقاييس الأمنية لمنع اختراق أنظمة معلومات المصرف المبحوث ، و تحديد العلاقات بين مؤشرات أمن أنظمة المعلومات و طبيعة ارتباطها بالقياسات الأمنية لتشخيص مستويات الدقة في توفير الأمن و الحماية لها.

و من جملة النتائج التي توصلت إليها الباحثة ما يلي :

- نظام معلومات المصرف المبحوث لا يستعمل إلا من قبل المخول في قسم نظم المعلومات ، مما يؤكد أن هناك حماية للنظام الأمني من الاختراق غير المفوض .
- المصرف لا تتوافر فيه برامج الكشف عن الاختراقات الأمنية بشكل مبكر مما يؤكد ضرورة تعزيز المصرف لاستخدام نظام التنبيه عند التعرض للمخاطر.
- المصرف يستعمل اجراءات الحماية البسيطة كاستعمال كلمة السر و التي من السهل اختراقها.
- انخفاض القيام بكشف المخاطر بالسرعة المطلوبة مما يستدعي قيام المصرف بتعزيز استخدام الوسائل التي تؤدي إلى توافر نظام المخاطر المتعلقة بالوقت.

[7] **ندى اسماعيل جبوري** ، حماية أمن أنظمة المعلومات – دراسة حالة في مصرف الرافدين/فرع شارع فلسطين ، مجلة تكريت للعلوم الادارية و الاقتصادية، المجلد 7 ، العدد 21 ، 2011.

- أسفرت النتائج عن عدم توفر صيانة كافية في المصرف لحماية أنظمة المعلومات ، و إذا ما حدث خلل أو اختراق للأجهزة يستعين المصرف بفريق عمل خارجي.

5- دراسة زكريا أحمد عمار (2011)[8]:

بعنوان : حماية الشبكات الرئيسية من الاختراق و البرامج الضارة

تمثلت اشكالية هذا البحث في التساؤل التالي : **ما هي طرق و وسائل حماية موارد شبكات الحاسب الآلي ؟** و تهدف هذه الدراسة إلى تحديد وسائل و إجراءات حماية الشبكات الرئيسية و مصادر المعلومات الموجودة فيها أو المنقولة منها على مستوى المؤسسات التعليمية بمدينة الرياض بالمملكة السعودية،حيث قام الباحث بتطبيق دراسته المسحية على العاملين في ادارة التشغيل و الحماية لتلك الشبكات ، و خلصت الدراسة إلى أن مشكلات حماية و تأمين موارد شبكات الحاسب الآلي ، لا تكمن في توريد و تثبيت الأجهزة و البرمجيات فقط ، و إنما في توفير و إعداد الانسان القادر على ادارة و تشغيل تلك الأجهزة و البرمجيات. و لعدم وجود توافق بين الهياكل التنظيمية و إجراءات و وظائف الموارد البشرية العاملة في مجال الحماية بالعينة المدروسة ، فان الوصول إلى حماية أفضل لشبكات الحاسب الآلي تتطلب إعادة تصميم الهياكل التنظيمية ، و للتغلب على صعوبات الحماية لابد من توفير أخصائيين في أمن المعلومات ، و توفير عدد كافي من موظفي أمن المعلومات يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية و توفير مسميات وظيفية مع بيان المهام و الواجبات .

6- منصور بن سعيد القحطاني (2008)[9]

بعنوان :مهددات الأمن المعلوماتي و سبل مواجهتها- دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض-.

تنحصر مشكلة الدراسة في التعرف على **مهددات الأمن المعلوماتي و سبل مواجهتها في ضوء تزايد معدلات الاختراقات غير المشروعة**، و هدفت هذه الدراسة إلى التعرف على مهددات الأمن المعلوماتي و سبل مواجهتها كهدف رئيسي للدراسة من خلال الكشف عن مصادر التهديدات و أشكالها ، و مدى فاعلية استخدام التقنية الحديثة لمواجهتها .

و خلصت الدراسة إلى مجموعة من النتائج أهمها :

[8] **زكريا أحمد عمار** ، حماية الشبكات الرئيسية من الاختراق و البرامج الضارة ، رسالة ماجستير ، جامعة النيلين ،كلية الدراسات العليا ، 2011.

[9] **منصور بن سعيد القحطاني** ، مهددات الأمن المعلوماتي و سبل مواجهتها- دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض ، رسالة ماجستير ، جامعة نايف العربية للعلوم الأمنية ،كلية الدراسات العليا ،2008.

- إن مصدر التهديد الذي يهدد الأمن المعلوماتي بمركز الحاسب الآلي بالقوات البحرية بدرجة قوية هو : عدم ضبط الاتصال بشبكة الانترنت ، و بدرجة متوسطة : إساءة الاتصال بشبكات خارجية مع مراكز المعلومات الأخرى و إساءة الاتصال بشبكات داخلية مع أفرع القوات البحرية .
- أشكال التهديد المحتملة تتمثل في : الفيروسات، و التنصت على حزم المعلومات عند تبادلها أو نسخها،و سرقة المعلومات الأمنية.
- التقنيات الحديثة التي تساهم في مواجهة التهديدات بمركز الحاسب الآلي للقوات البحرية هي : كاميرات المراقبة ، برامج مكافحة الفيروسات ، برامج تعريف المستخدم.
- من المعوقات التي تحد من فاعلية استخدام التقنيات الحديثة في مواجهة التهديدات هي : التطور المتسارع في ابتكار فيروسات جديدة ذات قدرات عالية في الاختراق ، سرقة و اتلاف و تغيير البيانات و الملفات، و استخدام برامج تحوي على ثغرات أمنية ، و استخدام وسائل تقليدية في تحديد هوية مستخدم النظام.
- السبل المهمة في تطوير قدرات المركز لمواجهة التهديدات هي : التزود بتقنيات متطورة في مجال نظم الحماية ، استخدام برامج مكافحة الفيروسات ، استقطاب خبراء حماية نظم المعلومات.

7- فاتن سعيد بامفلح (حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى) (2002)[10]

تهدف الدراسة إلى قياس مدى كفاية الاجراءات الأمنية المطبقة على شبكة مكتبات جامعة أم القرى ، و التعرف على مواطن القوة و جوانب القصور فيها و ذلك في سبيل تطوير تلك الاجراءات و زيادة أحكامها.

و خلصت الدراسة إلى النتائج التالية :

- تهتم عمادة شؤون المكتبات بجامعة أم القرى بتطبيق أساليب متعددة لحماية المعلومات على الشبكة منها : تأمين الشبكة من الناحية المادية ، ضبط إتاحة الوصول إلى شبكة المكتبات ، عمل نسخة احتياطية كاملة على قرص مدمج مرة كل شهر ، إضافة إلى عمل نسخ احتياطي تراكمي على القرص الصلب كل أسبوع ، استخدام مضاد الفيروسات على خادم الشبكة و محطات العمل ، إعتماد بعض القواعد التنظيمية لاستخدام الشبكات في الجامعة ، و لكن هناك عدة سلبيات في تطبيق الأمن نذكر : افتقاد بعض الأساليب الضرورية للأمن مثل الجدران النارية ، دعم أجهزة عدم انقطاع التيار الكهربائي ، نظام التشفير ، عدم تحديث مضادات الفيروس بشكل منتظم ،

[10] **فاتن سعيد بامفلح** ،حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى ، مقالة علمية ، مجلة الاتجاهات الحديثة في المكتبات و المعلومات ، المجلد 9 ، العدد 18 ، 2002.

تباعد الفترة الفاصلة بين كل نسخ احتياطي و النسخ الذي يليه ، عدم تحديد صلاحيات المستخدمين ، عدم تدريب الموظفين على كيفية التعامل مع المشكلات ، عدم الالتزام بالقواعد التنظيمية.

- **الدراسات الأجنبية :**

1- **دراسة (CLUSIF , 2014,2016,2018)[11] بعنوان :**

Menaces Informatiques et Pratiques de sécurité en France

نادي أمن المعلومات الفرنسي (CLUSIF) يقوم كل سنتين بتحقيق حول **التهديدات المعلوماتية و طرق الحماية** ، وذلك منذ 2008 إلى غاية 2018 ، و سنتطرق في هذا الجانب إلى آخر 3 دراسات ،ففي طبعته لسنة 2014 شملت الدراسة عينة متكونة من 350 مؤسسة و 150 مستشفى ، إضافة إلى تجارب مستخدمي الانترنت من البيت و تمثلت العينة في 1000 شخص ، و في سنة 2016 شملت الدراسة عينة متكونة من المؤسسات(334)و السلطات المحلية (203) ، و مستخدمي الانترنت من البيت (1008) ، أما في طبعة 2018 فتمثلت العينة في المؤسسات (350) و المرافق الصحية (200) ، إضافة إلى مستخدمي الانترنت من البيت (1000). و خلصت الدراسات إلى مجموعة من النتائج الخاصة بكل من المؤسسات و المرافق الصحية و مستخدمي الانترنت من البيت في فرنسا ، و لكن ما يهمنا هو النتائج الخاصة بالمؤسسات . و من النتائج التي خلصت إليها هذه الدراسات ما يلي :

- عدد أعوان أمن نظم المعلومات في تزايد مستمر على مر السنوات:2012 ، 2014 ، 2016 ، 2018.
- من ناحية الميزانية : يقصد بالميزانية قيمة الانفاق المخصصة للأمن من مجمل الميزانية المخصصة للمعلوماتية و المتمثلة أساسا في الحلول التقنية ، و هي في تزايد مستمر ، ففي سنة 2014 عرفت نسبة الانفاق انتعاش طفيف عن السنة التي قبلها ب26 % ، و 31% سنة 2016 ، أما سنة 2018 فعرفت ركود مقارنة ب 2016 (23%).
- من ناحية سياسة أمن المعلومات : عدد المؤسسات التي أضفت الطابع الرسمي على سياساتها الأمنية بلغت : 63 % ، 63 % ، 64 % ، 69 % ، 75 % ، على الترتيب التالي : 2010 ، 2012 ، 2014 ، 2016 ، 2018. وتأخذ مديرية نظم المعلومات الحصة الأوفر في إعداد السياسة بنسبة 54 % سنة 2014 ،

[11] CLUSIF (Club de la Sécurité de l'Information Français) , Menaces informatique et pratiques de sécurité en France, Enquête statistique réalisée pour le CLUSIF par le cabinet GMV conseil et Survey Sampling International , France , Edition 2014 ,2016 ,2018.

63 % سنة 2016 و 52 % سنة 2018 ، في حين بلغت مساهمة مسؤول أمن نظم المعلومات في إعداد السياسة 38 % سنة 2014 ، 39 % سنة 2016 و 43 % سنة 2018.

- وظيفة مسؤول أمن المعلومات أصبحت مع مرور الوقت أكثر وضوحا و تعريفا على مستوى المؤسسات، 62 % في 2014 مقابل 37 % في 2008 ، و بقيت النسبة في ارتفاع إذ بلغت سنة 2016 67 % ، إلا أنها عرفت بعض التراجع سنة 2018 من 67 % إلى 63 %. و في أغلب الحالات يكون مسؤول أمن نظم المعلومات مرتبط أو تابع لمديرية نظم المعلومات بنسبة تتراوح بين 42 إلى 46% و هذا ما يحد من قدرته التحكيمية لكن يبقى أفضل من عدمه ، و مؤخرا (2018) بدأت النسب في التغير إذ انخفضت نسبة مسؤولي الأمن المرتبطة بمديرية نظم المعلومات إلى 30 % ، و أصبح 49 %منهم مرتبطين بالمديرية العامة ، ما يحسن من قدرتهم التحكيمية.
- مستوى التحسيس لدى المؤسسات في ارتفاع مستمر.
- ما يقارب نصف المؤسسات صرحت أنها لا تقوم بترتيب و تصنيف المعلومات الحساسة لديها ، و فقط نصف المؤسسات تقوم بتحليل المخاطر ، و حتى إن كان 80 % منها جردت المخاطر الممكن أن تتعرض لها إلا أن 29% منهم فقط من يستخدم طرق مرجعية (Mehari , Ebios , ISO27005…).
- الحماية المادية تمحورت في 3 أنواع : كاشف الحريق (73%) ، مراقبة الدخول عن طريق الشارات (62%) ، و الكاميرات (57%).
- من ناحية تكنولوجيات الحماية : استعمال التشفير على مستوى الحواسب المحمولة بنسبة (33% سنة 2014، 43% في 2016) ، أنظمة كشف التدخل و التعريف بالهوية بنسب تتراوح ما بين 53% سنة 2014 و 64 % سنة 2016 ، جدران الحماية على مستوى الحواسب المحمولة (من 80% إلى 88% سنة 2018) ، مضادات الفيروس و البرامج الخبيثة على مستوى اللوائح الاكترونية و الهواتف الذكية بنسبة (42% إلى 54% سنة 2018).
- 44 % من المؤسسات وضعت نظم معلوماتها جزئيا أو كليا تحت بند الاستعانة بمصادر خارجية ، و ما بين 30 و 38 % منها لا تضع أي مؤشرات للأمن ، و ما بين 40 و 55 % من المؤسسات لا تقوم بأي تدقيق على هذه المصادر الخارجية.
- بالنسبة لحوادث أمن المعلومات : سنرتبها حسب السنوات :

تقرير 2014 : فقدان الخدمات الأساسية (39%) ، السرقة (37%) ، الأعطال الداخلية (35%)، أما بالنسبة للحوادث الناتجة عن الاصابة ببرمجيات خبيثة فالفيروسات تتصدر المشهد تليها الهجمات المنطقية المستهدفة.

تقرير 2016 : الاصابة بالفيروسات (44%) ، الاحتيال المعلوماتي (11%) ، الابتزاز المعلوماتي (11%) ، الهجمات المنطقية المستهدفة (7%).

تقرير 2018 : الأعطال الداخلية (28%) ، الفيروسات (27%) ، فقدان الخدمات الأساسية (22%).

رغم كل هذه الأرقام المخيفة إلا أن حوالي 50% أو أكثر من المؤسسات ليس لديها خلية لجمع أو معالجة حوادث أمن المعلومات.

- بالنسبة لاستمرارية النشاط ، ما يقارب ثلث المؤسسات لا تضع ضمان استمرارية النشاط ضمن حساباتها ،حيث أن سيناريو عد اتاحة نظم معلومات التسيير هو الأكثر حدوثا ، و حتى التي لديها مخططات استمرارية النشاط ، 25 % منها لا تقوم باختبارها ، فهل هي فعالة إذن؟

2- **دراسة Christophe Guillou و Alain Marcay (2015):**

Etude prospective et stratégique : Réseaux internet et sécurité

تهدف هذه الدراسة إلى إجراء تحليل مستقبلي إلى غاية عام 2030 للأمن السيبراني لشبكة الإنترنت المدنية ، لا سيما على المستوى التقني ، ولكن أيضا على الصعيد الاجتماعي والتنظيمي والقانوني والاستخدامات ، و من بين توقعات الدراسة أن الثورة القادمة بحلول 2030 ستكون حول :

- انترنت الآلات و بالتحديد (آلة مقابل آلة) ففي الواقع ، لن تكون شبكة الإنترنت مجرد ناقل للاتصال بين الأفراد والآلات ، بل بين آلات مستقلة تماماً وذكية بشكل متزايد .
- بخصوص الشبكات ذات الكفاءة المتزايدة ، فإن اتساع نطاق الأجهزة وخاصة البرمجيات ، سواء في المجال المهني أو عامة الناس ، سيوسع نطاق الهجمات الإلكترونية وشدتها ؛ و في هذا السياق الجديد المعايير الأمنية ستتغير و ستصبح أكثر تعقيدا .
- ستصبح حماية البيانات الشخصية ، التي كان تسبب في بادئ الأمر قلق إيديولوجي ، دعامة لمكافحة الجريمة المعلوماتية وانعدام الأمن المعلوماتي.

- كما أن التقدم المتوقع في مجالات تحديد الموقع الجغرافي سيزيد من الشعور بالترصد الدائم للسكان وربما يؤدي إلى تفاقم بعض المخاطر النفسية والاجتماعية .
- يصل نموذج المصادقة الحالي المستند بشكل أساسي إلى تركيبة تسجيل الدخول / كلمة المرور إلى حدوده ومن المتوقع حدوث تغييرات كبيرة في السنوات القليلة القادمة لتحسين المستوى العام للأمن وتبسيط حياة المستخدمين والتكيف مع خصوصيات الانترنت.

3- دراسة **Fernand Lone Sang (2012)**[12]**:**

Protection des systèmes informatiques contre les attaques par entrées-sorties

يركز الباحث في هذه الدراسة على التهديدات الخطيرة و يعالج بالتحديد الهجمات عن طريق الادخال و الاخراج و التي تحول و تزيف الوظائف الشرعية للأجهزة ، فالهدف من هذا البحث هو دراسة هذه الهجمات التي يكون من الصعب جدا تحديدها عن طريق تقنيات برمجية كلاسيكية ، لاقتراح معايير مضادة ملائمة و مرتكزة على مكونات مادية موثوقة و ثابتة . هذه الدراسة تركز على حالتين : المكونات المادية التي يمكن تصميمها بشكل مقصود لتكون ضارة وتعمل بنفس طريقة برنامج يضم حصان طروادة ؛و المكونات المادية الضعيفة التي تم تعديلها بواسطة مقرصن معلوماتي ، محليًا أو عبر الشبكة ، لإدراج وظائف ضارة . و لتحديد هجمات الإدخال / الإخراج ، قام الباحث بتطوير نموذج هجوم يأخذ في الاعتبار المستويات المختلفة من التجريد لنظام الكمبيوتر،ثم اعتمد على نموذج الهجمات هذا لدراستها وفقا لنهجين تكميليين: تحليل تقليدي للثغرات يتمثل في تحليل الثغرة و تطوير دلالات المفهوم و من ثم اقتراح معايير مضادة ، و تحليل الثغرات عن طريق الادخال /الاخراج ، بالارتكاز على أداة لحقن الخطأ الذي تم تصميمه و المسمى **IronHide** و القادر على محاكاة هجمات من مكون مادي خبيث.

4- دراسة **Géraldine Vache Marconato (2009)**[13] **:**

Evaluation quantitative de la sécurité informatique :approche par les vulnérabilités

هذه الدراسة حاولت تقديم منهجية جديدة حول التقييم الكمي لأمن نظم المعلومات ، و كان الهدف من هذه الأعمال هو تعريف و تقييم عدة معايير كمية ، هذه المعايير هي معايير احتمالية تهدف إلى تحديد تأثيرات المحيط على النظام المعلوماتي في وجود الثغرات . فقام الباحث بتعريف ثلاث عوامل لها تأثير كبير على حالة النظام :

[12] **Fernand Lone Sang** , Protection des systèmes informatiques contre les attaques par entrées-sorties, thèse de doctorat ,université de Toulouse , France , 2012.
[13] **Géraldine Vache Marconato** , Evaluation quantitative de la sécurité informatique :approche par les vulnérabilités, thèse de doctorat ,université de Toulouse , France , 2009.

1- دورة حياة الثغرة ، 2- سلوك فئة المهاجمين ، 3- سلوك مسؤول النظام ، و قام بدراسة هذه العوامل و ترابطها، و استنتج بذلك سيناريوهين أساسيين مرتكزين على طبيعة الثغرة المكتشفة خبيثة أو لا. هذه الخطوة سمحت بتحديد الحالات المحتملة للنظام من خلال النظر في عملية استغلال الثغرات وتحديد أربعة معايير تتعلق بحالة النظام الذي يمكن أن يكون ضعيف ، مكشوف ، مخترق ، مصحح أو آمن.

5- **دراسة Tim Lane (2007)**

بعنوان : Information Security Management in Australian Universities-an exploratory analisis(إدارة أمن نظم المعلومات في الجامعات الاسترالية)

تهدف هذه الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الجامعات الاسترالية ، و العوامل التي تؤثر على فاعليتها و كيفية تحسينها ، و أجريت الدراسة على مستوى 38 جامعة استرالية ، و خلصت إلى مجموعة من النتائج نذكر منها :

- العوامل المؤثرة في فاعلية إدارة أمن المعلومات هي نقص الخبرات و ضعف هيكلة إدارة أمن المعلومات ، ضعف الوعي الأمني و عدم الاكتراث لخطر التهديدات .
- يختلف واقع إدارة أمن المعلومات من جامعة لأخرى و ذلك حسب منهجية كل جامعة في الادارة الأمنية ، و مدى وعي و اهتمام الادارة العليا و حجم الانفاق على أمن المعلومات ، إضافة إلى الجهد المبذول في مواجهة التهديدات الأمنية و ثقافة المؤسسة.
- ضعف أو قوة إدارة أمن المعلومات مرتبط بمدى فاعلية العناصر البشرية باعتبارها الركيزة الاساسية للادارة الأمنية.

مكانة الدراسة الحالية من الدراسات السابقة :

- تتفق الدراسة الحالية مع دراسة **Tim Lane** و دراسة **زكريا أحمد عمار** و دراسة **قارة ملاك** في أن ضعف أو قوة إدارة أمن المعلومات مرتبط بمدى وعي و تكوين العنصر البشري باعتباره الركيزة الأساسية في الادارة الأمنية ، فتوفير الأجهزة و البرمجيات تحتاج كوادر بشرية ذات قدرات عالية من أجل التعامل معها ، و عليه فان العوامل المؤثرة على ادارة أمن المعلومات هو نقص الخبرات و ضعف الهيكلة التنظيمية.
- تتفق الدراسة الحالية مع دراسة **الشريف بوفاس و فاطمة الزهراء طلحي** و دراسة **يحياوي إلهام و بن بوزة الصديق** حول أهمية معيار ايزو 27001 و أنه من المعايير العالمية المتميزة إن لم يكن الوحيد في مجال أمن المعلومات و مواجهة التهديدات و التقدم في مجال امن المعلومات و الدخول في مصاف العالمية إضافة على قدرته في التناسب مع جميع أنواع المنظمات .
- تتفق الدراسة الحالية مع دراية **أيمن فارس الدنف** و **رؤى يونس** في أن المؤسسات لها ادراك تام بأهمية السياسات الأمنية إلا أنه لا يتم العمل بها و تطبيقها على أسس واضحة .
- تتفق الدراسة الحالية مع دراسة **قدايفة أمينة** في ان أمن المعلومات يحتاج إلى استراتيجية قوية ، بهدف حماية البنية التحتية و مواجهة التهديدات.
- تتفق الدراسة الحالية مع كل الدراسات السابقة حول أن معظم تدابير الحماية المتخذة تتمثل في : الكاميرات و مراقبة الدخول ، و برامج مكافحة الفيروسات و هذا لا يكفي خصوصا مع تطور التهديدات و تعقدها يوما بعد يوم فالأمن عبارة عن منظومة متكاملة و ليس شراء أجهزة و برمجيات و تركيبها.
- تختلف الدراسة الحالية مع دراسة **رابحي عزيزة** و دراسة **بوربابة صورية** في طريقة معالجة الموضوع ، فالدراسة الحالية عالجت الموضوع من وجهة اقتصادية إدارية تنظيمية في حين الدراستين المذكورتين عالجتا الموضوع من وجهة قانونية قدمت و حللت لنا كل القوانين و التشريعات التي تخص أمن المعلومات في الجزائر و مقارنتها مع قوانين في دول أجنبية. و تختلف الدراسة الحالية مع دراسة **Fernand Lone Sang** و دراسة **Géraldine Vache Marconato** لنفس السبب فهذين الأخيرين عالجا الموضوع بطريقة معلوماتية بحتة استخدموا فيها طرق كمية لقياس التهديدات و الثغرات و ابتكار برامج لاختبار مدى فعالية النظم القائمة.
- تختلف الدراسة الحالية مع كل الدراسات السابقة حول العينة المدروسة و مجال الدراسة ، إذ لم نجد دراسة واحدة تطرقت لموضوع أمن المعلومات على مستوى المؤسسات الجزائرية ما عدا دراسة قارة ملاك و لكنها خصصت

دراستها على القطاع البنكي فقط ، في حين الدراسة الحالية تتطرق للموضوع من كافة جوانبه و في نطاق أوسع شمل جميع أنواع المؤسسات الاقتصادية الجزائرية.

❖ **حدود الدراسة :**

- تقتصر حدود البحث النظرية في دراسة التهديدات المتعلقة بأمن المعلومات و الأساليب الصحيحة في مواجهتها سواء المادية أو البرمجية أو التنظيمية.
- تقتصر حدود البحث التطبيقية على عينة من المؤسسات الاقتصادية الجزائرية العاملة سواء في القطاع الصناعي أو القطاع الخدماتي ، أما بالنسبة للحد البشري فتمثلت وحدة المعاينة في المسؤولين عن نظم المعلومات أو مديري المؤسسات نظرا لخصوصية الموضوع و صعوبة التحكم فيه من غير المختصين ، و امتدت الدراسة من سبتمبر 2017 إلى ديسمبر 2018 .

❖ **صعوبات الدراسة :**

واجه هذا البحث مجموعة من الصعوبات منها :

- ندرة المراجع التي تعالج الموضوع باللغة العربية ما دفعنا إلى الاعتماد على المراجع الأجنبية خصوصا باللغة الفرنسية و هذا كلفنا وقتا أطول في الترجمة.
- عدم تجاوب المؤسسات الكبرى التي نعتقد وجود الظاهرة المدروسة فيها معنا ، فبمجرد سماع عنوان أو موضوع الدراسة يتم مباشرة رفض المقابلة و الاجابة على الاستبيان بحجة السرية و حساسية الموضوع ، الأمر الذي أثر سلبا على نتائج الدراسة فكيف ندرس واقع الأمن على مستوى المؤسسات الجزائرية إن لم تعطنا هذه الأخيرة المعلومات التي تساعدنا في الدراسة.
- تعامل بعض المؤسسات مع الموضوع باستخفاف كبير ، و أن الظاهرة المدروسة لن نلمسها في المؤسسات الجزائرية.

❖ **خطة البحث** :

تم تقسيم البحث إلى ثلاث فصول نظرية و فصل تطبيقي :

- الفصل الأول : **مدخل إلى أمن المعلومات** تم تناوله من خلال ثلاث مباحث ، المبحث الأول تم التطرق إلى مختلف المفاهيم الخاصة بالأمن الاقتصادي على مستوى الدولة و المؤسسات ، و المبحث الثاني كان حول تعريف المعلومات و أنظمتها ، أما المبحث الثالث فتم من خلاله دراسة أمن المعلومات من مختلف الجوانب (تعريف أهمية، مبادئ.....)
- الفصل الثاني : **تهديدات أمن المعلومات و سبل التصدي لها** ، تم تناوله من خلال مبحثين ، المبحث الأول تم التفصيل فيه في كل أنواع التهديدات التي يمكن أن تتعرض لها المؤسسة و خصائص مرتكبيها و الأسباب التي تدفعهم إلى ذلك ، أما في المبحث الثاني تم ذكر أهم طرق الحماية لمواجهة التهديدات المذكورة من حماية مادية و برمجية إلى حماية قانونية (ملكية فكرية).
- الفصل الثالث : **استراتيجية أمن المعلومات في المؤسسة** و تم تقسيم هذا الفصل إلى ثلاث مباحث ، حيث تم دراسة الجانب التنظيمي لأمن المعلومات من خلال المبحث الأول ، أما المبحث الثاني فتم من خلاله شرح عملية تسيير المخاطر و تم تخصيص المبحث الثالث لدراسة معيار الايزو 27001 و شرح دورة ديمنغ لأمن المعلومات.
- الفصل الرابع : **واقع أمن المعلومات في المؤسسات الجزائرية** ، حيث تم من خلال هذا الفصل اسقاط الجانب النظري على عينة من المؤسسات الجزائرية ، حيث تضمن المبحث الأول واقع أمن المعلومات على مستوى المؤسسات الجزائرية عامة و المؤسسة الوطنية للأشغال البترولية الكبرى خاصة ، أما المبحث الثاني فتم التعريف فيه بمنهجية الدراسة ، و تحليل النتائج كان من خلال المبحث الثالث.

الفصل الأول : مدخل إلى أمن المعلومات

المبحث الأول : مفاهيم حول الأمن الاقتصادي

المطلب الأول : الأمن الاقتصادي على المستوى الكلي (الدولة)

المطلب الثاني : الأمن الاقتصادي على المستوى الجزئي (أمن المؤسسة)

المطلب الثالث : علاقة الأمن الاقتصادي بالذكاء الاقتصادي

المبحث الثاني : مفاهيم حول المعلومات و أنظمة المعلومات

المطلب الأول : ماهية المعلومات

المطلب الثاني : أنواع المعلومات و مصادرها

المطلب الثالث : ماهية نظم المعلومات

المطلب الرابع : أنواع نظم المعلومات و مكوناتها

المبحث الثالث : مفاهيم حول أمن المعلومات

المطلب الأول : ماهية أمن المعلومات

المطلب الثاني : عناصر أمن المعلومات و خصائصها

المطلب الثالث : أهمية أمن المعلومات و اهم أهدافها

المطلب الرابع : مبادئ أمن المعلومات

تمهيد

لقد أصبح المجتمع في العصر الحديث يعتمد بالدرجة الأولى على المد المعلوماتي ، فظهور الأجهزة الإلكترونية المستخدمة في تكنولوجيا المعلومات ،و مختلف التقنيات و البرامج الحديثة ، و البيئة المعتمدة على المعلومات و الأفراد المستعملين لها ، و تطور الشبكات ، و الاعتماد الكبير على الحاسب الآلي و ظهور شبكة الانترنت ، كل هذا أكسب العالم مسمّى عصر المعلومات ، و أصبحت هذه الأخيرة مؤشر قوة المؤسسات ، إذ أن المعلومات و أنظمة المعلومات تعتبر من أساسيات الإدارة الفعالة في المؤسسات المعاصرة .

كما أن التطور المستمر لهذه العوامل سهّل من عمل المؤسسات و زاد من انتاجيتها ، و أصبحت معظم المؤسسات تستغل الإيجابيات و الفرص التي توفرها التكنولوجيات الجديدة ، و هذا يعد من مميزات عصر تكنولوجيا المعلومات ، و لكن في مسار موازي برز الوجه السلبي لاستخدام التقنية ، فالتطور التقني ساهم في ظهور أنواع جديدة من الجريمة لم تكن معروفة أهمها الجرائم المعلوماتية التي تعمل على التعدي على المعلومات و البيانات بمختلف الطرق ، و أصبحت المؤسسة الذكية هي من تتقن التعامل مع مخاطر التكنولوجيا ، و من هنا جاءت الحاجة إلى ايجاد طرق دفاعية و وقائية لحماية المعلومات ، و تكاثف جهود الباحثين و المتخصصين أدى إلى ظهور مفهوم جديد تستطيع المؤسسة أو الدولة تطبيقه و هو أمن المعلومات و الذي لا يقتصر فقط على حماية المعلومات و البيانات بشكل منفرد بل و يشمل الأمن المادي ،أمن الأفراد ، أمن العمليات و الاتصالات إضافة إلى أمن الشبكات.

و من هذا المنطلق يأتي هذا الفصل و الذي تم تقسيمه إلى ثلاث عناوين رئيسية ، فبالمبحث الأول سيتم إعطاء لمحة عن الأمن الاقتصادي للدولة و المؤسسة باعتباره مفهوم عام للأمن ، أما بالمبحث الثاني فسيتم استعراض المفاهيم و التعاريف الخاصة بالمعلومات و نظم المعلومات و هذا عبارة عن تمهيد للمبحث الثالث الذي يعتبر جوهر البحث و الذي سنغطي من خلاله الجانب النظري للبحث عن طريق التطرق لمختلف جوانب أمن المعلومات.

المبحث الأول : مفاهيم حول الأمن الاقتصادي

لقد عمل تحرير نشاطات العديد من القطاعات و تطوير التبادل الحر على رفع التهديدات الاقتصادية العالمية و تعدد أنواعها ، فبعد ما كانت كلمة خطر أو تهديد حصر على المجال العسكري ، تراجع خطر هذا الأخير فاسحا المجال لمخاطر من نوع آخر ، مخاطر غير مباشرة على رأسها الخطر ضد المصالح الاقتصادية الذي أصبح يبرز بصفة خاصة ، و عليه صار الأمن الاقتصادي يُحدد ضمن مفهوم "المصالح الأساسية للأمة " في ظل المنافسة الشرسة التي تعيشها الدول و التي أصبحت تُمثل بالحرب الاقتصادية ، إذ لم تعد الدولة هي المسؤولة الوحيدة عن الأمن ، بل المؤسسات جميعها ملزمة بالمشاركة لكونها متغير أساسي في الأمن الاقتصادي لحماية و متابعة مصالحها الحيوية ، و من خلال هذا المبحث سنتطرق إلى ثلاث نقاط أساسية :

- إعطاء لمحة عامة عن الأمن الاقتصادي للدولة بصفة عامة.
- إعطاء لمحة عن الأمن الاقتصادي للمؤسسة بصفة خاصة ، و هو ما يطلق عليه بأمن المؤسسة بما يشمله من حماية للممتلكات المادية و غير المادية.
- توضيح العلاقة بين الأمن الاقتصادي و الذكاء الاقتصادي.

المطلب الأول : الأمن الاقتصادي على المستوى الكلي (الدولة)

نتيجة للتطورات الاقتصادية و التكنولوجية الأخيرة ، و تلاشي كل أنواع الحواجز بين البلدان ليصبح العالم سوقا واحدا ، زادت التحديات و زادت المخاطر التي أصبح من الصعب التحكم فيها بصفة كاملة ، خاصة الجوسسة الاقتصادية أو التجسس الاقتصادي أو الصناعي بين البلدان ، ما جعل الأمن الاقتصادي ضرورة حتمية للدولة من أجل البقاء في هذا السوق الموحد و ليس خيارا يمكن التفكير فيه.

الفرع الأول:مفهوم الأمن الاقتصادي للدولة

هناك عدة تعاريف للأمن الاقتصادي نذكر منها:

- بالنسبة ل INHESJ[1] مفهوم الأمن عموما (على مستوى الدولة) هو : " القدرة على توفير للمجتمع و أعضائه مستوى كافي من الوقاية و الحماية ضد المخاطر و التهديدات من أي نوع و أي أثر." [2]
- تعرف الأمم المتحدة الأمن الاقتصادي على أنه: "أن يملك المرء الوسائل المادية التي تمكنه من أن يحيا حياة مستقرة و مشبعة."[3]
- كما يعرف الأمن الاقتصادي الوطني على أنه "المحافظة على الظروف المواتية المشجعة للزيادة النسبية لإنتاجية العمل و رأس المال و التي تضمن للأفراد مستوى معيشي مرتفع و يتحسن باستمرار ، و تأمين وضع اقتصادي عادل و آمن يشجع الاستثمار الداخلي و الخارجي و النمو الاقتصادي."[4]

التعاريف السابقة اعتمدت في مضمونها على الجانب الاجتماعي في تعريف الأمن الاقتصادي ،و اتفقت جميعها على أن هذا الأخير يتلخص في توفير الحياة المستقرة للأفراد و اشباع حاجاتهم و لكن هذا لن يتحقق إلا إذا فكرنا من منظور اقتصادي بحث في تعريف الأمن الاقتصادي.

- و لعل أنسب تعريف للأمن الاقتصادي يتوافق مع موضوع بحثنا هو التالي : " الأمن الاقتصادي هو تجسيد لسياسة دولة من أجل حماية و ترقية المصالح الاستراتيجية للدولة ، ففي جانبه الدفاعي يتضمن النشاطات التالية : حماية الممتلكات و الارث المعلوماتي و التكنولوجي للمؤسسات و السلطات العمومية ، تحديد المحيط الصناعي و التكنولوجي الخطر ، المقاومة ضد نشاطات الاستعلام الاقتصادي الأجنبية ، أما جانبه الهجومي يتمثل في مرافقة التطور الى العالمية".[5]

و من خلال هذا التعريف يتضح أن الأمن الاقتصادي ليس مجرد تأمين مأوى و ملبس و مأكل ، بل هو سياسة متكاملة هدفها حماية الدول و المؤسسات من التعديات الخارجية ، و تشمل الحماية الإرث المادي و الإرث المعلوماتي.

---

[1] INHESJ : Institut National des Hautes Etudes de la Sécurité ET de la Justice.

[2] **Pierre-Luc Réfalo** , "la sécurité numérique de l'entreprise « l'effet papillon du hacker »" , groupe Eyeolles , Paris, p85

[3] **سعيد علي حسن القليطي** ، "التخطيط الاستراتيجي لتحقيق الأمن الاقتصادي و النهضة المعلوماتية بالمملكة العربية السعودية"، مؤتمر تقنية المعلومات و الأمن الوطني ، الرياض ، 2007.

[4] نفس المرجع.

[5] Sécurité économique, portail de l'IE, centre national de ressources et d'information sur l'intelligence économique et stratégique, TROYES 24-26 septembre 2014 IES 2014 sur : http://www.portail-ie.fr/lexiques/read/44 visité le 26 septembre 2014.

الفرع الثاني : تطور سياسات الأمن الاقتصادي عبر الزمن[6]

لقد شهدت استراتيجيات الأمن الاقتصادي للدول تطورات عديدة تبعا لتطور الفكر التنموي ، فلمدة طويلة أكد الفكر الاقتصادي أن الدولة لن تتمكن من تحقيق أمنها الاقتصادي ما دامت عاجزة عن سد حاجياتها الغذائية عن طريق قدرتها الزراعية ، ثم تطور المفهوم و شمل بقية السلع الصناعية و أنه من أجل تحقيق أمن اقتصادي يجب توفير بدائل الواردات ، ثم تطور ليصل أنه على الدولة تنمية صادراتها و زيادة الموارد المالية المتأتية منها ، و مع اتساع سياسات الحرية الاقتصادية أصبحت استراتيجية الأمن الاقتصادي تقوم على:

- ✓ توفير البيئة المناسبة للاستثمار و التنمية.
- ✓ توسيع فرص العمل.
- ✓ تسيير سبل التقدم و الرفاهية و تقليص الانكشاف و منع التهديد الاقتصادي.
- ✓ تعظيم التنافسية و تعزيز القدرة الاقتصادية للمجتمع.
- ✓ السيطرة على معدل و اتجاه التنمية الاقتصادية.
- ✓ مقاومة وتحدي التداعيات السلبية للأزمات الاقتصادية الخارجية.

و في ظل الانطلاق السريع لاقتصاد المعرفة و ثورة المعلومات أصبحت الاستراتيجية الأساسية للأمن الاقتصادي المعاصر مبنية على الارتقاء بالتصنيع و تحقيق نقلة نوعية في انتاج السلع و الخدمات ذات القيمة المضافة المرتفعة ، و تعزيز بناء القدرات العلمية و التقنية و توفير مقومات اقتصاد يعتمد الابتكار بأولوية و أهمية قصوى و بمنهجية علمية هادفة إلى خلق تنافسية معززة لدور الدولة و جعلها أكثر تأثيرا في صنع القرار الاقتصادي العالمي.

و أصبح التحدي الرئيسي للأمن الاقتصادي الوطني يتمثل بفجوات الموارد المعرفية و التكنولوجية و البشرية ، وهذا ما يستدعي التأكيد على أهمية البعد الانساني في الأمن الاقتصادي.

الفرع الثالث : تحقيقات تقرير منظمة العمل الدولية حول الأمن الاقتصادي

لقد قامت منظمة العمل الدولية بعمل ثلاث تحقيقات على مستوى عدد كبير من المؤسسات على مختلف دول العالم من أجل الخروج بنتيجة حول مدى تطبيق الأمن في المؤسسات و الدول ، و مدى اختلاف درجة الأمن بين الدول حسب مستوى التقدم فيها و عناصر أخرى سيتم شرحها أكثر ، و يمكن ذكر التحقيقات كالتالي:[7]

[6] **أسعد حمود السعدون** ، " الأمن الاقتصادي : القديم الجديد "، جريدة أخبار الخليج البحرينية ، عدد يوم الثلاثاء 11 ماي 2010. أنظر : http://www.akhbar-alkhaleej.com/

التحقيق الأول:

إن **الأمن الاقتصادي عامل أساسي في تحقيق النمو و الاستقرار الاجتماعي،كما أنه العامل الأساسي في تحقيق السعادة** ، و هذا ما خرجت به منظمة العمل الدولية (OIT) كنتيجة للتحقيق الذي قامت به على مستوى 90 بلد مما يغطي 86 % من سكان العالم ، حيث ارتكز هذا التحقيق على 7 أشكال للأمن متعلقة بالعمل في ظل ادراك للسياسات و الأنظمة و النتائج في كل حالة.

و من جملة الاستنتاجات التي خرج بها التحقيق ما يلي:

- ✓ الأفراد في البلدان التي تقدم مستوى عال من الأمن الاقتصادي للصلاحيات و الاختصاصات لهم مستوى سعادة أعلى في العموم.
- ✓ المحدد الأساسي للسعادة الوطنية الأكثر أهمية ليس مستوى الدخل و إنما هو عامل درجة أمان الدخل و المقاس بمبدأ حماية الدخل.
- ✓ مستوى الكفاءة ليس هو المؤشر الأساسي للسعادة في العمل ، حيث يبين تقرير منظمة العمل الدولية أن مستوى أمن و أمان الكفاءات المقاس بمساعدة مرشدي التربية و التكوين هو العامل الأساسي في تحقيق السعادة و هذا سببه أن الكثير من الأفراد يدركون أن كفاءاتهم و مؤهلاتهم لا تتوافق مع الوظائف و الأعمال التي يقومون بها، و بالتالي يجب تعديل جودة و حركية العمل نحو الاعلى.
- ✓ الديمقراطية السياسية و الاتجاه المفضل للحريات المدنية يرفع من الأمن الاقتصادي ، كما أن نفقات الحكومة في مجال سياسة الأمن الاجتماعي هي أيضا عامل ايجابي.
- ✓ 73 % من مجموع العمال يعيشون في وضعية عدم الأمان الاقتصادي ، في حين 8 % فقط يعيشون في وضعية جيدة و في مؤسسات تمنحهم الأمن الاقتصادي المفضل.
- ✓ تحقيق الأمن في العمل يؤدي إلى تحقيق الأمن الاقتصادي العام.

[7]" l'insécurité économique est une crise mondiale ": un rapport de l'OIT montre comment et ou l'indice de la sécurité économique est lié au bonheur.2004 voir :
https://www.ilo.org/public/french/protection/ses/download/docs/happiness.pdf

- **التحقيق الثاني:**

في هذا التحقيق قامت منظمة العمل الدولية بضم 15 بلد خص حوالي 48000 عامل و عاملة تم التحقيق معهم حول **عملهم و عوامل عدم الأمن التي يعرفونها** ، فعدم الأمن الاقتصادي يؤدي إلى عدم التسامح و الضغوطات مما يؤدي إلى العنف الاجتماعي ، و من بين النتائج التي توصل اليها التحقيق ما يلي:

- ✓ أغلب العمال في البلدان النامية لا يعرفون النقابات ، و أغلبية العمال في البلدان المعنية بالتحقيق ليس لديهم ثقة كبيرة بها .
- ✓ النساء يعرفن اكثر من الرجال عن عدم الامان و انواعه.
- ✓ أمن العمل تناقص تقريبا في كل مكان بسبب عدم تهيئة ظروف العمل و الانفتاح.
- ✓ عدد كبير من الناس يمتلكون كفاءات لا يستعملونها في عملهم.

- **التحقيق الثالث:**

التقرير عمل أيضا **تحقيق خاص حول استقرار و أمن اليد العاملة للمؤسسات** عن طريق استجواب مسيري أكثر من 10000 مؤسسة في 12 بلد حول تجربتهم في مجال العمل ، فكانت النتائج أن المؤسسات التي توفر لليد العاملة مستوى أعلى من الأمن الاقتصادي لديهم فرص أكبر في النجاح في المخطط التجاري ، و في تطوير و تعميم العمل الاجتماعي.

تحليل المنظمة لنتائج هذه التحقيقات **خلص** إلى نتيجة أن الأنظمة التقليدية للأمن الاجتماعي و الاقتصادي غير مناسبة للإجابة على الأشكال الجديدة للمخاطر و عدم التأكد النظامي التي تشكل النظام الاقتصادي العالمي الجديد.

المطلب الثاني : الأمن الاقتصادي على المستوى الجزئي (أمن المؤسسة)

في ظل هذه المنافسة الاقتصادية العالمية أصبح الأمن الاقتصادي عامل فعالية المؤسسات ، فمهما كان حجم و نشاط المؤسسة ، فعلى رئيس المؤسسة إدماج الأمن الاقتصادي في استراتيجيته من أجل مواكبة التطورات و الاستعداد ضد التهديدات المتأتية من التكنولوجيات الجديدة من أجل ضمان مستقبل المؤسسة، فماذا نقصد بأمن المؤسسة؟

الفرع الأول : مفهوم الأمن الاقتصادي على المستوى الجزئي (أمن المؤسسة) :

أمن المؤسسة أو الأمن الاقتصادي للمؤسسة له عدة تعريفات نذكر منها:

- "أمن المؤسسة هو التحضر و التحسب ضد يقظة الآخرين ، إضافة إلى تزويد العمال بالمعارف و توضيح مضمون الحوارات الداخلية ، خلق ردود أفعال ، وضع بنود سرية في عقود العمل ".[8]
- "الأمن الاقتصادي هو الاعتماد في نفس الوقت على استراتيجية قانونية (ايداع براءات الاختراع ، حماية الماركات...) و على الأمان (معايير حماية المعرفة الاستراتيجية من خلال أنظمة المعلومات ، تحسيس أفراد المؤسسة ، ملاحظة تجارب و تصرفات المنافسين...) اضافة إلى انتباه المؤسسة للواجب القانوني في حماية مستخدميها و التيقظ على أن المعلومات الخاصة بهم محمية و مؤمنة و الفهم المعمق لشروط المنافسة ".[9]

نستنتج من خلال تعريفات أمن المؤسسة أن هذا الأخير أصبح جد ضروري في ظل الانفتاح المشهود ، و باعتبار أن المعلومة أصبحت مورد مهم من موارد المؤسسة ، بل ممكن أن تكون هي الأهم ، فضياعها أو افشاءها يمكن أن يكون له نتائج ثقيلة خاصة في ما يخص صورة المؤسسة ، رقم الأعمال و حصة السوق.

الفرع الثاني : أهداف الأمن الاقتصادي للمؤسسة

إن أمن المؤسسة ليست سياسة عشوائية و إنما هي عملية ذات أهداف من بين هذه الأهداف نذكر:[10]

- تعريف و تحليل المخاطر التي تستهدف المؤسسة.
- حماية المؤسسات و منشآت البحث مهما كان حجمها أو قطاع نشاطها مهما كان تطوره ، فكل مؤسسة قادرة على القيام بفعل الهجوم منذ الوقت الذي تكون فيه مبدعة و متطورة في قطاع المنافسة ، نفس الشيء بالنسبة لمنشآت البحث.
- بث ثقافة أمن الممتلكات المادية و غير المادية على مستوى مجموع المؤسسات و المجمعات الكبرى مثل المؤسسات الصغيرة و المتوسطة ، و مؤسسات البحث.

[8] la veille stratégique « du concept à la pratique » IAAT : Institut Atlantique d'Aménagement des Territoires, note de synthèse, juin,2005,p3.voir :www.iaat.org.
[9] le guide de l'intelligence économique, le guide du routard, HACHETTE LIVRE (hachette tourisme) 2014, p 40.
[10] Ibid, p 39.

و بالتالي فانه من الواضح أنه في هذا المجال لا يوجد صفر مخاطر ، و منه يكون همّ المؤسسة الوصول الى مستوى جيد من الانتباه و الحذر الذي لا يعيق نشاطها.

كما أن الهدف من الأمن الاقتصادي ليس مراقبة الأرض بأكملها و الحماية ضد كل ما يمكن تخيله ، و إنما الهدف هو محاولة فهم محيط المؤسسة خاصة المخاطر و التهديدات التي يمكن أن تواجهها و بالتالي التنظيم بطريقة متناسقة من أجل التخفيض من هذه المخاطر.

ومن بين الأهداف أيضا نذكر:

- توفير جو ملائم من أجل العمل و التطور.
- العمل بكل ثقة مع الشركاء و المساعدين داخل المؤسسة و كذلك مع الشركاء خارج المؤسسة.
- الترابط المنطقي و الواضح بين الأفكار حول النشاطات و المشاريع الاستراتيجية.
- القدرة على الدفاع في وجه المنافسين المستخدمين للطرق غير الشرعية (قرصنة المعلومات ، التجسس الاقتصادي، التزوير....).

الفرع الثالث : آلية تحقيق سياسة أمن المؤسسة

وضع سياسة أمن اقتصادي تسمح قبل كل شيء بإثارة الوعي بالمخاطر و التهديدات الخاصة بالمؤسسة من قبل مجموع المساعدين ، و تقليل الحيرة لرئيس المؤسسة.

و من أجل وضع سياسة أمن جيدة وجب المرور بعدة خطوات:

- **الحذر** : و يكون من خلال تبني موقف واقعي عملي يرتكز على واقع من الذكاء يعمل في نفس الوقت بالحذر و الانفتاح ، و يجب على كل واحد أن يفهم أن حماية مؤسسته يعني حماية عمله.
- **تحديد المخاطر و التهديدات**:كل المؤسسات معرضة للمخاطر مهما كانت صغيرة أو متوسطة أو قطاع منافستها قليل أو كبير، فالكل مستهدف من قبل المنافسين الذين لا يترددون لوهلة استغلال الضعف و قلة الحماية ، و بالتالي فانه من الضروري أخذ الوقت في تحليل أهم التهديدات التي يمكن أن تصيب المؤسسة. ومنها:

- **الأفعال الممنوعة** : التي تستغل ضعف سياسة الأمن كالتدخلات ،السرقة ،عدم استقرار الأشخاص ، القرصنة و التزوير و الوصول إلى الملكية الفكرية ، ضياع المعطيات بفعل اخطاء في التحكم ، تدمير وسائل الاعلام الآلي ، التشهير...
- **الأفعال المسموحة** :هناك أفعال خطيرة و لكن ليست ممنوعة قانونيا لأنها عبارة عن استغلال لقلة المهارة كاسترجاع سلة المهملات ، ملاحظة لقاءات الأشخاص ، التصنت للحوارات في الأماكن العامة ، الثرثرة.
- **الأفعال غير المباشرة** : و التي تستهدف الشركاء و المتعاملين المميزين للمؤسسة كالموردين و الزبائن و الوسطاء...
- **استغلال الثغرات** في سياسة الأمن و التهاون أو التهور.
- **غياب الحكمة و الرزانة** : افشاء الأسرار العامة ، نشر الحياة المهنية عبر مواقع التواصل الاجتماعي ، غياب الدقة في تطبيق الاجراءات.
- تحليل المعلومات الموجودة في المصادر المفتوحة بدقة.

- **التحفظ على المعلومات** : فقبل وضع برامج متخصصة في عملية الأمن يجب أولا أن تمر حماية المعلومة في الطريق الصحيح ، فالتحفظ يكون بالحذر في ما نقول خاصة في القطار أو الطائرة التي أصبحت أماكن تمر فيها المعلومة الاقتصادية بحرية تامة ، و بالتالي يجب تفادي الكلام عن العمل في الأماكن العامة لأن هناك أشخاص وظيفتهم التصنت و التقاط المعلومات عن المنافسين من خلال هذه الأماكن.

و بالتالي بعد هذه المراحل يمكن تسيير سياسة أمن عامة تضع في حساباتها دورة حياة المعلومة كالآتي:[11]

- ✓ تعيين شخص مسؤول عن الأمن داخل المؤسسة.
- ✓ القيام بتشخيص عام نستخلص من خلاله:
  - المخاطر و الحساسيات الموجودة.
  - ترتيب المعلومات الواجب حمايتها حسب درجة حساسيتها.
- ✓ تعريف و ترتيب الأهداف حسب الأولوية و متابعة تحققها من خلال المراقبة.

[11] " la sécurité économique au quotidien en 22 fiches thématiques", délégation interministérielle à l'intelligence économique , république française, avril 2014.voir : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/outils/fiches/22-fiches-rassemblees.pdf

- ✓ تسخير الوسائل البشرية و المادية في خدمة وضع سياسة أمن دقيقة.
- ✓ التحسيس: و يكون عن طريق اتاحة وسائل الاتصال لجميع الأفراد ، و وضع نشاطات تحسيس و تكوين ملائمة لكل مصلحة داخل المؤسسة.
- ✓ كتابة و نشر اجراءات الأمن اليومية، و تنظيم حوار منظم حول إشكالية الأمن أفقية أكثر منها عمودية.
- ✓ تنظيم خلية أزمات و مخطط تواصل النشاط ، و وضع معايير متبناة في حالة الحوادث.
- ✓ وضع قواعد للدخول إلى البيانات ، وسائل الاعلام الآلي ، الانترنت.....

هذه السياسة هي سياسة عامة على كل رئيس مؤسسة تكييفها مع حجم مؤسسته و ظروفها ، كما أنه لا يجب إغلاق و تشفير كل شيء و إنما يجب التيقظ لما هو مهم ، و أهم شيء أن تبقى هذه السياسة فعالة طوال الوقت رغم تغير الأشخاص و الأجهزة و الأنظمة.

المطلب الثالث : علاقة الأمن الاقتصادي بالذكاء الاقتصادي

إن الذكاء الاقتصادي هو الضمان الأساسي للدولة من أجل الدفاع عن مصالحها و حماية بقاء و استمرارية مؤسساتها ، و لكن لم تبقى سياسة الذكاء الاقتصادي حكرا على الدولة فقط ، بل المؤسسات بمختلف أنواعها أخذت نصيبها من هذا المفهوم الجديد من أجل حماية مصالحها الخاصة و ضمان بقاءها في ظل المنافسة الشرسة التي تعمل فيها ، و من خلال هذا المطلب سنقوم بإعطاء لمحة صغيرة عن الذكاء الاقتصادي ، و توضيح العلاقة بينه و بين الأمن الاقتصادي.

الفرع الأول : تعريف الذكاء الاقتصادي

تعددت تعاريف الذكاء الاقتصادي و اختلفت،و هنا سنذكر بعض التعاريف التي تتضمن عنصر الأمن و الحماية:

❖ أعمال المحافظة العامة للتخطيط بفرنسا مع تقرير " مارتر " سنة 1994 هم أول من أعطوا أول تعريف عملي للذكاء الاقتصادي ، إذ أن تقرير " مارتر " يعرفه كالتالي :" الذكاء الاقتصادي هو مجموعة الأعمال المرتبطة بالبحث ، معالجة ، و بث المعلومة المفيدة للأعوان الاقتصاديين ، مختلف هذه النشاطات موجهة بطريقة **شرعية**

مع توفير كل **ضمانات الحماية الأساسية لممتلكات المؤسسة** في ظل أحسن الظروف سواء من حيث الوقت الجودة ، أو التكلفة ."[12]

فبالتالي نفهم من هذا التعريف أن المعلومة يجب أن تكون محمية بمجموعة من الضمانات في جميع المراحل التي تمر بها من بحث وتحليل و بث.

❖ تعريف "Alain Juillet " المسؤول الأعلى للذكاء الاقتصادي بفرنسا : " الذكاء الاقتصادي هو أسلوب تحكم يعمل على السيطرة و حماية المعلومة الاستراتيجية لكل الأعوان الاقتصاديين من أجل الوصول إلى المنافسة ، الأمن الاقتصادي و أمن المؤسسات ."[13]

أي أن الذكاء الاقتصادي أسلوب يحقق الأمن الاقتصادي عن طريق التحكم الجيد في المعلومة الاستراتيجية.

❖ B.Besson,J.C.possin عرفا الذكاء الاقتصادي على أنه " السيطرة على المعلومة و انتاج المعارف الجديدة ، فهو فن اكتشاف الفرص و التهديدات ، بالإضافة إلى تحصيل ، اختيار ، تخزين ، مصادقة ، تحليل و نشر المعلومة المفيدة أو الاستراتيجية لمن هم بحاجة إليها في ظل توفير الحماية الملائمة لكل هذه المراحل ، و حماية ممتلكات المؤسسات. "[14]

من مجمل التعريفات السابقة نستنتج أن الذكاء الاقتصادي هو أسلوب تنتهجه المؤسسة من أجل الحفاظ على بقاءها و تحقيق التنافسية من خلال شقيه الدفاعي المتمثل في الأمن الاقتصادي ، و الهجومي المتمثل في اليقظة.

---

[12] **Henri Martre** ,« Intelligence économique et stratégie des entreprises », rapport du commissariat général au plan, la documentation française 1994, p 11.voir : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/rapport-martre.pdf

[13] **Jean Pierre Legendre «** l'intelligence économique » guide pratique pour les PME, rapport 2006 du CIE (le Cercle d'Intelligence Economique) du MEDEF paris, novembre 2006, p 5.

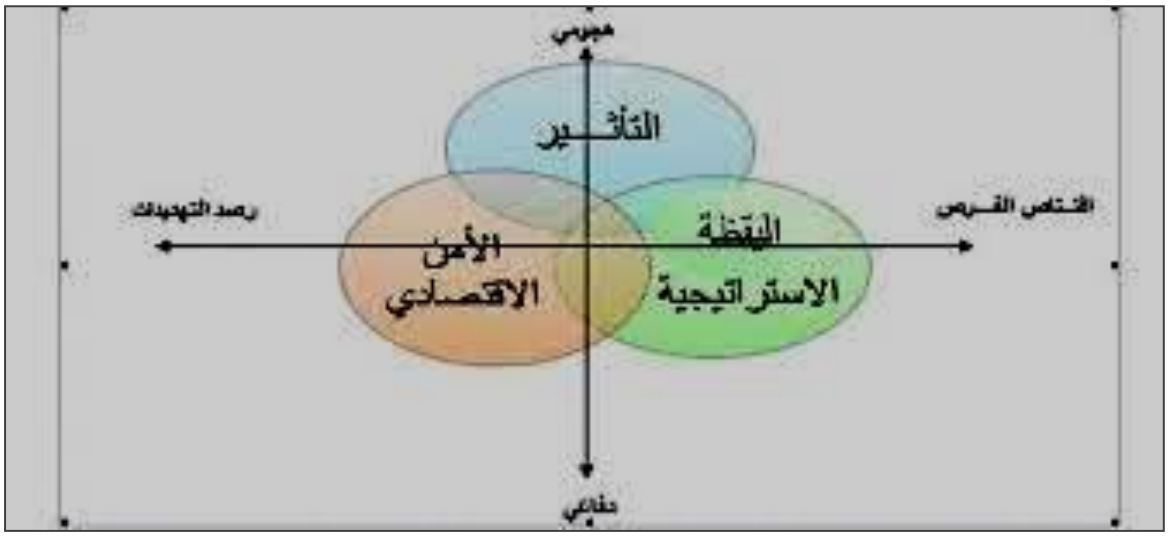
[14] définitions de l'intelligence économique, voir :http://www.actulligence.com/ressources/définitions-de-lintelligence-économique visité le 13/12/2012

الفرع الثاني:الأمن الاقتصادي عنصر من عناصر الذكاء الاقتصادي

حسب Sylvianne Descharmes المسؤول عن اليقظة الصناعية على مستوى l'ARIST[15] فان الذكاء الاقتصادي يتمحور حول ثلاث عناصر:[16]

- اليقظة.
- الأمن.
- التأثير.

الشكل1.1 : مكونات الذكاء الاقتصادي



Source : **Philippe CLERC**, « la veille stratégique institutionnelle, Association Internationale Francophone d'intelligence économique » ; CCI France ; 2013 , p.04

و بالتالي فان الأمن هو عنصر من عناصر الذكاء الاقتصادي.

[15] l'ARIST : الوكالة الاقليمية للمعلومة الاستراتيجية و التكنولوجية

[16] la veille stratégique « du concept a la pratique »IAAT « Institut Atlantique d'Aménagement des Territoires , note de synthèse, juin 2005, p 3, voir www.iaat.org.

أما عناصر الذكاء الاقتصادي بالنسبة للدولة فهي ثلاثة:[17]

- ضمان يقظة استراتيجية تسهل عملية اتخاذ القرار.
- دعم تنافسية المؤسسات.

- ضمان الأمن الاقتصادي للمؤسسات و مؤسسات البحث:فمن المهام الرئيسية للدولة في مجال الذكاء الاقتصادي هو ضمان الأمن الاقتصادي، و هذا يتطلب تعريف و توقع المخاطر التي تهدد المؤسسات و منشآت البحث من أجل ضمان حمايتها، فالمؤسسات اليوم تمارس نشاطاتها في إطار اقتصاد العولمة، السوق المفتوح، المنافسة المتزايدة، هذا الانفتاح و هذه المنافسة تفرض العديد من المخاطر على المؤسسات والتي تمس:

1- الإرث الاقتصادي العلمي و التكنولوجي.

2- صورة و سمعة المؤسسة.

3- رأس مال المؤسسة.

كما أن الذكاء الاقتصادي هو مفهوم يحتوي في مضمونه معنى " ذكاء المخاطر "، فبالنسبة ل CIE (دائرة الذكاء الاقتصادي) الذكاء الاقتصادي يجدد حماية المؤسسة عن طريق الأخذ بعين الاعتبار المخاطر و التهديدات المتعلقة بالأمن و حماية المحيط و الإدارة.[18]

أما Bernard Carayon في تقريره الذكاء الاقتصادي و التنافسية سنة 2003 خصص فصلا كاملا للأمن الاقتصادي أسماه " **من الدفاع الاقتصادي إلى الأمن الاقتصادي الفعال** " نوّه فيه بالدور الذي يمكن أن تلعبه الدولة في توقع المخاطر التي تتعرض لها المؤسسات الوطنية ، من أجل ذلك على المؤسسة وضع سياسة عامة للأمن الاقتصادي مما يفرض تكييف حديث للنصوص التشريعية من أجل تدعيم دور مصالح الدفاع الوطني.[19]

---

[17] **François Fillon,** "Actions de l'Etat en matière d'intelligence économique" , république Française, Paris le 15/09/2011 voir : www.**economie**.gouv.fr/.../2011_09_15_Action_de_l_Etat_en_matiere_d_IE .**pdf** Visité le 13/12/2012 à 10 :05

[18] **Jean Pierre Legendre**, op.cit, p33.

[19] **Rapport Carayon** 2003 : « Intelligence économique, compétitivité et cohésion sociale », publié par le portail de l'IE, centre national de ressources et d'information sur l'intelligence économique et stratégique le 09/02/2013 voir : http://www.portail-ie.fr/

من خلال ما تم التطرق إليه يمكن القول أنه و بالرغم من أن المبادرة و التدابير الهجومية هي من أولويات معظم الأعمال المتعلقة بالذكاء الاقتصادي إلا أن الجانب الدفاعي لهذا الأخير لا يمكن تجاهله ، فغياب أدوات التحكم للذكاء الاقتصادي يمكن أن يؤدي إلى عدم احترام السلوكيات و القوانين.

من خلال هذا المبحث الأول من البحث تم التطرق إلى كل جوانب الأمن الاقتصادي أو أمن المؤسسة باعتباره مفهوم شامل و عام و استخلصنا أن الأمن الاقتصادي هو سياسة عامة يمكن تطبيقها داخل المؤسسة بإتباع مجموعة من الخطوات لكن هذا لا يكفي فالمؤسسة التي تريد فعلا المحافظة على تنافسيتها عليها التعمق أكثر في هذا المفهوم و معرفة أن أهم شيء في الأمن الاقتصادي في الوقت الراهن هو حماية المعلومات و أنظمة المعلومات و التي سيتم التفصيل فيها في المبحث الموالي.

المبحث الثاني : مفاهيم حول المعلومات و أنظمة المعلومات

خلال السنوات الأخيرة ظهرت تغييرات نوعية في العديد من أوجه الحياة ، و بوتيرة عالية ، حيث مهّدت الطريق للانتقال من المجتمع الصناعي إلى مجتمع المعلومات أين أصبحت المعلومات تتبوأ موقع الصدارة في مختلف القطاعات الاقتصادية ، و أصبح العالم يتسم بغلبة المعلومات و الاتصالات و التكنولوجيات المستخدمة لها إلى درجة اكتسب فيها العصر اسما جديدا ، اسم عصر المعلومات ، فما المقصود بمجتمع المعلومات ؟ و ما هي المراحل التي مرت بها المجتمعات إلى غاية الوصول إلى مجتمع المعلومات ؟ ما المقصود بالمعلومات ؟ ما هي مصادرها الأساسية ؟ و ماذا نعني بنظم المعلومات و مما تتكون ؟ كل هذه الأسئلة ستتم الإجابة عليها من خلال هذا المبحث المخصص لتوضيح الجانب النظري للمعلومات و نظم المعلومات.

المطلب الأول:ماهية المعلومات

من خلال هذا المبحث سيتم تعريف مجتمع المعلومات ، و المراحل التي مرت بها المجتمعات إلى غاية مجتمع المعلومات ، كما سيتم إعطاء مجمل التعاريف التي تطرقت إلى مصطلح المعلومات و توضيح الفرق بينها و بين البيانات ، و أخيرا ذكر خصائص المعلومات الجيدة.

الفرع الأول : مجتمع المعلومات

أولا : تعريف مجتمع المعلومات

لابد من الإشارة أن هناك عدة تسميات لمجتمع المعلومات كالمجتمع الرقمي ، مجتمع المعرفة ، المجتمع الشبكي ، مجتمع اقتصاد المعرفة....

و من بين التعريفات التي تخص مجتمع المعلومات ما يلي:

- " هو المجتمع الذي يحرص على تصميم و إنشاء و تقييم و استخدام و صيانة منظمات معالجة المعلومات لما تشتمل عليه من معدات (Hardware) و برمجيات (Software) و جوانب تنظيمية و إدارية و سياسية و اجتماعية مترتبة على تلك المنظومات ".[20]

- كما يعتبر أنه " البيئة الاقتصادية و الاجتماعية التي تطبق الاستخدام الأمثل لتكنولوجيا المعلومات و الاتصالات الجديدة بما في ذلك الانترنت لنشر المعلومات نشرا عادلا يعم بالنفع على الأفراد في جميع نواحي حياتهم الشخصية و المهنية ".[21]

- و يعرف أنه :" البديل للمجتمع الصناعي بعد أن حصلت التطورات الهائلة في حجم و نوعية المعلومات ، و أصبحت تغطي مختلف مجالات الحياة للإفادة منها في التحديث و برامج التنمية و تطوير المجتمع ، كما أن فكرة هذا المجتمع تعني أن مجتمع المعلومات يعتمد على استخدام المعلومات و ليس على إنتاج المعلومات فحسب ، و المطلوب في هذا المجتمع توافر أساليب فنية مستحدثة تسمح للناس بصفة عامة و للباحثين بصفة خاصة بمسايرة و مواكبة النمو المتزايد في المعلومات ."[22]

و من خلال ما سبق تعرف الباحثة مجتمع المعلومات على انه المجتمع المعتمد على المعلومات في تطوره ، فبدل الاعتماد على الأراضي و المحاصيل الزراعية في المجتمع الزراعي و الآلات و الأجهزة في المجتمع الصناعي ، جاء مجتمع المعلومات الذي أساسه هو تكنولوجيا المعلومات الجديدة ، و التقنيات و البرامج الحديثة ، و أجهزة الحواسب الآلية و الشبكات التي أزالت الحواجز الزمنية و المكانية.

---

[20] **ثابت عبد الرحيم ادريس** ،" نظم المعلومات الإدارية في المنظمات المعاصرة "، دار الجامعة الاسكندرية ، دون طبعة ، 2005 ، ص 90.

[21] مشروع وثيقة نحو مجتمع معلومات عربي ، إطار خطة العمل المشترك ، المؤتمر العربي رفيع المستوى للتحضير للقمة العالمية لمجتمع المعلومات ، القاهرة ، 18/16 يونيو 2003.

[22] **زكي حسين الوردي** ، و **جميل لازم المالكي** ، "المعلومات و المجتمع "، الوارق للنشر و التوزيع ، طبعة 1 ،2006 ، ص 268.

ثانيا : نشأة و تطور مجتمع المعلومات

لقد مر مفهوم مجتمع المعلومات بعدة مراحل من التطورات جاءت في العديد من الدراسات و مناقشات علماء الاقتصاد و الاجتماع ، و غيرهم من المفكرين ، فنجد مثلا الباحث "**جاك لوزورن**" يوضح أن مجتمع المعلومات يمثل المرحلة الرابعة من مراحل تطور البشرية ، هذه الأخيرة مرت حسبه بثلاث مراحل و هي تمر الآن بمرحلة رابعة من تاريخها ، فالمرحلة الأولى تتمثل في الصيد و جني الثمار ، و المرحلة الثانية تتمثل في الزراعة ، و المرحلة الثالثة تتمثل في الصناعة ، أما الرابعة فهي في طور التشكيل مع انتشار تكنولوجيا المعلومات ، و تسمى هذه المرحلة بمرحلة المجتمع المعلوماتي.[23]

أما المجتمع المعلوماتي فهو بدوره مر بعدة مراحل جوهرية:[24]

أ- المرحلة الأولى : مجتمع غني بالمعلومات (1960-1979)

تعتبر هذه المرحلة الحاضنة المناسبة التي ترعرعت فيها البذرة الأولى لمجتمع مستحدث ، و التي ساهمت فيما بعد بظهور مجتمع المعلومات ، أهم ما يميز هذه المرحلة هو بروز المعلومات و التقنيات الأولية لخزنها و توظيفها و انتاجها.

ب-المرحلة الثانية : مجتمع مرتكز على المعلومات (1980-1989)

برزت هذه المرحلة نتيجة للتزايد في حجم المعلومات و التطور الهائل في تقنياتها ، و آليات توظيفها المتعددة ، و تعد العولمة الحجر الأساس الذي استندت إليه هذه المرحلة بعد أن زالت الحدود الجغرافية ، و السياسية التقليدية، و أصبح الطريق مفتوحا أمام نقل المعلومات ، و تداولها في كل مكان. كما ساد مبدأ الترابطية بعد طغيان شبكة الانترنت على جميع الفضاءات المعلوماتية ، فأتاحت تناقل البيانات و النصوص و الصور و الوسائط المتعددة بشتى أشكالها و صورها.

[23] **محمد لعقاب** ، "مجتمع الإعلام و المعلومات" ، دار هومة للنشر و التوزيع ، الطبعة الاولى ، الجزائر ، 2003 ، ص 69.
[24] **حسن مظفر الرزو**، "الفضاء المعلوماتي "، مركز دراسات الوحدة العربية ، الطبعة الاولى ،بيروت ، 2007 ، ص ص 245-246.

ت– المرحلة الثالثة : مجتمع هيمنة المعلومات (1990 إلى يومنا هذا)

أصبحت فيها عملية انتاج المعلومات ، و وسائطها المتعددة ، و نقلها و استخداماتها المتعددة رائدة الأنشطة الاجتماعية و الاقتصادية و الصناعية في المجتمع ، و بات التعامل معها لوصفها منتجا قائما بذاته ، أو خدمة تساهم في العملية الانتاجية أو الاستهلاكية للمواد التي ينتجها المجتمع.

الفرع الثاني: تعريف المعلومات

أشار "**يوزوا**" (الباحث الصيني) إلى أن مفهوم المعلومات له أكثر من ثلاثمائة تعريف ، و هو يعود اشتقاقيا إلى المصطلح اللاتيني information، و يعني عملية توصيل أو شيء يتم توصيله ، و يرى البعض أن المعلومات كالجاذبية و الكهرباء لا نستطيع وصفها بدقة ، و لكننا نعرف كيف تعمل و ندرك أثرها[25] و عليه يمكن ذكر التعاريف التالية:

- أول من عرف المعلومات "**MCKay** "سنة 1969 كما ورد في كتاب " **le Moigne** " حيث اعتبرت أنها " تغيير في المعرفة ".[26]

بمعنى أنه بمجرد الحصول على أي معلومة فإنه من الطبيعي حدوث تغيير في المعارف.

- " تعتبر المعلومات بمثابة الدم في عروق الإنسان ، فهي تغذي جميع وحدات و أقسام المنظمة بما تحتاج إليه لأداء أعمالها و مهامها ، إذ تشكل موردا استراتيجيا لها ، و الذي ينبغي توفيره بالمواصفات المطلوبة من حيث الدقة ، الوقت و الثقة ."[27]
- و حسب R.Reix: " المعلومة هي من يعطي لنا المعرفة، من يحسن نظرتنا للعالم، من ينقص من حالة عدم التأكد ."[28]
- و تعرف أيضا على أنها:"منتوج موجه للاستهلاك قابل للتخزين ، التحويل و المعالجة يشكل موردا هاما للمؤسسة ."[29]

---

[25] **عبد الرحمن القوي** ، "تكنولوجيا المعلومات و الاتصال و أثرها على إدارة الموارد البشرية "، رسالة ماجستير في العلوم التجارية غير منشورة ، جامعة محمد بوضياف ، المسيلة ، الجزائر ، 2007 ، ص 13.

[26] **Le MOIGNE Jean-Louis**, « les systèmes d'informations dans les organisations », cité par : **CHARRON Jean-Luc** et **SEPARI Sabine**, « organisation et gestion de l'entreprise », 2 éme édition, ED : Dunod, paris, 2001, p 307.

[27] **عزاوي عمر** و **عجيلة محمد** ، "مؤسسات المعرفة و ثقافة المؤسسات الاقتصادية – رؤية مستقبلية – " ، مجلة الباحث، كلية الحقوق و العلوم الاقتصادية ، جامعة ورقلة ، العدد الرابع ، 2006 ، ص 57.

[28] **Robert Reix**, « systèmes d'information et management des organisations » ,4 éme édition, Ed Vuibert paris,2002 , p 16

هذا التعريف تعامل مع المعلومة كمنتج يمكن استهلاكه.

- أما ضمن الدراسات المرتبطة بنظم المعلومات فهي تمثل " البيانات التي تم اعدادها لتصبح في شكل أكثر نفعا للفرد مستقبلا ، و التي لها قيمة مدركة في الاستخدام الحالي أو المتوقع أو في القرارات التي يتم اتخاذها "[30].

من خلال التعريفات السابقة تخرج الباحثة بتعريف شامل للمعلومات: المعلومات هي عبارة عن مورد استراتيجي يتم تخزينه، تحويله، معالجته من أجل الخروج بمعرفة تساهم في إزالة عدم التأكد، و المساعدة في عملية اتخاذ القرار.

❖ **الفرق بين المعلومات و البيانات:**

البيانات هي :" رموز لغوية أو رياضية أو معنوية متفق عليها رسميا لتمثيل الأفراد أو الأشياء أو الحوادث أو المصطلحات ، أما **المعلومات** فهي ما نحصل عليه من تمثيل أو تأطير أو تنظيم أو تحرير البيانات بطريقة تزيد مستوى المعرفة للأشخاص الذين يحصلون عليها ."

فالبيانات إذن هي حقائق تم تسجيلها بشأن أحداث معينة تمت أو ستتم مستقبلا ، هذه الحقائق قد تكون مستقلة و غير مرتبطة ببعضها و غير محدودة العدد ، أما **المعلومات** هي بيانات قد تم معالجتها بشكل أعطى لها معنى بالنسبة لمستقبلها أو مستخدمها ، و أضاف إليها قيمة حقيقية بالنسبة لعمليات صنع القرارات الحالية و المستقبلية و يمكن التعبير عن العلاقة بينهما كالعلاقة بين المادة الخام و المنتج النهائي ."[31]

الفرع الثالث : خصائص المعلومات

يحتاج متخذ القرار إلى معلومات ذات جودة عالية ، و تحدد جودة المعلومات بمدى ملاءمتها مع الموقف الذي يتخذ بشأنه القرار ، و يمكن تحديد خصائص المعلومات الجيدة من خلال الأبعاد الثلاثة التالية:[32]

1- **المحتوى:**

أ- **الموضوعية** : المعلومات ذات الجودة هي معلومة ذات موضوعية ، أي المعلومة التي تصف الوضعية المشاهدة بكل موضوعية و تكون بعيدة عن التحيز الذاتي للملاحظ.

---

[29] **Pierre Carrier et autres**, « bases de données dans le développement de système », Gartan Morin édition, canada , 1991, p 9.

[30] **Michel Ferrary** et **Yvon Pasqueux**, « management de la connaissance », éd Economica, paris, p 15.

[31] **عبد الرحمن الصباح ، عماد الصباغ ، "**مبادئ نظم المعلومات الإدارية الحاسوبية **"**، دار زهران للنشر و التوزيع، عمان، 2008، ص ص 5-4.

[32] **منال محمد الكردي ، طلال ابراهيم العبد ، "** مقدمة في نظم المعلومات الإدارية : المفاهيم الأساسية و التطبيقات **"**، دار الجامعية الجديدة ، الاسكندرية ، 2003 ، ص 40.

ب- **الدقة** : تكون المعلومات دقيقة إذا توفرت بكيفية كاملة و دون أي غموض في الحقيقة التي تصورها.

ت- **المصداقية** : يجب أن تكون المعلومات خالية من الأخطاء ، و كلما كانت قليلة الأخطاء كلما زادت درجة مصداقيتها.

ث- **الأثرية** : تكمن في قدرة إثبات صحة المعلومات ، و هذا بإعطاء مصدرها.

2- التوقيت (البعد الزمني):

أ- **ملائمة التوقيت** : يجب توفير المعلومات عند الحاجة إليها ، أي في الوقت المناسب.

ب- **الحداثة** : يجب أن تجاري المعلومات كل ما يحدث داخل المؤسسة أو خارجها.

ت- **الفترة الزمنية التي تغطيها المعلومات** : يجب أن يكون تقديم المعلومات حول ماضي و حاضر و مستقبل المؤسسة.

ث- **السرعة** : يجب أن يحصل المستعمل على المعلومات بأكبر سرعة ممكنة ، و هذا لاستخدامها في أقرب وقت ممكن ، و تكمن أهمية هذه الخاصية في بعض أنواع القرارات التي تحتاج إلى السرعة في التنفيذ.

3- **الشكل (الهيكل) :**

أ- **الوضوح** : يجب توفير المعلومات بطريقة و صورة سهلة الفهم.

ب- **درجة التفصيل** : يجب أن يكون هناك قدرة على توفير المعلومات في صورة ملخصة و مفصلة.

ت- **الترتيب** : يجب أن تعرض المعلومات في ترتيب منطقي.

ث- **أسلوب العرض** : يجب أن يكون هناك العديد من بدائل عرض المعلومات مثل : النصوص و الأرقام و الأشكال البيانية.

ج- **الركائز** : يجب أن تكون هناك إمكانية توفير أو عرض المعلومات من خلال حوامل مختلفة مثل الورق و وسائل الإعلام الآلي.

و هناك خصائص أخرى متعددة نذكر منها: [33]

- **الشكل** : تكون المعلومات كمية أو وصفية ، رقمية أو بيانية ، مطلوبة أو معروفة ، ملخصة أو مفصلة ، و عادة نحتاج إلى عدة أشكال وفقا لكل موقف.

- **المدى** : هو نطاق الأحداث و الأماكن و الأفراد التي تمثلها المعلومات.

[33] **محمد الفيومي** ،"مقدمة الحاسبات الإلكترونية و تطبيقاتها في نظم المعلومات المحاسبية"، مؤسسة شباب الجامعة، الإسكندرية، 1992، ص 44.

- **الشمولية** : أن توفر المعلومات لمستخدمها كل شيء يحتاجه لمعرفة موقف معين.
- **المرونة** : بمعنى قابلية تكييف المعلومات و تسهيلها لتلبية الاحتياجات المختلفة للمستفيدين.[34]
- **الإيجاز** : حيث أن تلقي المستخدم لمعلومات موجزة سيوفر عليه الوقت ، و يمكن الوصول للإيجاز عبر تلخيص البيانات ذات الصلة. [35]

و هناك خصائص ثانوية يمكن ذكرها كالتالي:[36]

- **إمكانية الوصول إليها** : يمكن الوصول للمعلومة وقت الحاجة لها و بالشكل المراد.
- **قابلة للتحقيق** : بمعنى أن تكون واقعية ، ليس هناك صعوبة في تحقيقها.
- **لها قيمة تنبؤية** : أي أنها مفيدة لمتخذ القرار كي يتنبأ بمآل الحال الذي سيتم اتخاذ القرار بشأنه .

و عليه تختلف خصائص المعلومات المطلوبة حسب رغبة و نشاط المؤسسة.

المطلب الثاني : أنواع المعلومات و مصادرها

لقد اكتسبت المعلومات في السنوات الأخيرة مكانة و بعدا استراتيجيا كبيرا في المؤسسة ، فأصبح لزاما على المؤسسة البحث ، و من ثم التحكم في الكم الهائل للمعلومات حتى تستطيع البقاء و الاستمرار ، و هذا لا يكون إلا من خلال التعرف على أنواع المعلومات التي يختلف تصنيفها من مستخدم لآخر ، و تختلف مصادرها من مصدر لآخر.

الفرع الأول : أنواع المعلومات

تحتاج المؤسسات إلى معلومات متنوعة و يمكن أن يختلف تصنيف المعلومات حسب أحد المعايير التالية:

- **معيار مصدر المعلومات**

هناك مصدران فإما أن تكون ناتجة عن عمليات المؤسسة ، فتعد معلومات داخلية ، أو تكون ناتجة عن بيئة المؤسسة فتعد معلومات خارجية.[37]

---

[34] **أحمد صالح الهزايمة** ، "دور نظام المعلومات في اتخاذ القرارات في المؤسسات الحكومية "، مجلة جامعة دمشق للعلوم الاقتصادية و القانونية، المجلد 25 ، العدد الأول ، 2009، ص395.

[35] **Bagad**, V.S, "Management Information Systems", 3 rd Revised Edition, India Technical publication pune, 2008, p15.

[36] **Bodnar , Jeorge and William Hipwood**," Accounting Information system" , new Jersy .Prentice-hall , 1995.

- **معيار طبيعة المعلومات**

تنقسم المعلومات حسب هذا المعيار إلى **أولية** و **ثانوية** ، **فالأولية** هي التي تجمع بصفة خاصة لمشكلة معينة ، و هي المعلومات المقدمة لأول مرة لمجموعة معينة أو فرد معين ، و قد يكون ما جمعه الأفراد لأول مرة مماثلا لما قد جمعته المنشأة في وقت مضى ، كما أن هذه المعلومات المجمعة هي أولية بالنسبة للمؤسسة حتى و لو قامت شركات أخرى بتجميعها.

أما المعلومات **الثانوية** فهي التي تم تجميعها و تخزينها مسبقا مع قابليتها للاسترجاع ، و غالبا ما يحتاج المديرون لهذا النوع من المعلومات الخاصة بالمشاكل التي يواجهونها ، و تتحدد منفعة و أهمية كل نوع حسب خصائص الصناعة أو المنشأة أو المستوى الوظيفي الذي تستخدم فيه هذه المعلومات.[38]

- **درجة التغيير**

فالمعلومات قد تكون **ثابتة** لا تتغير كأسماء العمال و تواريخ ميلادهم في مصلحة الموارد البشرية ، أما عناوينهم و حالتهم الاجتماعية ، و كذا مناصبهم فتعتبر معلومات **متغيرة**.[39]

- **درجة الرسمية**

فنجد هناك نوعين هما المعلومات الرسمية التي تقدمها نظم المعلومات للمؤسسة و المعلومات غير الرسمية التي تحصل عليها خارج نظم المعلومات للمؤسسة.[40]

و هناك تقسيم آخر لأنواع المعلومات و هو كالتالي : [41]

- **معلومات حسب طبيعتها** : تتمثل في المعلومات التسويقية و التجارية و المالية و الاجتماعية و التقنية و المحاسبية.....

[37] **محمد عبد العليم صابر** ،" نظم المعلومات الادارية "، دار الفكر الجامعي ، الاسكندرية ، 2007 ، ص 44.
[38] محمد الفيومي ، مرجع سابق ، ص 55.
[39] **محمد الفيومي** ، مرجع سابق ، ص 55.
[40] **محمد عبد العليم صابر** ، مرجع سابق ، ص 43.
[41] **CHARRON Jean-Luc et SEPARI sabine** , op.cit, p 310.

- **معلومات حسب هدفها** : هي معلومات حول التنظيم الداخلي، و معلومات حول أبعاد البيئة، و معلومات سياسية و جبائية، و معلومات على المؤسسات و معلومات تكنولوجية، و قانونية، أي تقسيمها حسب ما ترمي المؤسسة الحصول عليه من خلالها.
- **معلومات حسب شكلها** : هي معلومات مكتوبة، مسموعة، رقمية، رسوم، أشكال.....
- **معلومات حسب حاملها** : هي معلومات ورقية، و معلومات موجودة في أجهزة الإعلام الآلي، و معلومات على شكل ملصقات....

مما سبق نستنتج أن المؤسسة دائما بحاجة إلى توفير معلومات مختلفة ، و لكن مختلف هذه المعلومات من أين نأتي بها ؟، ما هي مصادرها المختلفة ؟ وهذا ما ستتم الإجابة عليه في الفقرة الموالية.

الفرع الثاني : مصادر المعلومات

يقصد بمصادر المعلومات " جميع الأوعية أو الوسائل أو القنوات التي يمكن عن طريقها نقل المعلومات للمستفيدين، كما أنه هناك من عرفها على أنها كافة المواد التي تحتوي على معلومات يمكن الإفادة منها لأي غرض من الأغراض ".[42]

و هناك مجموعة من التقسيمات لهذه المصادر اعتمدت على معايير عدة، لا يمكن التطرق لها جميعا، و عليه سنذكر التقسيمين الأكثر تماشيا مع طبيعة المؤسسة :

التقسيم الأول:

سنقوم بتلخيص هذه المصادر في الجدول التالي:

[42] **عامر قندلجي و آخرون** ، "مصادر المعلومات التقليدية و الإلكترونية "، دار اليازوري العلمية ، عمان 2009 ، ص23.

الجدول 1.1: المصادر الاولية و المصادر الثانوية للمعلومات

المصادر الأولية	المزايا	النقائص
الملاحظة	معرفة أولية ، تتجنب الانحياز في رد الفعل.	تأثير الملاحظة على ما يتم ملاحظته.
التجربة	التحكم في المتغيرات الهامة.	قد لا تصمم التجربة بطريقة جيدة.
المسح	وسيلة جيدة للوصول إلى عدد كبير من الأفراد.	تصميم قائمة الاستبيان و حجم المسح.
التقدير الشخصي	معلومات مستمدة من الخبرة ، قد تكون الوسيلة الوحيدة للحصول على المعلومات.	قد لا يمكن الاعتماد على رد الفعل.
المصادر الثانوية	**المزايا**	**النقائص**
معلومات الشركة	محددة للموقف ، موجودة بالفعل ، منخفضة التكاليف نسبيا.	التوقيت ، قد لا تكون متكاملة و في شكل صالح للاستخدام.
مشتراة من مصادر خارجية	غير متاحة من مصدر آخر ،سهولة الحصول عليها.	التكلفة ، احتمال انحيازها.
النشرات	منخفضة التكلفة.	قد لا تكون متحيزة.
الوكالات الحكومية	كم كبير من المعلومات ، معلومات مجردة ، و غير متحيزة.	قد لا تكون في شكل قابل للاستعمال.

المصدر : محمد الفيومي ،"مقدمة الحاسبات الإلكترونية و تطبيقاتها في نظم المعلومات المحاسبية"، مؤسسة شباب الجامعة، الإسكندرية، 1992، ص 54.

التقسيم الثاني :

يمكن تقسيم مصادر المعلومات أيضا إلى مصادر معلومات خارجية و أخرى داخلية.

- **مصادر المعلومات الخارجية**

باعتبار المؤسسة جزء من البيئة المحيطة ، فهي دوما بحاجة إلى التيقظ و جمع المعلومات عن أو من البيئة التي تعمل فيها ، و يمكن تلخيص مصادر المعلومات الخارجية كالتالي:

- **موردي المعلومات** : عن طريق شراءها من بنوك المعلومات و مراكز المعلومات.
- **المؤسسات** الدولية و الوطنية.
- **المتعاملون الاقتصاديون** من الموردين و العملاء و النقابات المتخصصة و غرف التجارة.

- **مصادر المعلومات الداخلية**

المؤسسة عبارة عن نظام يتكون من أنظمة فرعية كالنظام الفرعي التسويقي، النظام الفرعي المالي، النظام الفرعي للإنتاج...، هذه النظم تكون متفاعلة مع بعضها البعض من جهة، و مع المحيط الخارجي من جهة أخرى، فمن خلال التفاعل الداخلي والخارجي تتمكن المؤسسة من التزود بالمعلومات اللازمة لسير نشاطاتها.

المطلب الثالث : ماهية نظام المعلومات

لقد أصبحت نظم المعلومات في المؤسسات الحديثة مجال وظيفي مثله مثل أي مجال وظيفي آخر ، بل و أصعب مجال باعتبار أنه يتعامل مع المعلومات التي تعتبر عنصراً حساسا ، إذ أن مسؤولية نظم المعلومات هو توفير معلومات صحيحة و مناسبة و دقيقة و تقديمها للإدارة في المكان و الزمان الصحيح من أجل مساعدتها على القيام بمختلف وظائفها.

الفرع الأول : مفهوم نظام المعلومات

مع كثرة الباحثين في هذا الموضوع إلا أنهم لم يستطيعوا إيجاد تعريف موحد و محدد لنظم المعلومات ، لذا سنقوم بإعطاء مجموعة من التعاريف المختلفة ، و لكن قبل ذلك سنقوم بتعريف النظام.

أولا : مفهوم النظام

كلمة " système " من أصل يوناني ، و تعني مجموعة منظمة ، ظهرت و نمت أولا في مجالات العلوم الطبيعية، و بالخصوص في علم الأحياء من طرف الباحث " Bertalanffy " في سنة 1930.[43]

- أما عند الاقتصاديين مثل "André Marchal" فالنظام هو عبارة عن " مجموعة متناسقة ، لها غاية ، و مكونة من عناصر مترابطة ، و تسودها حالة من الاستقرار ."[44]
- "Jacque Lesourne" عرف النظام بأنه "مجموعة عناصر مرتبطة مع بعضها بمجموعة من العلاقات" [45]
- كما يعرفه Jean Gerbier بأنه " مجموعة من العناصر المتداخلة و المتفاعلة فيما بينها تشكل وحدة واحدة تقوم بوظيفة معينة ". [46]

[43] **LE MOIGNE Jean-Louis** , « les systèmes de décision dans les organisations » , ED : P.U.F , paris , 1974 , p 9.
[44] **LAMIZET Bernard** et **SILEM Ahmed** , « dictionnaire encyclopédique des sciences de l'information et de la communication » , ED : Ellipses , paris , 1997 , p 534.
[45] **Jean Gerbier** , «organisation et fonctionnement de l'entreprise », Edition Tec Doc-Lavoisier, paris , 1993 , p 49.

- أما J.Rosnay فيعرفه أنه " مجموعة من العناصر التي تكون في تفاعل ديناميكي ، منظمة من أجل تحقيق هدف معين ".[47]

- و من هذا المنطلق ، و وفقا لهذا التصور حول النظام يتفق العديد من الباحثين على أن النظام هو " مجموعة من الأجزاء المترابطة تهدف إلى تحقيق جملة من الأهداف ".[48]

و عليه فإن النظام هو عبارة عن مجموعة من العناصر المرتبطة ببعضها ، للقيام بوظيفة ما بطريقة متناسقة من أجل تحقيق مجموعة من الأهداف.

و لعل أقرب الأنظمة للإنسان هو " الجسم البشري " بعناصره الأساسية من الدورة الدموية و نظام الدورة العصبية، و الأنظمة التنفسية و الهضمية ، و التي تجمعها علاقات متكاملة و مترابطة و معتمدة على بعضها البعض ، و تعمل بكفاءة بهدف حفظ الحياة و أداء الجسم لوظائفه المختلفة.

ثانيا : مفهوم نظام المعلومات

إن مفهوم " نظام المعلومات " من المفاهيم الحديثة نسبيا ، و يرجع تاريخ ظهوره إلى بداية استعمال أجهزة الإعلام الآلي في ميدان التسيير في بداية سنوات السبعينات بفرنسا و بداية سنوات الستينات بالولايات المتحدة الأمريكية.[49]

- و يعرف نظام المعلومات على أنه " التكوين المتفاعل بين مكونات جوهرية للنظم و المعلومات، وبمعنى أوسع هو توليفة أو تركيبة منظمة من الأفراد، المكونات المادية للحاسوب، البرامج، شبكات الاتصال، و موارد البيانات التي يتم جمعها و معالجتها وتحويلها لمعلومات، و بالتالي توزيعها للمستخدمين في المنظمة ".[50]
- و يعرفه Reix أنه " مجموعة منظمة من الموارد المادية و البشرية ، و البرامج و البيانات ، و الطرق التي تسمح بجمع و معالجة و تخزين و ايصال المعلومات على أشكال مختلفة من بيانات و نصوص و صور و أصوات في المؤسسات ".[51]

---

[46] **Jean Gerbier**, op.cit , p 49.
[47] **PAULET Jean-Pierre** , « dictionnaire d'économie » , Ed :Eyrolles , paris , 1992 , p 228.
[48] LE MOIGNE Jean-Louis ,1974 , op.cit, p 9.
[49] **BALANTZIA Gérard** , « les systèmes d'information , art et pratique » , ED :organisation , paris , 2003 p 179.
[50] **سعد غالب ياسين** ، "أساسيات نظم المعلومات الادارية و تكنولوجيا المعلومات" ، عمان ، دار المناهج ، 2009 ، ص 19.
[51] **Robert Reix** , op.cit , p 75

- أما Dayan فيعرف نظام المعلومات على أنه " مجموعة منظمة و مترابطة من التقنيات، و الطرق، و القواعد المخصصة لإنجاز مهام جمع و تخزين و معالجة و نشر المعلومات بهدف مساعدة الأفراد و الجماعات داخل المؤسسة (المصالح ، الورشات ، الأقسام ، فرق العمل ، المدراء....) على اتخاذ قرارات التسيير ". [52]

من خلال تعريف Reix و Dayan نلاحظ أن الأول ركز فقط على المراحل التي تمر بها المعلومة داخل المؤسسة، و لم يذكر الهدف من نظام المعلومات، على عكس Dayan الذي ركز في تعريفه على الهدف من نظام المعلومات، و المتمثل في مساعدة الأفراد و الجماعات على اتخاذ قرارات التسيير مما يبين وجود وحضور العامل البشري ضمن أنظمة المعلومات.

و ضمن هذا السياق أكد كل من Mirrof و Mason بصفة قطعية وجود العنصر البشري للسير العادي لأي نظام معلومات.[53]

الفرع الثاني : الفرق بين نظام المعلومات و النظام المعلوماتي

نظرا للاعتقاد السائد أن نظام المعلومات و النظام المعلوماتي هما مصطلحان لمفهوم واحد ، وجب علينا تصحيح هذا الاعتقاد و تبيين الفرق بينهما ، من خلال إعطاء تعريف للنظام المعلوماتي و مقارنته مع تعاريف نظام المعلومات المذكورة آنفا .

فالنظام المعلوماتي (نظام الإعلام الآلي) هو مجموعة تتضمن أجهزة الاعلام الآلي ، الطابعات ، السكانير...) و برامج التشغيل (مجموعة البرامج الضرورية لسير الأجهزة) بهدف معالجة البيانات.[54]

من خلال هذا التعريف يتضح أن النظام المعلوماتي يتكون فقط من الأجهزة و برامج التشغيل، و الهدف من وجودها هو معالجة البيانات، أي هو مجموعة من الموارد المادية فقط، في حين أن نظام المعلومات هو مجموعة من الموارد المادية و البشرية و الاجراءات و البرامج هدفه انتاج معلومات محددة تساعد في عملية اتخاذ القرار .

و منه **نستنتج** أن النظام المعلوماتي ما هو إلا جزء من نظام المعلومات ، لأن نظام المعلومات يتكون من جزئين : النظام المعلوماتي المعتمد على استخدام الإعلام الآلي ، و نظام المعلومات اليدوي أو التقليدي.

[52] **DAYAN Armand**, « Manuel de gestion », Volume 1, Ed : Ellipses, Paris, 1999, p 949.
[53] **DUPUY Y et autres** , « les systèmes de gestion » , ED : Vuibert , paris , 1989 , p 35.
[54] **LAMIZET Bernard et SILEM Ahmed** , op.cit , p 303.

كما أن النظام المعلوماتي يشكل الجانب المادي أو التقني لنظم المعلومات في حين أن هذا الأخير لا يقوم فقط على الجانب التقني ، بل يرتكز أيضا على الجانب التنظيمي لتحقيق أهدافه ، و بالتالي النظام المعلوماتي هو عبارة فقط عن تكنولوجيا المعلومات المتمثلة في أجهزة الاعلام الآلي و برامج التشغيل يستعملها نظام المعلومات من أجل تحويل البيانات إلى معلومات.

الفرع الثالث : أهداف نظام المعلومات

تهدف نظم المعلومات إلى ضمان تدفق البيانات و المعلومات و تبادلها بين مراكز الأنشطة المختلفة بالمنظمة ، و جمع البيانات بطريقة متكاملة و تشغيلها بالطرق المناسبة ، و تخزينها ، و متابعة جميع التعديلات و التغيرات التي تحدث على البيانات و المعلومات المخزنة و تحديثها و استرجاعها في الوقت المناسب ، و تحقيق الأمن الكامل للمعلومات. و يحدد الكثيرون هدفا واحدا ملخصا في أن نظام المعلومات يهدف إلى تقديم الخدمة النهائية للمستفيدين.[55]

و يمكن تجزئة هذا الهدف إلى الأهداف التالية:

- مساعدة المديرين في مهامهم عن طريق تقديم المعلومات الدقيقة و الكاملة في الوقت المناسب.
- ربح الوقت و عدم شغل المسؤولين و المديرين في عملية البحث عن المعلومات و تحليلها .
- ضمان أمن المعلومات و عدم تسريبها بطرق غير شرعية.
- تحضير و تصفية المعلومات التي يعتمد عليها متخذ القرار في المؤسسة.

المطلب الرابع : أنواع نظم المعلومات و مكوناتها

تختلف أنواع نظم المعلومات باختلاف طبيعة المؤسسات، درجة تطور الدول، إضافة إلى عوامل أخرى كثيرة ، و من خلال هذا المطلب سنقوم بذكر أكثر الأنواع انتشارا من خلال عدة تقسيمات ، في حين أن مكونات نظم المعلومات هي نفسها مهما تغيرت العوامل و سنقوم بتلخيصها في أربعة مكونات كل مكون يتضمن عناصر فرعية.

[55] **أحمد صالح الهزايمة** ، مرجع سابق 2009، ص394.

الفرع الأول : أنواع نظم المعلومات

هناك عدة تصنيفات لأنظمة المعلومات ، سنتطرق لنوعين من التقسيمات:

التقسيم الأول : يمكن تصنيف نظم المعلومات كالتالي:

- **نظم العمليات التشغيلية** : هذا النوع من النظم له أهمية بالغة عند إدخال أنظمة المعلومات في المؤسسة نظرا للدور الكبير الذي تؤديه في تسيير العمل و في معالجة حجم كبير من البيانات و الأعمال الروتينية ، و ينقسم إلى ثلاثة أنواع:

أ- نظم معالجة المعاملات.

ب- نظم مساندة و مراقبة الإجراءات الصناعية.

ت- نظم مساندة الأعمال المكتبية و الاتصالات.

- **أنظمة دعم القرارات**:هي نظم تهدف إلى مساندة القرار الذي يتصف بسرعة التغير و صعوبة تحديد احتياجاته من المعلومات بصفة مسبقة، و يتم تصميم نظم دعم القرار بهدف مساندة مهمة إدارية معينة أو مشكلة محددة ، حيث يتم البحث عن المعلومات بصفة ذكية سواء كانت تلك المعلومات متواجدة داخل المؤسسة أو خارجها.[56]

- **النظم الخبيرة** : هي برامج تتسم بالذكاء ، تعتمد على معارف مستمدة من الخبرة الشخصية ، و تستخدم خبرة متخذي القرار في تقديم المشورة و النصح للمدراء في اتخاذ القرارات الصعبة ، كما تستخدم الاستدلال المنطقي للوصول إلى النتائج.

كما يعرف النظام الخبير على أنه نظام معلومات يقوم بحل المشاكل الخاصة ، حيث يعطي عدة حلول ، هدفه هو رسملة المعارف الخاصة بموضوع معين للوصول إلى تشخيص .[57]

- **نظم دعم الادارة العليا**:هي نظم مصممة و مكيفة مع حاجات مدراء الادارة العليا ، تدعمهم بالمعلومات و النماذج التحليلية اللازمة لصنع القرارات غير المهيكلة ، و تمكنهم من الوصول إلى المعلومات بطريقة سهلة و سريعة ، كما أن هذه المعلومات تكون ذات خصائص استراتيجية.

[56] **Robert Reix** , op.cit , p 82

[57] **Alain Bonnet , Jean Haton** , « Systèmes experts vers la maitrise technologique » ; Inter édition 1986 , p 44.

التقسيم الثاني :تقسم نظم المعلومات إلى نظم المعلومات التقليدية التي تشغل يدويا و نظم المعلومات المرتبطة بالحاسب الآلي و التي تعالج إلكترونيا .

- **نظم المعلومات اليدوية** : و هي الأنظمة التي تعتمد على الوسائل التقليدية و اليدوية في التعامل مع المعلومات كالورق و الأقلام في مختلف مراحل تشغيلها.
- **نظم المعلومات الآلية** : و هي النظم المرتبطة بالحاسب الآلي و تقسم إلى أربعة أنواع رئيسية:[58]

أ- نظم دعم القرارات.

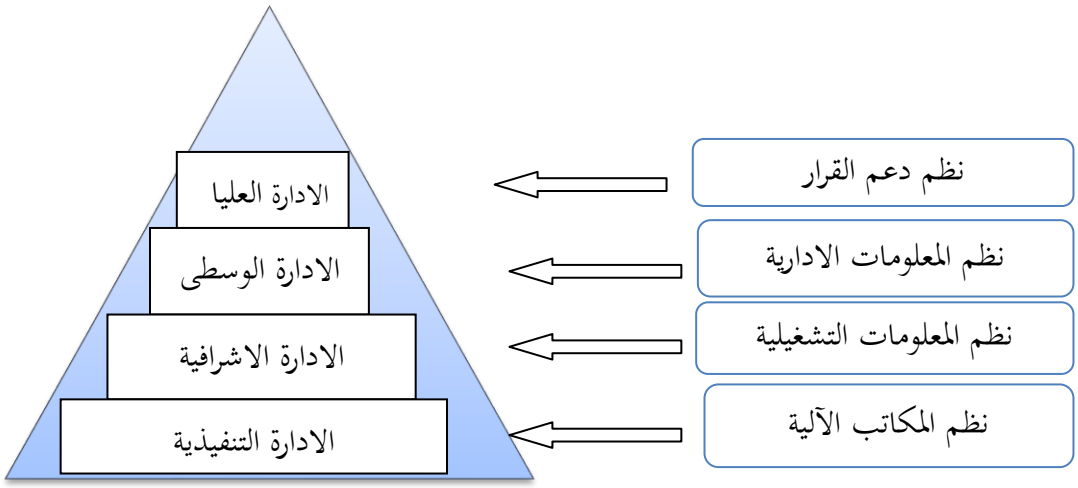
ب- نظم المعلومات الادارية.

ت- نظم المعلومات التشغيلية.

ث- نظم المكاتب الآلية

و سيتم التوضيح من خلال الشكل التالي:

الشكل (1.2): نظم المعلومات الآلية



المصدر : مدحت ابو النصر ، قواعد و مراحل البحث العلمي مرجع سابق ص 70

وضح لنا الشكل المستويات الادارية في أي منظمة معلوماتية و ما يقابل كل مستوى من نظم معلوماتية مناسبة له. فقاعدة الهرم هي أساس قيام الهرم، فالإدارة التنفيذية ضرورية للإدارة الإشرافية، و الإدارة الإشرافية ضرورية للإدارة الوسطى، و الإدارة الوسطى ضرورية للإدارة العليا و عليه فان نظم المكاتب الآلية تلزم لنظم المعلومات

[58] **مدحت ابو النصر** ،" قواعد و مراحل البحث العلمي" ، مجموعة النيل العربية ، الطبعة الأولى ، القاهرة ،2004 ، ص ص 69-70.

التشغيلية، و نظم المعلومات التشغيلية تلزم لنظم المعلومات الادارية، و نظم المعلومات الادارية تلزم لنظم دعم القرار.

الفرع الثاني : مكونات نظام المعلومات

يتضمن نظام المعلومات مجموعة مكونات تعتبر البنية التحتية المكونة له ، و يمكن تلخيصها كالتالي:

- **المكونات التقنية (مكونات تكنولوجيا المعلومات)**

و تشمل المكونات التقنية الملموسة و غير الملموسة ، و تسمى تكنولوجيا المعلومات (IT) أو تكنولوجيا المعلومات و الاتصالات (CIT) و تضم:

- **المكونات المادية للحاسوب (Hardware)**: و تشمل كل أنواع الحاسوب و ما يتصل به من معدات كالطابعات و الماسحات الضوئية و أجهزة الرسوم أو أي أجهزة أخرى تستحدثها تكنولوجيا المعلومات.[59]

- **المكونات البرمجية للحاسوب (Software)**: و تشمل لغات البرمجة التقليدية و الحديثة بكل مستوياتها و البرامج التي تعد بها ، و نظم التشغيل المختلفة ، و قواعد البيانات و نظم دعم القرارات، و قواعد المعرفة و النظم الخبيرة ، و لغات الذكاء الاصطناعي.[60]

و تعرف البرامج كذلك على أنها " مجموعة التطبيقات و الاجراءات و الطرق و الخدمات الأساسية من أجل سير أجهزة الاعلام الآلي "[61]. مما يعني أن برامج التشغيل يرتبط وجودها فقط بحضور أجهزة الاعلام الآلي.

و باعتبار البرمجيات المستخدمة هي العنصر الأساسي لنجاح النظم ، فمن الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ، و يمكن أن تحقق حماية للبرامج.

- **الشبكات و وسائط الاتصال** : تتشكل شبكة الحاسوب من ربط مجموعة أجهزة حاسوب باستخدام وسائط الاتصال لتكوين شبكة تبادل البيانات و المعلومات بين نظم الحاسوب المرتبطة بالشبكة ، كما أن نظم التشغيل المسؤولة عن ادارة الحواسيب يجب ان تتمتع بقدرة عالية على الكشف عن التسلل إلى الشبكة.

[59] **Stair, Relaph, Reynolds, George**, "Principles of information systems", USA: course technology ptr;2010
[60] Ibid,2010.
[61] **LAMDANI Sadek** « ,A la découverte de l'informatique » ,3éme édition, ED : Berti, Alger,2001 ;p 50.

و من مبدأ أهمية الشبكات فقد ذكر الكثيرون أنه لا معنى و لا قيمة لأي حاسوب يوجد منفردا و يعمل بصورة مستقلة من دون اتصاله من خلال الشبكة مع نظام الحواسيب الأخرى.[62]

- **الموارد البشرية (الأفراد):**

يرى الكثيرون أن أثمن مورد في بنية نظم المعلومات هي الثروة المعرفية و الفكرية و الادارية و التنظيمية المتمثلة بالعاملين في إدارة هذه النظم ، و تنقسم فئات الموارد البشرية إلى :

- **المستعملين** : و يقصد بهم الموظفين و الإطارات الذين يستعملون مخرجات و منتجات النظام في تنفيذ الوظائف و المهام الموكلة إليه ، كما يقصد بهم أيضا المشاركون في جمع و تخزين و معالجة و ايصال المعلومات.

- **العاملون في حقل المعرفة** : و هم من يقوم بانتاج المعرفة ، تخزينها و توزيعها ، و يقعون في المستويات التنظيمية العليا .[63]

- **المختصون في مجال تكنولوجيا المعلومات** : و يشملون هؤلاء العاملون في حقل نظم المعلومات من لجان الإشراف و مراقبة نظم المعلومات و مطوري النظم و محللي النظم ، و المبرمجين و مهندسي الحاسوب ، مديري الشبكات و الفنيين و غيرهم.

- **الإجراءات و السياسات:**

هي القواعد و الخطوات المكتوبة لإنجاز مهمة معينة ، و العمليات التي تتضمن مجموعة الخطوات و التعليمات المحددة لإنجاز العمليات الحسابية ، حيث ترسم السياسة العامة لنظام عمل الأجهزة و البرمجيات و تنسيق عمل الأفراد ضمن منظومة تحقق أهداف نظام المعلومات الجزئي أو نظام المعلومات بشكل كلي.

- **البيانات و المعلومات:**

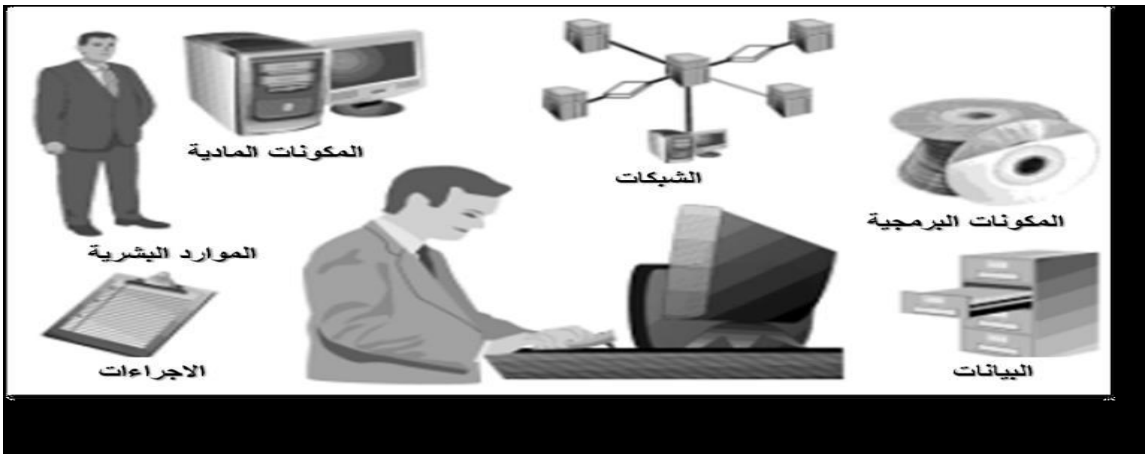
و هي بمثابة الوقود المشغل لنظام المعلومات ، و عصب المؤسسة و محركها الذي تدور فيه للتطوير و البناء.

و سيتم تلخيص مجمل هذه المكونات في الشكل التالي:

[62] **ياسين سعد غالب** ، مرجع سابق - ص 162 .

[63] **Laudon , Kemeth , Laudon , Jane**, "management information systems" , Managing the Digital Firm ,9th Edition , New jersy : Prentice-hall Inc , 2010.

الشكل:(1.3): مكونات نظم المعلومات



المصدر: course technology– cent age learning عن : أيمن محمد فارس الدنف ، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة و سبل تطويرها ، رسالة ماجستير ، كلية التجارة ، جامعة غزة ، 2013 ، ص 27

في نهاية هذا المبحث صارت لدينا فكرة جيدة حول المعلومات و أنظمة المعلومات و المكونات الأساسية لها و موقعها و أهميتها داخل المؤسسة ، و لكن هذه المعلومات لا يمكن أن تكون متاحة للجميع و في كل الأوقات و إنما يجب أن تكون محمية ، لهذا ظهر مؤخرا مصطلح أمن المعلومات ، أو أمن نظم المعلومات ، أو الأمن المعلوماتي و هذا ما سيتم تناوله من منظور نظري في المبحث الموالي.

المبحث الثالث : أمن المعلومات

لقد واجهت الإدارة في العصر الحديث حالة من التحدي نتيجة الثورة العلمية أو بمصطلح أكثر دقة الثورة المعلوماتية ، فالتطورات الحديثة في تقنية المعلومات أحدثت تغيرات مستمرة في جميع الميادين ، جعلت من عملية تداول المعلومات و انتقالها أمرا سهلا و سريعا و في متناول الجميع ، ما جعلها عرضة للخطر، و من هنا اشتدّ الانتباه إلى ضرورة و أهمية حمايتها و الحفاظ عليها و نتيجة لجهود الباحثين و المتخصصين في هذا المجال ظهر مصطلح أمن المعلومات. فما المقصود بأمن المعلومات ؟ هذا ما سيتم التفصيل فيه من خلال هذا المبحث عن طريق التطرق للنقاط التالية المصممة في شكل مطالب :

- ماهية أمن المعلومات.
- عناصر أمن المعلومات و خصائصها.
- أهمية أمن المعلومات و الأهداف التي تسعى المؤسسات إلى تحقيقها من خلال تطبيق الأمن.
- مبادئ أمن المعلومات.

المطلب الأول : ماهية أمن المعلومات

أصبحت سرية المعلومات و أمنها موضوعا يؤرق الإدارة العليا لأي مؤسسة أو منظمة في عصر المعلوماتية ، إذ أصبح من المحتم على كل مؤسسة توفير حماية و رقابة على أنظمة المعلومات و تختلف أساليب الحماية باختلاف أنواع التهديدات و مصادرها.

الفرع الأول : تعريف أمن المعلومات

قبل تعريف أمن المعلومات سنعطي تعريف للأمن بصفة عامة.

فقد أورد "H.Fayol" في كتابه **الإدارة العامة و الصناعية** الصادر عام 1916 ، ستة أنشطة هامة من مهام و مسؤوليات الإدارة ، و ذكر من ضمنها الأمن ، و الذي عرفه أنه " حماية الأفراد و الممتلكات بما فيه من أصول معلومات و تقارير خاصة بالمؤسسة ".[64]

و يعرفه "Laudon" أنه : " السياسات و الإجراءات و القياسات الفنية المستخدمة لمنع الوصول غير المخول أو التغيير أو السرقة أو الضرر المادي لنظم المعلومات ."[65]

كما يعرف الأمن بأنه " تأمين و حماية الممتلكات ذات القيمة ضد الضياع ، الإفشاء ، الكوارث الطبيعية ، التخريب ، و كل أنواع التهديدات عن طريق الحماية المادية كالأقفال و السياج ، و الحماية التقنية ككلمات المرور و الجدار الناري..." [66] و لكن تبقى الحماية التقنية أقل تفهما من طرف المؤسسة من الحماية المادية.

و بوجه عام فان مصطلح الأمن يعبر " إما عن التحرر من الخطر أو استعراض القوة و القدرة على الاستجابة للتهديدات أو عرقلتها " .[67]

و عليه فان الأمن بصفة عامة هو الإجراءات المتخذة لمواجهة الخطر.

---

[64] Bagad , V.S , op.cit , p 10.

[65] **Laudon, K.C. & Laudon , J.P.**, " Management Information System" ,6th ed., Prentice – Hill , International , New Jersey, 2005 , p 524.

[66] **Susan.M.Caldwell** et autres ,Manager la sécurité d'information , une recommandation , la revue n 85 , Février 2007 ; p 13.voir : http://www.isaca.org/chapters6/paris/b%C3%A9n%C3%A9fices/documents/s%C3%A9curit%C3%A9/85_pp11_18.pdf

[67] **ادوارد.ب ، بورودزيكيس**، ترجمة أحمد المغربي،" إدارة المخاطر و الأزمات و الأمن "، دار الفجر للنشر و التوزيع، القاهرة 2008، ص 72.

- أما أمن المعلومات فقد عرفه Whitman et Mattod في كتابهما " **مبادئ أمن المعلومات** " بأنه " الحفاظ على سرية و توفر و سلامة المعلومات كأصل في مراحل المعالجة و الحفظ و النقل ، و يتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية و من خلال تعزيز الوعي و التعلم و التدريب.[68] و يرى كلاهما أن أي مؤسسة تهدف لتحقيق ادارة أمن نظم المعلومات فإنه يجب أن يشمل المكونات التالية :

- **الأمن المادي** : بما يشمله من مصادر و ممتلكات و مباني لمنع الوصول غير المشروع.
- **أمن الأفراد** : لحماية الافراد و المجموعات الذين لهم حق الوصول للمعلومات.
- **أمن العمليات** : لحماية الأنشطة و العمليات التي يقوم بها المخولون.
- **أمن الاتصالات** : لحماية الوسائط و التكنولوجيا المستخدمة و المحتوى.
- **أمن الشبكات** : لحماية مكونات الشبكة و التراسل و المحتويات.
- **أمن البيانات** : لحماية سرية و سلامة و توافر المعلومات.

الشكل (1.4): مكونات أمن نظم المعلومات

المصدر : **من** إعداد الباحثة بناءا على تعريف Whitman et Mattod

[68] **Whitman Michael , Mattod Herbert** ," Principles of Information Security" , 4th Edition , Boston: cengage learning/course technology , 2011.

و من خلال هذا التعريف يتضح لنا جليا أن أمن المعلومات ما هو إلا مصطلح يضم في محتواه أمن عام فحماية المعلومات تكون من خلال الأمن المادي كالأجهزة التي تضم المعلومات ، و أمن الأفراد الذين يملكون المعلومات ، و كل العناصر الاخرى التي لها علاقة بالمعلومات.

- كما يعرف أمن المعلومات أنه " مجموعة من الاجراءات الادارية و الفنية التي صممت لضمان حماية الأجهزة و ملحقاتها ، و البرامج و البيانات من السرقة أو التوقف أو التلف المتعمد أو غير المتعمد ، أو التخريب أو التبديل أو مجرد الإطلاع دون تصريح بالاستخدام ، و حماية شبكة المعلومات الداخلية و الاتصالات الخارجية من الاختراق أو التعطيل المتعمد أو غير المتعمد ".[69]
- و عرفه مجمع اللغة العربية في معجم الحاسبات أنه " حماية المعلومات من الكشف أو الاستنساخ أو التدمير من قبل أشخاص غير مصرح لهم سواء كان عرضا أو عمدا ".[70]

هذا التعريف ركز على حماية المعلومات بصفة خاصة من الأشخاص غير المصرح لهم بالإطلاع.

- و يرى "**غيطاس**" أن أمن المعلومات هو تلك " الرؤى و السياسات و الإجراءات التي تصمم و تنفذ على مستويات مختلفة ، فردية و مؤسسية و مجتمعية تستهدف تحقيق عناصر الحماية و الصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية ، و السلامة ، و التوافر حين الحاجة ".[71]

نلاحظ أن هذا التعريف عالج مصطلح أمن المعلومات بمفهوم عام ليس فقط على مستوى المؤسسة و إنما أيضا على مستوى المجتمعات و الأفراد ، و بين أن أمن المعلومات هو مجموعة سياسات هدفها ضمان سرية و سلامة و توافر المعلومات.

- و في ضوء فرض القيود و تحديد صلاحية الاستخدام يعرف أمن المعلومات على أنه " فرض ضوابط على سبل و أساليب الوصول للمعلومات، بهدف إضفاء الشرعية على حدود و صلاحية استخدام المعلومات ".[72]

أما هذا التعريف فهو ينظر لأمن المعلومات من منظور قانوني.

- و بالنظر إلى أمن المعلومات من عدة زوايا ، فيمكن تعريفه على هذا الأساس:

- **من زاوية أكاديمية (علمية)**: هو العلم الذي يبحث في نظريات و استراتيجيات و سياسات توفير الحماية للمعلومات من المخاطر التي تهددها و من مختلف أنشطة الاعتداء التي يمكن أن تتعرض لها.

---

[69] **الشدي طارق عبد الله** ،" آلية البناء الأمني لنظم المعلومات "، دار الوطن للطباعة و النشر و الإعلام ،الرياض ،2000 ، ص ص 82-83.
[70] معجم الحاسبات ، الطبعة الموسعة ، مجمع اللغة العربية ، مصر ، 1995.
[71] **غيطاس جمال محمد** ، "عصر المعلومات : القادم مذهل أكثر" ، مركز الخبرات المهنية ، مصر 2007.
[72] **العبود فهد بن ناصر** ، "الحكومة الالكترونية بين التخطيط و التنفيذ" ، السلسلة الثانية ، مكتبة الملك فهد الوطنية ، الرياض ، 2005 ، ص 152.

- **من زاوية تقنية (عملية)** : فهو مجموعة الوسائل و التدابير و الاجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من البيئة الداخلية أو الخارجية.[73]

- **من زاوية قانونية** : أمن المعلومات هو محل دراسات و تدابير حماية سرية و سلامة المحتوى و توفر المعلومات و مكافحة أنشطة الاعتداء عليها و استغلال نظمها في ارتكاب الجريمة.[74]

و على ضوء التعريفات السابقة يمكن القول أن أمن المعلومات هو كل السياسات و الإجراءات المطبقة بهدف حماية المعلومات عن طريق توفير الأمن لكل المكونات المادية من محلات و أجهزة و المكونات التقنية كالبرمجيات و الشبكات و الإتصالات و كل التكنولوجيات المستعملة في تداول المعلومات ، دون نسيان أهم عنصر و هو العنصر البشري الذي كلما زادت حمايته تطور تعامله مع المعلومات لأن التقنية مهما بلغت مستوياتها لا يمكن أن تحل محل العنصر البشري.

الفرع الثاني : مصطلحات مشابهة لأمن المعلومات

هناك لبس شديد بين مصطلحات الأمن الجديدة ، مما يعرقل عملية الدراسة الجيدة للموضوع و الإلمام به ، ما يدفعنا إلى توضيح هذا اللبس منذ بداية البحث ، و الاتفاق على المصطلح المستعمل.

- **أمن نظم المعلومات**

- عرفه المكتب الوطني الأسترالي للتدقيق بأنه " حماية أنظمة المعلومات بما تشمله من البنى التحتية التي تسهل استخداماتها كالتقنيات و العمليات و الخدمات و المعلومات ".[75]

- كما يقصد بأمن نظم المعلومات " كل السياسات و الإجراءات و الأدوات التقنية التي تستخدم لحماية النظام من كل أشكال الاستخدام غير الشرعي للموارد مثل : السرقة ، التغيير و التعديل ، إلحاق الضرر بالمعلومات أو قواعد البيانات ، أو إلحاق الضرر المادي المتعمد بالأجهزة ، بالإضافة إلى وجود تهديدات أخرى مثل الاخطاء الإنسانية و الحوادث الطبيعية و الكوارث " .[76]

---

[73] **علاء محمد حسونة عابد** ، بيان سعيد عبد الكريم وهبة ، السياسات الإدارية لأمن المعلومات. أنظر http://www.cst.ps/ar/?404;http://www.cst.ps:80/mfarra/ISM/Ola&Bayan.ppt

[74] **عبد الله بن شانع بيهان** ، "ثقافة أمن المعلومات "، الملتقى الدولي الثالث لأمن المعلومات و الاتصالات ، سوريا ، 2007

[75] Australian National Audit OfficeIT Security Management Audit Report No.23 2005-2006, www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf

[76] **سعد غالب ياسين** ، "تحليل و تصميم نظم المعلومات "، دار المناهج للنشر ،عمان ،الأردن ، الطبعة الأولى ، 2000 ، ص 349.

يكثر القول أن هناك خلافا بين أمن المعلومات و أمن نظم المعلومات باعتبار أن الأول هو حماية للمعلومات دون ذكر لنظام المعلومات بما يشمله من تقنيات و استراتيجيات ، و الثاني هو عبارة عن حماية للموارد التقنية و ما تحتويه من معلومات ، و لكن كيف يمكن حماية هذه المعلومات دون توفير حماية للأنظمة فالمعلومات هي موجودة داخل الأنظمة.

كما أنه من خلال التمعن في تعاريف أمن المعلومات و تعاريف أمن نظم المعلومات نجد نفس التعريف بالضبط فحماية المعلومات لا يمكن أن تتحقق دون توفير حماية لنظم المعلومات ، و عليه سنقوم باستخدام مصطلح أمن المعلومات في بقية بحثنا مفترضين أن أمن المعلومات و أمن نظم المعلومات هما مصطلحين لمفهوم واحد.

- **الأمن الالكتروني و أمن المعلومات**

نتيجة الاستخدام المكثف لتكنولوجيا المعلومات و الاتصال في المؤسسة و في الحياة العامة ، أصبحت عدة أجهزة مرتبطة بالحاسوب و لواحقه ، فتطور مفهوم أمن المعلومات إلى الأمن المعلوماتي فالأمن الالكتروني ، و هو ذلك الفرع من علم الالكترونية و التكنولوجيا الدقيقة الذي يهدف إلى توفير السرية و الأمان لكافة الأجهزة الالكترونية المرتبطة بالوحدات الحاسوبية.

- و يعبر عن الأمن الالكتروني بأنه " مجموعة الإجراءات الوقائية المتخذة لحماية المعلومات من السرقة أو الضياع أو التلف ، و وضعها في شكل آمن لحمايتها من أي اعتداء عليها ".[77]

و بالتالي هو عبارة عن تطبيق لأمن المعلومات في وسائل الحوسبة و الاتصال ، فالأمن الالكتروني إذن هو مصطلح يطلق على أمن مختلف الأجهزة الالكترونية.

و إن سلمنا بالاستخدام المكثف لتكنولوجيا المعلومات و الاتصال ، و طغيان الاستخدام لوسائل التقنية و الالكترونية في مجال معالجة و نقل البيانات ، لا يمكن أبدا و لا بأي حال من الأحوال تجاهل أنظمة المعلومات التقليدية التي مازالت العديد من المؤسسات تعتمد عليها و لو بشكل بسيط ، فمن خلال بحثنا هذا نحاول معالجة موضوع أمن المعلومات أينما كانت ، سواء في الأنظمة التقليدية أو الالكترونية ، و لكن طبعا سيكون التركيز

[77] **ايمان السمرائي ، هيثم الزعبي ،"** نظم المعلومات الادارية" ، دار الصفاء للنشر و التوزيع ، عمان ،الأردن ،الطبعة الاولى،2004،ص28.

الأكبر على حماية المعلومات في الأنظمة المحوسبة و عليه فان الأمن الالكتروني أو الأمن المعلوماتي ما هو إلا جزء من أمن المعلومات و لكنه الجزء الأكبر في الوقت الحالي.

الفرع الثالث : مراحل تطور مفهوم أمن المعلومات

- **مرحلة الستينات "60"**

مر مفهوم أمن المعلومات بمراحل تطور متلاحقة ، ففي "60" كانت أجهزة الحاسوب و عملها هي شغل العاملين في أقسام المعلومات ، و كان همهم هو كيفية تنفيذ البرامج و الأنشطة المحوسبة ، و لم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة ، و كان مفهوم الأمن يدور حول تحديد الوصول أو الاطلاع على البيانات من خلال منع كل غريب من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحاسوب و الذي يعني حماية الحاسوب و قواعد البيانات.[78]

- **مرحلة السبعينات "70"**

و نتيجة للتوسع في استخدام أجهزة الحاسوب و ما تؤديه من منافع تتعلق باتساع أحجام معالجة البيانات تغير الاهتمام ليمثل السيطرة على البيانات و حمايتها ، و في"70" تم الانتقال إلى مفهوم أمن البيانات ، و رافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات ، إضافة إلى وضع اجراءات الحماية لمواقع الحواسيب من الكوارث ، و اعتماد خطط لتخزين نسخ إضافية من البيانات و البرمجيات بعيدا عن موقع الحاسوب .

- **مرحلة الثمانينات و التسعينات"80" و "90"**

و في مرحلة "80" و "90" ازدادت أهمية استخدام البيانات ، و ساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات ، كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات ، و أصبح من الضروري المحافظة على المعلومات و تكاملها و توفرها و درجة موثوقيتها ، حيث أن الاجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة و تقلص اختراق نظم المعلومات و التلاعب بها .

[78] **Pierce ,c**, "collected papers of Charles Sanders Pierce", MA : Harvard University Press ,1958.

المطلب الثاني : عناصر أمن المعلومات و خصائصها

من خلال هذا المطلب سيتم التطرق أولا لعناصر أمن المعلومات و المتمثلة في السرية ، السلامة و التوفر ، و ثانيا ذكر أهم خصائص أمن المعلومات.

الفرع الأول : عناصر أمن المعلومات

إن المنظمات التي تسعى لتحقيق أمن نظم المعلومات إنما غايتها تحقيق الثالوث المسمى (CIA triangle) و يعني السرية (Confidentiality) ، التكاملية و السلامة (Integrity)، و التوفر و الإتاحة (Availability).[79]

أولا : السرية (Confidentiality)

تعني ضمان حفظ المعلومات المخزنة أو المنقولة ، و عدم الإطلاع عليها أو استخدامها إلا بموجب إذن ، حيث أن النظام الآمن هو الذي يضمن سرية و خصوصية البيانات المخزنة فيه ، فلا يسمح بكشفها بدون ترخيص ، أو الإطلاع عليها من قبل أشخاص غير مخول لهم بالإطلاع على تلك البيانات ، و بالتالي اتاحتها فقط لأصحابها ، إضافة إلى تأمين الطرق المناسبة لحمايتها من القراءة أثناء نقلها عبر شبكة الاتصال و السرعة في نقلها ، و تحديد حدود وصلاحية الاستخدام سواء كان كلي أو جزئي ، مع تحديد من له صلاحية التعديل أو الإدخال أو الحذف أو الإضافة او القراءة .

و من المهم جدا وضع شروط معالجة البيانات بطريقة آمنة تحميها من الكشف غير المرخص في اتفاقيات الشراكة و التعاون بين المنظمات لحماية المعلومات المتبادلة .

ثانيا : التكاملية و السلامة (Integrity)

هي بصفة عامة ضمان سلامة محتوى المعلومات ، و التأكد أن هذه المعلومات لم تتعرض لأي عملية حذف أو تخريب أو اتلاف كلي أو جزئي سواء بصفة متعمدة أو غير متعمدة في أي مرحلة من مراحل المعالجة او التبادل و إلا يكون قد تم ضياع تكامل المعلومات.

[79] **Whitson , G** , "Computer Security : theory, process and management", the journal of computing in small colleges, vol.18, no.6, 2003, p 57.

و يتكون عنصر سلامة المعلومة من شقين:[80]

- **سلامة المعلومة** : بمعنى عدم تغييرها بشكل غير ملائم سواء بقصد أو بدون قصد ، و أنها أدخلت بشكل صحيح يعكس الظروف الحقيقية للمعلومة.
- **سلامة المصدر** : و يقصد بها الحصول على المعلومة من مصدرها الأصلي.

و تشير سلامة المعلومات بصفة عامة إلى الإجراءات التي تضمن حفظ المعلومات خلال مراحل إدخالها أو نقلها بين الأجهزة و الشبكات للمحافظة على سريتها و سلامتها.

ثالثا : التوفر و الإتاحة (Availability)

و نعني به تمكين المستخدم (إنسان أو نظام حاسوب) الذي له حق التعامل مع المعلومات من ذلك بدون التدخل أو الإعاقة في أداء تلك المهمة ، و وصول المعلومات في الشكل المطلوب ، و لهذا العنصر مجموعة خصائص متمثلة في:[81]

- **المقاومة** : و هي قدرة النظام الحفاظ على نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه.
- **سهولة الاستخدام**.
- **المرونة** : و المتمثلة في توفر الامكانيات و الأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك توقفه.
- **المقدرة على التوسع** لسد الحاجيات المستقبلية.

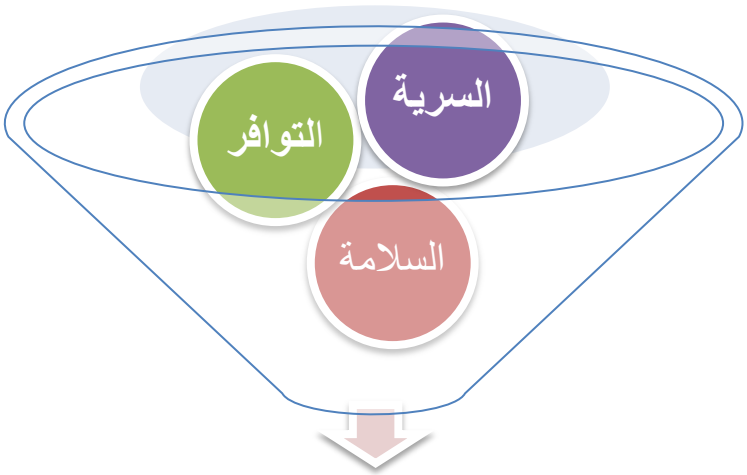
و حتى يستمر تطبيق ما بالتوفر يجب أن تكون جميع مكونات النظام متوفرة أيضا بحيث تتضمن التطبيق و قاعدة البيانات ، و الخادم ، و أجهزة التخزين و سلامة الشبكة من البداية إلى النهاية.[82]

[80] **أبو مغايض ، يحيى بن محمد** ،"الحكومة الإلكترونية : ثورة على العمل الإداري التقليدي "، مكتبة العبيكان ، الرياض ، 2004، ص 271

[81] جامعة الدول العربية ، المركز العربي للبحوث القانونية ، الإجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات ، المنعقد في 5-2012/03/7 ، بيروت لبنان. أنظر :.http://carjj.org/node/1242

[82] See: Cisco Systems , inc : Indiana , Cisco press , Cisco networking academy program; First year companion guide 2nd ed , 2001 , p12.

الشكل (1.5): عناصر أمن المعلومات



المصدر : من إعداد الباحثة

و يمكن القول أن الأبعاد الأساسية الثلاثة لإدارة أمن المعلومات (السرية ، السلامة و التوفر) لابد من توفرها في كل نظام ، و لكن قد يغلب أحدها على الآخر حسب طبيعة المعلومات و المنظمة و الظروف المحيطة بها ، و الأهم من ذلك كله التوازن بين المنع و الاستخدام ، و من المعروف أن اتخاذ قرار المنع الكلي سهل جدا و لكنه غير مناسب و غير مفيد.

الفرع الثاني : خصائص أمن المعلومات

يرى خبراء أمن المعلومات في المؤسسة الوطنية للمقاييس و التكنولوجيا أن :[83]

- أمن المعلومات يجب أن يحقق رؤية و أهداف المؤسسة.
- أمن المعلومات هو جزء أساسي من عمليات الإدارة الناجحة.
- أمن المعلومات يجب أن ينفذ برؤية اقتصادية فعالة.
- دراسة أنظمة أمن المعلومات شاملة و متكاملة.
- مسؤولية المعنيين بأنظمة المعلومات هي داخل و خارج المؤسسة.
- تحقيق أمن المعلومات يتطلب دراسة واعية لإدارة المخاطر.

[83] NIST : National Institue of Standard and Technology ;Risk Management Guide for Information Technology Systems , u.s ; department of commerce publication ; n:800-30 , 2002.

- أمن المعلومات يتأثر بالعوامل الاجتماعية.
- تتطلب برامج أمن نظم المعلومات إعادة تقييم دورية.

أيضا يمكن استخلاص خصائص أخرى من التعاريف المذكورة آنفا:

- إجراءات الأمن هي إجراءات إدارية و فنية.
- أمن المعلومات يتسم بوجود شرعية على حدود و صلاحيات استخدام المعلومات و الأجهزة.
- ينطوي الأمن على الحماية ضد الاختراقات و التجسس و السرقة و التبديل و التلف المتعمد أو الاطلاع بغير تخويل.
- هدف أمن المعلومات المحافظة على مكونات نظام المعلومات المادية و غير المادية.

المطلب الثالث : أهمية أمن المعلومات و أهم أهدافها

إن أهمية أمن المعلومات تتضح في المؤسسات المتطورة التي تعتمد على التكنولوجيات الجديدة أكثر منها في المؤسسات العادية أو الأقل تطورا ، و تبرز في جميع المستويات انطلاقا من طبقة المستعملين إلى غاية أجهزة الخادم و الحواسب المركزية ، و الوعي الجيد بهذه الأهمية من قبل أصحاب الادارة العليا و المستخدمين و أصحاب المعرفة و كل عمال المؤسسة حتما سيؤدي إلى تحقيق الأهداف المرجوة.

الفرع الأول : أهمية أمن المعلومات

استعمال أنظمة المعلومات يوفر الكثير من الفرص المباشرة و غير المباشرة ، و لكن يقدم بالمقابل الكثير من المخاطر المباشرة و غير المباشرة ، هذه المخاطر تترجم بالفجوة بين الحاجة لحماية الأنظمة و درجة الحماية المطبقة،و من هنا جاءت الحاجة لإيجاد نظام أمني يقوم بتوفير البيئة المناسبة للتعامل مع المعلومات، و من الأسباب التي زادت من أهمية أمن المعلومات ما يلي:[84]

- الحاجة للارتباط بنظم الاتصالات و الانترنت، و عدم امكانية عزل الأجهزة عن الشبكات المحلية و الشبكات واسعة النطاق لتوفير المعلومات لمن يحتاجها.
- اعتماد مختلف المنظمات على فعالية المعلومات.

[84] **القاسم محمد بن عبد الله** ، "سياسات أمن المعلومات" ، سلسلة اصدارات مركز البحوث و الدراسات ، مكتبة الملك فهد الأمنية ، الرياض ، 2005 ، ص ص 34-35.

– صعوبة تحديد المخاطر و التحكم بها ، أو متابعة المجرمين و معاقبتهم لعدم توافر حدود جغرافية عند استخدام الانترنت و الاتصالات الالكترونية لأنها تتيح الفرصة لاختراق الحدود المكانية.

– النمو المضطرد في الاستخدامات و التطبيقات الالكترونية و ظهور التجارة الالكترونية و الحكومة الالكترونية و الادارة الالكترونية التي تحتاج إلى بيئة معلوماتية آمنة.

إضافة إلى:

– الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية و ذلك من أجل استمرارية الأعمال التجارية.

– المؤسسات تعتمد على المعلومة الدقيقة ، الكاملة ، الصالحة ، المنطقية ، الملائمة والموثوقة ، و بالتالي الادارة مسؤولة عن ضمان و تأمين المؤسسة توفر لكل المستعملين محيط آمن لأنظمتهم المعلومات.

– قلة الأمن ، مثلا الافشاء غير المصرح به للمعلومات التنافسية أو الحساسة ، يمكن أن تؤدي بالمقابل إلى خسائر مالية أو خسائر غير ملموسة.

و عليه كل هذه الحاجات المذكورة و التطورات الطارئة على طرق تطبيق الاعمال زادت من أهمية أمن المعلومات و جعلت منه ضرورة يجب الالتفات إليها.

الفرع الثاني : أهداف أمن المعلومات

معايير الأمن يجب أن تكون متناسبة مع قيمة المعلومة الواجب حمايتها ، و تهدف هذه المعايير إلى:

- **ضمان سلامة المعلومة**

تقليص مخاطر ضياع و تشويه و تدمير المعطيات هو واحد من أهم الأهداف، و من أجل تحقيق هذا الهدف، يجب **أولا** العمل على وضع برنامج يضمن حماية معطيات نظام المعلومات، يتم اختباره و مراجعته بانتظام بالتنسيق و بمساعدة مستعملي نظام المعلومات بالمؤسسة، **ثانيا** يجب تزويد حامل المعلومة بالاستقرار و الاستمرار المطلوب.

و عليه فان سلامة المعلومة يعني حمايتها من كل تشويه أو تدمير أو ضياع بطريقة ما.

- **ضمان سرية المعطيات ذات الطابع الشخصي**

المؤسسة عليها تفعيل كل الإجراءات الضرورية من أجل ضمان خصوصية و سرية المعلومات الخاصة ، و الحد من تسريب المعلومة إلا للأشخاص المخولين و المصرح لهم ، هاته الإجراءات ليست فقط تقنية ، بل لكي تكون فعالة فهي تتطلب تكييف اجراءات عملية و مشاركة ذوي الخبرة في هذا المجال.

- **تثبيت المسؤوليات**

فمن أجل ضمان جودة المعلومة ، يجب أن يكون هناك قدرة على تثبيت المسؤوليات في حالة تشويه المعطيات،[85] و التصرف ضد أي شخص يرفض تحمل مسؤوليته في ما يتعلق بوثيقة أو أي غرض آخر.[86]

- **ضمان استمرارية المصالح في حالة خطأ فادح في الاعلام الآلي**

تأسيس برنامج استمرارية النشاط من أجل ضمان أنه في أي حال من الأحوال الأنشطة الحيوية للمؤسسة لن تتوقف ، و في حال توقف نظام المعلومات ، هذا البرنامج يحتاط بإجراءات مموهة و التي تكون متابعة من طرف المستعملين. هناك حالات بينت أن أي توقف يمكن تداركه إن لم يُسيَّر بصفة صحيحة فسيؤدي ذلك إلى ضياع فرص و نشاطات المؤسسة ، و هناك أمثلة عديدة عن مؤسسات توقف فيها عمل أنظمة المعلومات لعدة أيام بسبب انقطاع التيار الكهربائي أو التعرض لفيروس خطير ، لذا يجب الاحتياط قبل وقوع الكارثة.[87]

[85] Introduction à la sécurité des systèmes d'information , guide pour les directeurs d'établissement de santé , direction générale de l'offre de soins , novembre 2013 , p 13.
[86] Directive sur la sécurité de l'information gouvernementale , loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement , chapitre G-1.03,a.20 , Décret 7-2014 du janvier 2014 , conseil du trésor Québec , 23.01.2014 , p 3.
[87] Introduction à la sécurité des systèmes d'information , op.cit , p13.

المطلب الرابع : مبادئ أمن المعلومات

هدف الأمن مدعوم بالعديد من المبادئ نذكر منها:

الفرع الأول: المسؤولية

أمن المعلومات يتطلب الإسناد الواضح و الصريح للمسؤوليات في كل مستويات المؤسسة ، من أصحاب المعطيات ، أصحاب العمليات ، موردي الحلول التقنية و المستعملين ، و التعريف بالمستعملين الذين يستعملون النظام بصفة استثنائية.

الفرع الثاني : التحسيس

التحسيس بالمخاطر و المبادرات في مادة الأمن يجب أن تكون منتشرة ، كما يجب على المؤسسة احترام كل النقاط التالية في مبدأ التحسيس:[88]

- من أجل تأسيس ثقة في المعلومات على مالكي المعطيات ، مالكي العمليات ، موردي الحلول التكنولوجية ، المستعملين ، و الأطراف الأخرى التي لها مصلحة قانونية في المعرفة أن تكون لهم دراية بوجود مخاطر ، و بدرجة المخاطر التي تتعرض لها المنظمة و أنظمتها.
- مستوى التفاصيل المباحة لا يجب أن يعرض الأمن للخطر.
- المعرفة المناسبة تكون في متناول كل الاطراف التي لها الحق الشرعي في الإعلام و ليس فقط المستعملين.
- التحسيس يمثل جزء من برنامج استقبال العمال الجدد بالمؤسسة ، من أجل جعل التحسيس بالأمن كجزء أساسي في ثقافة المؤسسة.
- الأخذ بعين الاعتبار أن التحسيس هو عملية مستمرة.

و بالتالي معايير الأمن لا تكون كفئة و فعالة إلا بشرط أن يكون كل من له علاقة بهذه المعايير تم تحسيسه بطريقة عملها الصحيحة ، ة بالمخاطر التي تسمح بالإجابة عنها.

[88] **Susan.M.Caldwell** et autres, op.cit , p 14.

الفرع الثالث : الأخلاق و العوامل الاجتماعية

عملية تسيير أمن المعلومات يجب أن تكون بطريقة أخلاقية تهدف إلى ضمان انتظام القيادات و المسؤوليات الفردية ، فالمعلومة و أمنها يجب أن تعطى و تُستعمل في إطار احترام حقوق و مصالح الآخر ، و بمستوى أمن متناسق مع استعمال المعلومة.

الفرع الرابع : العالمية

التجارب و الحلول في مجال أمن المعلومة يجب أن تتوافق إلى أبعد حد ممكن مع طرق العمل المتعارف عليها ، و عموما المستعملة على المستوى العالمي و المحلي.[89] كما يجب أن تكون إجراءات الأمن متناسقة مع بعضها البعض و مع المعايير و التجارب العالمية في كل مستويات دوران المعلومة.

الفرع الخامس : إعادة التقييم و السرعة في رد الفعل

التجارب و الحلول في مجال أمن المعلومة يجب أن يعاد تقييمها دوريا من أجل الأخذ بالحسبان التغيرات القانونية ، التنظيمية ، التكنولوجية ، المادية ، المحيطية ، و كذلك تطور التهديدات و المخاطر.[90] إذ على المؤسسات أن تضع إجراءات مراقبة و ردود أفعال للانتهاكات الحقيقية أو مجرد محاولة انتهاك الأمن في الآجال المناسبة ، فالطابع الفوري و الخسائر الكامنة التي يمكن أن تنتج بسرعة تتطلب من المنظمات أن تستجيب بسرعة.

كما على المؤسسات وضع مخطط عمل في هذا المجال يتضمن الخطوات التالية:[91]

- التحديث الدوري لمخططات الاستمرارية باعتبار المؤسسة في اعتماد متزايد على أنظمة المعلومات.
- مواكبة التغييرات التي تتعرض لها أنظمة المعلومات و البنى التحتية الخاصة بها.
- وضع حلول و عروض جيدة تتماشى مع الأشكال الجديدة للتهديدات على انظمة المعلومات.
- الأخذ بعين الاعتبار كل تكنولوجيات الأمن البارزة التي تمد حلول و عروض بتكلفة أحسن من قبل.
- تغيير مستوى الأمن الحالي بتغير التشريعات و النشاطات و البنى التنظيمية.
- توقع تصاعد الانتهاكات على مستوى اتخاذ القرار.

[89] Directive sur la sécurité de l'information gouvernementale , op.cit , p 4.
[90] Ibid , p 4.
[91] **Susan.M.Caldwell** et autres, op.cit , p14.

عليه يجب القول أن الأمن و أنظمة المعلومات يجب إعادة تقييمها دوريا و القيام بالمتابعة من أجل أن يكون رد الفعل ضد المخاطر في الوقت المناسب ، لأن أنظمة المعلومات و احتياجاتها الأمنية تتطور مع الوقت.

الفرع السادس : المردودية

إن أمن المعلومات يجب ان يكون لديه مردودية على نشاط المؤسسة فقد اشارت العديد من الدراسات بالأهمية الاقتصادية لتطبيق أمن المعلومات في المؤسسات باختلافها ، و لكن مستويات الأمن يجب أن تكون لها علاقة بقيمة المعلومة ، و يمكن تلخيص هذا المبدأ في النقاط التالية:

- تتحدد قيمة المؤسسة بطبيعة الممتلكات المعلوماتية الخاصة التي بحوزتها.
- قيمة المعلومات و المعطيات تتحدد بدرجة و مستوى حساسيتها.
- تقاس التهديدات حسب خطورتها و حسب احتمال وقوعها.
- العروض المقدمة و المتاحة من أجل تخفيض أو إلغاء التهديدات تُقيَّم بمستوى تكاليف هذه العروض إضافة إلى التكاليف الهامشية لمستوى الأمن.
- يتم تقييم عروض الأمن بوضع مقارنة بين الخسائر التي تتكبدها المؤسسة عند انتهاك أمنها و بين تكاليف وضع سياسة أمنية ، بمعنى من أجل تحقيق مردودية على المؤسسة أن توازن بين التكاليف و المخاطر.

هذا من الناحية النظرية أما من الناحية التطبيقية فيمكن حساب العائد على الاستثمار في الأمن و الذي يعرف أنه " المنافع التي تحققها المؤسسة نتيجة للإنفاق على الأفعال المتعلقة بأمن نظم المعلومات ، بمعنى أي من الخيارات سوف يمنح المؤسسة القيمة الأفضل مقابل ما سأدفعه من مال."[92]

و يمكن حساب العائد على الاستثمار في الامن (ROSI) بالطريقة التالية:[93]

$$\text{العائد على الاستثمار في الأمن} = \frac{(\text{نسبة التعرض للخطر} \times \text{نسبة الخطر}) - \text{تكلفة الأمن}}{\text{تكلفة الأمن}}$$

(نسبة التعرض للخطر ×نسبة الخطر) = العائد المتوقع من الأمن

[92] **Sonnenreich, W. ,Albanese, j** ," Return on Security Investment (ROSI): A Practical Quantitative Model", Journal of Research and Practice in Information Technology, vol. 38, no.1.2005

[93] Ibid , p 46.

و باعتبار أن تكلفة الحماية عالية جداً ، فللإدارة العليا صاحبة القرار الخيار إما بحماية أنظمتها و معلوماتها من خلال الموازنة بين التكلفة و درجة المخاطر ، أو تحمّل المخاطر إذا ما رأت في ذلك مصلحة ، فلا يمكن أبدا حماية ما قيمته بسيطة بتكلفة حماية باهظة تفوق قيمته بكثير.

و عليه فان أمن المعلومات مصطلح معقد و يضم تحت طياته عدة مصطلحات و مفاهيم أخرى كأمن نظم المعلومات ، الأمن الالكتروني ، الأمن المعلوماتي ، الأمن السيبراني...و لكن يبقى أمن المعلومات هو المصطلح الأشمل ، عناصره الأساسية هي السرية ، التوافر و الاتاحة.

خلاصة الفصل

من خلال الفصل الأول تم التطرق على مجموعة من المصطلحات ذات الصلة بموضوع بحثنا ، و تمثلت هذه المصطلحات أساسا في : الأمن الاقتصادي ، الذكاء الاقتصادي ، المعلومات ، أنظمة المعلومات ، أمن المعلومات، أمن أنظمة المعلومات ، الأمن الالكتروني و الأمن المعلوماتي ،كما تم أيضا توضيح اللبس الحاصل بين هذه المصطلحات الجديدة ، مما ساعدنا على تكوين خلفية نظرية حول الموضوع و الخروج ببعض الاستنتاجات :

- الأمن الاقتصادي هو مفهوم عام يمكن تطبيقه على مستوى الدولة أو المؤسسة.
- الأمن الاقتصادي هو عنصر من عناصر الذكاء الاقتصادي حيث يمثل الجانب الدفاعي من الذكاء.
- نتيجة تطور المجتمعات ، و ظهور التقنيات الجديدة ، و اكتساب العصر مسمى جديد و هو عصر المعلومات، أكسب هذه الأخيرة و الأنظمة التي تعمل من خلالها أهمية كبيرة ، فأصبح التحكم الجيد في المعلومات هو أساس التطور و مفتاح النجاح .
- إن ظهور التكنولوجيات الجديدة ، أدى بالمقابل إلى ظهور مخاطر و تهديدات جديدة ، جعلت من المؤسسات و المختصين في هذا المجال أمام ضرورة إيجاد حلول فورية من أجل مواجهة التهديدات و توفير حماية فعالة للمعلومات ، هذا ما أدى إلى ظهور مفهوم جديد و هو أمن المعلومات.
- أمن المعلومات هو عبارة عن مجموعة من السياسات و الإجراءات التي تعمل على توفير الأمن و الحماية لكل ممتلكات المؤسسة من معلومات و أجهزة و تقنيات و برامج من أي تخريب أو تشويه أو سرقة أو إطلاع بغير تصريح سواء كان بطريقة متعمدة أو عن طريق الخطأ ، في ظل ضمان سرية و سلامة و توافر المعلومة.
- اكتسب أمن المعلومات في العصر الجديدة أهمية كبرى لا يمكن تجاهلها.

بعد التعرض في الجانب النظري لمفاهيم أمن المعلومات، سنتناول في الفصل الثاني كيفية تطبيق أمن المعلومات داخل المؤسسة ، و معرفة الخطوات المتبعة لضمان نجاحه ، و التطرق لأهم و أشهر التهديدات التي تتعرض لها نظم المعلومات و وسائل حمايتها.

الفصل الثاني : تهديدات أمن المعلومات و سبل التصدي لها

المبحث الأول : تهديدات أمن المعلومات

المطلب الأول : ماهية التهديدات

المطلب الثاني : أنواع القراصنة المعلوماتية و دوافعهم

المطلب الثالث : أنواع التهديدات على المعلومات و نظمها

المبحث الثاني : وسائل تحقيق أمن المعلومات

المطلب الأول : الحماية البرمجية للمعلومات و أنظمة المعلومات

المطلب الثاني : الحماية المادية لممتلكات المؤسسة المادية (الأمن المادي)

المطلب الثالث : الحماية القانونية للممتلكات غير المادية (حقوق الملكية الفكرية)

تمهيد

الحديث عن أمن المعلومات خصوصا الأمن المعلوماتي يقود مباشرة إلى التفكير في قراصنة الانترنت ! بالتأكيد عدم الأمان يتولد بفعل التفاعل مع الانترنت ، و لكن بالأساس الإجرام لم يتولد مع المعلوماتية ، و لكن معلوماتية أو شبكة دون رقابة تضاعف المشكل ، و البحث عن الأمن لا يقتصر فقط في مقاومة الإجرام ، بل هناك أمور أخرى كثيرة ، إذ في ما يفيد عرض آخر صيحة لجدار حماية إذا كان في اليوم الموالي مؤسستك ستكون ضحية لكارثة معلوماتية بسبب عطل تافه في القرص الصلب أو عدم تحديث الحماية ؟ ف **ثلث** المؤسسات لا تختبر حمايتها ، من بين تلك التي تفعل 77 % منها تجد أخطاء.[1]

لذا فإن مسألة أمن المعلومات مسألة عميقة و ليست بالبساطة التي تظهر عليها ، طبعا لا يمكن الانكار أن أحدث البرامج و الطرق المعلوماتية في مجال الأمن هي أمر في غاية الأهمية لحماية أنظمة معلومات المؤسسة ، لكن لا يكفي ! فاستحضار أحدث البرامج و وضعها في أيدي غير كفئة أو تسييرها بطريقة خاطئة لن يجدي نفعا ، لذا الاهتمام بالجانب التنظيمي و العامل البشري أهم بكثير ،و هذا ما يهم خلال هذا البحث الذي يجب التأكيد أنه بحث أكاديمي تسييري ، و ليس معلوماتي ، و عليه تم تقسيم هذا الفصل الثاني من البحث إلى مبحثين مهمين:

- **المبحث الأول** الذي سيتم من خلاله دراسة تهديدات الأمن المعلوماتي من خلال ثلاث مطالب تعطينا نظرة واضحة حول طبيعة هذه التهديدات و مصادرها ، و دوافع مرتكبيها و مختلف طرق تنفيذها.
- **المبحث الثاني** الذي سيقسم بدوره إلى ثلاث مطالب تشرح مختلف أنواع الحماية الممكنة للحفاظ على سير المؤسسة ، من حماية برمجية إلى حماية مادية و حماية قانونية ، أما الجانب التنظيمي فلأهميته و طول شرحه سنقوم بدراسته في فصل كامل لاحقا.

[1] **André Vaucamps**, CISCO : « Sécurité des routeurs et contrôles du trafic réseau », éditions ENI , 2010, p9

المبحث الأول : تهديدات أمن المعلومات (تهديدات نظم المعلومات)

في عالم أصبح معقد و يمتاز بعدم التأكد ، أصبح من الصعب على المؤسسات تسيير التهديدات التي أصبحت عديدة و معقدة ، و بنظرة عامة و سطحية نرى أن طبيعة التهديدات في عالم المعلوماتية لا تختلف عن طبيعة التهديدات في العالم الحقيقي ، و الاختلاف يكون فقط في خصائص العالم الالكتروني و طرق اطلاق الهجمات ، لكن الأمر أكثر تعقيدا ، ففي مجال المعلوماتية تعريف و تحديد أصل التهديد هو أمر في غاية الصعوبة، أين الحدود الجغرافية لا معنى لها ، و توجيه الهجمة يمكن أن يكون عن بعد ، من أبعد نقطة متوقعة ، كما يمكن أن يكون على بعد أمتار منك ، دون الانتباه لها ، لذا سنعالج الموضوع و نحلله من خلال هذا المبحث و الذي تم تقسيمه إلى ثلاث عناوين رئيسية :

المطلب الأول :سنعرف التهديدات و نبين مصادرها الطبيعية و البشرية ، المطلب الثاني : سنحاول معرفة أنواع المهاجمين في هذا المجال و فهم دوافعهم لارتكاب الجرائم ، و أخيرا و أهم نقطة سنفصل بكل أنواع التهديدات التي يمكن أن تتعرض لها المؤسسة سواء من اعتداءات أو ثغرات على مستوى أنظمتها ، فمعرفة التهديدات المحتملة هو نصف الطريق نحو الأمن.

المطلب الأول : ماهية التهديدات

تهديدات أمن المعلومات أو تهديدات نظم المعلومات هو مصطلح حديث نوعا ما ظهر بظهور الاعلام الآلي و الحواسيب ، و انتشر بتوسع استخدامها و تطور خدماتها ، فكلما زادت فوائد هذه الأنظمة و زاد الاعتماد عليها ، زادت التهديدات عليها.

الفرع الأول : مفهوم تهديدات نظم المعلومات

يعرف التهديد بصفة عامة على أنه : " هدف عدائي يحمل تحت تصرفه وسائل حقيقية من أجل تعريض مؤسسة، أشخاص ، مواقع للخطر "[2].

كما يمكن أن يعرف كنشاط أو حدث يمكن أن يحمل خسائر على ما نرغب في حمايته[3].

[2] **Eric Delbecque , Jean-Renaud Fayol** , « Intelligence économique », ED Vuibert , paris 2012 , p 89.
[3] **Didier Godart** , « sécurité informatique : risques , stratégies et solutions » , 2éme édition , éditions des CCI de wallonie s.a , Belgique ,2005 , p 51.

أما في مجال الاعلام الآلي ، فالتهديد إذن يمكن أن يعرف كنشاط أو حدث و الذي بمجرد إطلاقه يمكن أن يحدث إصابات على أحد أو كل الخصائص الحرجة للمعلومة و الأنظمة التي تحملها و تحفظها و هي السرية، التكامل و الإتاحة (التوافر).[4]

و يعرف أيضا على أنه حدث أو جهة تشوش نظام المعلومات عن طريق استغلال ثغرة من أجل الحصول، تعديل أو إعاقة الوصول لأصل من الأصول أو تعريضه للخطر ، و يتلخص في الأخطاء الإرادية و غير الإرادية، الاحتيال، النشاطات المحتملة من العمال الخبيثين ، الحوادث و الأسباب الطبيعية ، الهاكر ، البرامج الخبيثة.[5]

و عليه تستنتج الباحثة أن التهديد هو أي خطر محتمل للمعلومات أو الأنظمة التي تحويها سواء كان هذا الخطر متعمد أو غير متعمد، أو بصفة أخرى هو كل تصرف يمكن أن يؤثر سلبا على سرية ، تكامل و توافر المعلومات.

الفرع الثاني : مصادر التهديدات

مصادر التهديد مختلفة و متنوعة منها الطبيعية ، و البشرية. و من خلال هذا البحث سنقوم بشرح بسيط لمصادر التهديد الطبيعية مع التركيز على التهديدات البشرية خلال البحث.

أولا : التهديدات الطبيعية

و هي كل التهديدات الخارجة عن الإرادة و ليست بفعل عوامل بشرية منها:

أ- **الكوارث الطبيعية** : فالكارثة هي " حادثة محددة زمنيا و مكانيا ينجم عنها تعرض مجتمع بأكمله أو جزء من مجتمع إلى أخطار شديدة مادية ، و خسائر في أفراده تؤثر على البناء الاجتماعي بإرباك حياته و توقف توفير المستلزمات الضرورية لاستمرارها ."[6]

و من بين الكوارث الطبيعية التي تؤثر على أنظمة المعلومات : الزلازل و الأعاصير و الفيضانات و النيران ، إضافة إلى درجة الحرارة العالية و الرطوبة العالية التي تحدث و تلحق الضرر بالحاسوب و الأجهزة الالكترونية.

[4] **Didier Godart** , op.cit ,p 51.

[5] **Jean –François Carpentier**, « la sécurité informatique dans la petite entreprise » ,ED ENI, France,2009 ,p23,p31.

[6] **الشعلان فهد أحمد** ، "إدارة الأزمات : الأسس –المراحل – الآليات" ، جامعة نايف العربية للعلوم الأمنية الرياض، الطبعة 2، 2002، ص 27.

ب- **التهديدات التقنية** : و تتلخص التهديدات التقنية في العديد من المشاكل التي تؤدي إلى توقف الأعمال لفترات مما يسبب خسائر كبيرة للمؤسسات كانقطاع التيار الكهربائي ، انقطاع الانترنت ، حدوث أعطال في مكونات نظم المعلومات.

ثانيا : التهديدات البشرية

التهديدات البشرية يمكن أن تكون متعمدة كما يمكن أن تكون غير متعمدة ، فالمتعمدة تكون منظمة و لها هدف تصبو إلى تحقيقه و هو إلحاق الضرر بالمؤسسة و أنظمة معلوماتها ، أما غير المتعمدة فتتمثل في أخطاء العاملين الذين يتعاملون مع أنظمة المعلومات و تنقصهم الخبرة و التدريب في هذا المجال و لكن رغم ذلك لا يمكن التمييز الجيد ما إذا كان التصرف خاطئا أو متعمدا ، لذا سيتم التعامل على أساس أن التهديدات هي تهديدات متعمدة.

و تنقسم مصادر التهديد البشرية إلى مصادر خارجية تصدر من أعوان خارجية (المنافسين ، الحكومات أو المصالح الخارجية ، الأعوان المالية ، الانحراف الاجتماعي ، المنظمات الإجرامية ، الجماعات الإرهابية ، جماعات الضغط ، المجتمع المدني...) ، أو داخلية (أجراء غير راضين أو أجراء قدماء ، متدربين ..)[7].

أ- التهديدات البشرية الداخلية

هي التهديدات الصادرة من داخل المؤسسة و التي يتسبب فيها العامل أو الموظف الذي يتعامل مع أنظمة المعلومات ، و له حق الوصول إلى شبكة المنظمة أو أماكن تواجد الأجهزة و المعدات ، أو أي شخص يكون دخوله طبيعيا إلى المؤسسة أو ينتمي إليها ، و يكون له نية إلحاق الضرر بأنظمة معلومات المؤسسة أو معلوماتها الحساسة من أجل استخدامها في تحقيق مصالح معينة.

و حتى نهاية القرن العشرين مصدر الجرائم المعلوماتية الأكثر خطورة كانت ذات مصدر داخلي صادرة من العمال نظرا لامتلاكهم المعارف ، و قدرتهم في الوصول إلى الأنظمة ،[8] إضافة إلى أن المهاجم الداخلي ليس معرض لكثير من الاحترازات الأمنية التي تضعها المؤسسة ضد المهاجم الخارجي ، و عليه يمكنه القيام بأعمال يصعب على غيره

[7] **Eric Delbecque , Jean-Renaud Fayol** , op cit , pp 89-90.

[8] **Kenneth Laudon et Jane Laudon** , « Management des systèmes d'information » , édition Pearson, 9éme édition , France, 2006, p 355.

القيام بها ، و إذا كان متمكنا يمكنه إخفاء أي أثر أو دليل يبين ارتكابه الهجوم. و من بين الأفعال التي يقوم بها المهاجم الداخلي دونا عن غيره ما يلي:[9]

- مهاجمة الشبكة الداخلية للمنشأة التي يعمل فيها.
- مهاجمة المعلومات بالسرقة أو التغيير أو الحذف.
- فتح ثغرات في أنظمة الحماية التي وضعتها الجهة لتحصين أنظمة معلوماتها.
- ردم الفجوة أو الفاصل بين الشبكات المستقلة : و ذلك أن الجهات التي لديها معلومات مهمة جدا تسعى دوما لفصل شبكة معلوماتها الداخلية عن الانترنت ، فنجد لكل من هذه الجهات شبكتين احداهما داخلية تحوي المعلومات السرية ، و أخرى خارجية (انترنت) تحوي المعلومات التي ترغب الجهة توفيرها للعالم الخارجي ، و الفصل بينهما يحمي الشبكة الداخلية من المهاجمين الخارجيين ، لكن المهاجم الداخلي يقوم بردم هذه الفجوة فيقوم مثلا بنقل بعض المعلومات الحساسة من الشبكة الداخلية إلى الشبكة الخارجية ، أو بنقل بعض البرامج الخبيثة كالفيروسات من الشبكة الخارجية إلى الداخلية.

و السبب في تجاهل التهديدات الداخلية هو الإعلام ، فالإعلام المعاصر للإجرام الإلكتروني يوجه الأنظار حول أن التهديدات في مجال الأمن تجاه المؤسسة مصدرها من الخارج ، و في الحقيقة ، التهديدات الناتجة من داخل المؤسسة هي فعلية و لكن الإعلام لا يركز عليها أو غير متداولة إعلاميا ، كما أن هناك دراسات كشفت أن إهمال المستخدمين هي من أهم أسباب إصابات أمن الشبكة ، فالعديد من العمال ينسون كلمة المرور للدخول إلى النظام المعلوماتي أو يسمحون لأصدقائهم باستعماله مما يهدد أمن النظام.[10]

و مقارنة بين حجم الخطر الداخلي و بين حجم الخطر الخارجي سنذكر بعض الاحصائيات :

وفقا **لمكتب التحقيقات الفدرالي** (FBI)تشكل التهديدات الداخلية من 60% إلى 80% من التهديدات التي يتم الإخبار عنها.[11]

[9] **خالد بن سليمان الغثبر ، مهندس محمد بن عبد الله القحطاني ،"** أمن المعلومات بلغة ميسرة" ، مكتبة الملك فهد الوطنية ، الرياض ، الطبعة الأولى ، 2009، ص ص 28 -29.

[10] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p 357.

[11] See :Cisco systems ,inc :Indiana, cisco press, cisco networking academy, first year companion guide , 2nd ed, 2001, p 20.

و حسب دراسة قامت بها Gartner Group على المخطط الأوروبي سنة 1997 ، ذكرت المنظمات فيها أن مشكل الأمن هو بنسبة 47% من الأعوان الداخليين (المستخدمين) و يعتبر العمال القدماء مسؤولين بنسبة 10% من الحوادث ، أما الخارجيين فهم مسؤولين بنسبة 39%.[12]

و حسب دراسة أجريت سنة 2003 على 408 خبير معلوماتي يقولون أن 94% من الأدوات المعلوماتية المسؤولة تعرضت لمشكل أمني من مصدر داخلي قام به المستخدمون.[13]

كما كشفت دراسة أجرتها الأمم المتحدة عام 2005 أن 37% من جرائم الاختراق و التعدي داخلي ، و أن 23% يرجع إلى مصادر خارجية ، و بلغ حجم الخسائر الاقتصادية لهذه الجرائم عام 2004 فقط حوالي 3.5 مليار دولار ، كما كشفت الدراسة أن حالات الاختراق بصفة خاصة كإحدى الجرائم المعلوماتية التي وقعت على أجهزة الحكومة الأمريكية لعام 2004 بلغت 354000 حالة اختراق ، 64% منها ناجحة و لم يكتشف سوى 4% منها.[14]

و بخصوص تحصين أنظمة المعلومات فتكون الجهود المبذولة و المسخرة في التحصين ضد التهديد الخارجي على حساب الاستعداد ضد التهديد الداخلي ، في حين هذا الأخير غالبا ما يحدث دمارا باهظ التكاليف ، فحسب تقديرات معهد أمن الحاسوب فإن معدل تكاليف الهجوم الداخلي هو 2.7 مليون دولار للهجوم الواحد ، بينما لا يزيد معدل الهجوم الخارجي الواحد عن 57 ألف دولار.[15]

هذه الدراسات و الإحصائيات أثبتت و بالإجماع أن التهديد الأكبر الذي تتعرض له المؤسسة و أنظمتها المعلوماتية هو من الداخل و بنسب كبيرة جدا مقارنة بالتهديد الخارجي ، و يتم التهديد الداخلي على يد مستخدمين غير راضين على وضعيتهم في العمل أو يدفعهم الانتقام ، أو يمكن أنهم يعملون لصالح جهة أخرى منافسة ، كما أن المستخدمين القدماء لهم يد كذلك في هذا الجانب نظرا لامتلاكهم مفاتيح و كلمات مرور تخولهم الدخول لأنظمة المعلومات و قد لا تنتبه المؤسسة في تغييرها بعد خروج أي مستخدم كانت له الصلاحية في امتلاكها ، هذا إضافة إلى تكلفة الدمار التي هي أضعاف مضاعفة مقارنة بالتهديد الخارجي نظرا لامتلاك كل الوسائل من أجل التنفيذ الكامل للهجوم.

---

[12] **Didier Godart**, op cit , p23.

[13] Ibid , p23.

[14] **الرشيدي علي بن ضبيان** ، "العدوان على البيئة المعلوماتية : خطورته و مواجهته" ، مجلة كلية الملك خالد العسكرية، العدد 81 ، الرياض ، 2005 ، ص 12.

[15] " Internal threat-Risks and countermeasures", 15/12/2001 in : http://www.sans.org/rr/papers/60/475.pdf.

ب- **التهديدات البشرية الخارجية:**

هي تهديدات تنفذها هيئات من خارج المنظمة و تكون إما من خلال الانترنت أو خطوط الهاتف نظرا لعدم امتلاكها حق الوصول إلى الشبكة الداخلية للمؤسسة ، و تكمن خطورة هذا النوع من التهديد في عدم أو صعوبة معرفة المخترق و أهدافه من وراء الاختراق ، و مدى الاختراق الذي مس النظام.[16]

و يتطلب تنفيذ الهجوم الخارجي مهارات تقنية من أجل اختراق أنظمة الحماية المتخذة من قبل المؤسسة و يختلف مستوى الهجوم حسب مهارة المخترق و الوسائل المتخذة في عملية الاختراق ، فنجد المبتدئين ليس لهم مهارات عالية و إنما يستخدمون برامج جاهزة على الانترنت و رغم بساطة الوسائل المستعملة إلا أنهم يمثلون خطرا على الأنظمة ، لأنهم يجربون برامج الهجوم بدون خلفية عن تطبيقها و آثارها مما يحدث دمار واسع دون أن يدري ، و نجد المتمكنين الذين يمتلكون مهارات عالية في اختراق أنظمة الحماية مهما كانت قوية و هؤلاء هم الذين يعتبرون خطرا على المؤسسة لعدم معرفتهم و معرفة أهدافهم.

و لكن رغم كل هذا يبقى تطور الاعتداءات الداخلية هو الأكثر اقلاقا ، فهي تتكاثر و من الصعب تحديدها ، كما أنها تحدث خسائر كبيرة.[17]

المطلب الثاني : أنواع المهاجمين و دوافعهم

مصادر الهجوم و أنواع المهاجمين تتعدد و بالتالي دوافع الهجوم تختلف ، و لكن معرفة أنواع المهاجمين و فهم دوافعهم و مستواهم التقني يسمح بتحديد قدرتهم الهجومية و معرفة كيفية التصدي لها. و من خلال هذا المطلب سنقوم أولا بمعرفة أنواع المهاجمين الذين يمكن أن تتعرض لهم المؤسسة بصفة عامة و الأنظمة المعلوماتية بصفة خاصة ، ثم نسرد أهم الدوافع و الأسباب التي تدفعهم لذلك.

[16] **محمد دباس الحميد ، ماركو ابراهيم نينو ، "**حماية انظمة المعلومات **"**، دار الحامد للنشر و التوزيع ، عمان ، الأردن ، 2009 ، ص ص 40-39

[17] **Christian Harbulot**, « manuel d'intelligence économique, presse universitaires de France », 1er édition, paris, 2012, p 283.

الفرع الأول : أنواع المهاجمين (القراصنة)

قراصنة المعلومات هم أشخاص يبحثون عن الحصول على مدخل غير مسموح به من أجل الدخول لأنظمة المعلومات ، الأغلبية لديهم نية إجرامية ، لكن عموم الناس لا يستطيعون التمييز بين مختلف القراصنة .[18] من خلال هذا الفرع سنقوم بذكر أكثر أنواع المهاجمين شهرة و مختلف الخصائص التي يتميز بها كل منهم.

1- المعتدين أو المخترقين (Agresseurs)

ينقسم المعتدين أو المخترقين إلى نوعين:

أ- الهاكر (الإنفعالي) :

و يعرفون على أنهم أشخاص فضوليين ، يبحثون عن المتعة ، يقرصنون بهدف اللعب أو بسبب تحد ما ، لا يحدثون الضرر بتعمد أو قصد ، غالبا ما يكونون غير واعين بمقاس أعمالهم فالمعتدي الانفعالي أقل خبرة و حنكة من الكراكر.[19] كما أن فئة الهاكر عبارة عن شباب مراهقين بين 12 و 25 سنة ، هم غريبي الأطوار، صبورين ، يقضون ليال بيضاء في استكشاف أنظمة المعلومات بحثا عن المعلومات و المعطيات و الروابط نحو أنظمة أخرى ، و يعتبر الهاكر أول نوع من القراصنة المعلوماتية و هو أول قاعة ضروري أن يمر عليها كل القراصنة.[20]

من خلال ما تم وصف الهاكر به يظهر لنا أنهم عبارة عن مراهقين هدفهم المتعة إلا أن العديد من الأقوال و الأفكار التي طرحت حولهم تبين أنهم شباب مراهقين فعلا و لكنهم يتمتعون بذكاء عالي و هدفهم ليس التخريب و إنما المساعدة حتى أنه أحيانا يتم الاستعانة بهم من قبل شركات لاكتشاف الثغرات الأمنية و سدها.

ب- الكراكر (المحطّم):

الكراكر أكثر خطورة من الهاكر ، يستعملون ذكاءهم بطريقة شريرة ، يبحثون عن إلحاق الضرر و إظهار أنهم الأقوى و يسعون دائما لإظهار و تأكيد تميزهم [21]، تتراوح أعمارهم بين 25 و 45 سنة ، و من أبرز سمات و خصائص أفراد هذه الطائفة بأنهم ذوي مكانة في المجتمع ، و متخصصين في مجال التقنية الالكترونية.[22]

[18] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p 354
[19] Menaces sur les systèmes informatique « Guide N 65 », bureau conseil de la direction centrale de la sécurité des systèmes d'information , paris , version du 12 septembre 2006 , p 8
[20] **Didier Godart** , op cit , p 25
[21] Menaces sur les systèmes informatique « Guide N 65 », op.cit , p 8.

2- المحتالين :

هذا النوع يحكمه طمعه ، و يتميز بالحذر و السرعة و الفعالية ، يقتنص فرص المبادرة ، يعرف متى ، أين و كيف ينفذ هجومه[23] ، هذا النوع من القراصنة يشبه كثيرا المجرمين التقليديين لأن هدفه الحصول على المال بأي طريقة كانت سرقة ، تزوير ، اختلاس...لذا غالبا ما تكون وجهتهم المؤسسات المالية كالبنوك ، مؤسسات التأمين...

3- المستخدمين الخبيثين :

و يطلق على هذه الطائفة أيضا المنتقمون ، لأن صفة الانتقام و الثأر هي ما تتميز به عن بقية الطوائف ، و هي الباعث لتصرفاتهم لأنها تنطلق ضد أصحاب العمل ، و المنشآت التي كانوا يعملون بها[24] . يعرفون جيدا الثغرات فهم غالبا ما يكونون خبراء في الاعلام الآلي ، و بالتالي يستطيعون الوصول إلى الملفات و البرامج غير المصرح لهم ولوجها ، أو تكون لهم الصلاحية بذلك بما أنهم موظفين و لكنهم يخونون الثقة و يستعملونها لأغراض خبيثة ، كما أنهم لا يفاخرون كبعض الفئات ، بل يقومون بإخفاء و انكار كل ما ينسب إليهم من تهم.

4- المناضلين أو الإرهابيين

هذا النوع من القراصنة هم الأكثر خطورة ، لديهم قضية ما يدافعون عنها ، و عادة ما يقومون بإرسال رسائل التهديد و تدمير البيانات المخزنة لمجرد أن يسجلوا وجهة نظرهم ، لا يعملون داخل حدود الدولة ، بل يمكن أن يعمل من أي مكان في العالم مما يصعب عملية اقتناصهم[25] ، لا يسعون لتحقيق أهداف شخصية أو مكاسب مالية بل يحاولون الإضرار بكل من يخالف معتقداتهم و يعارض مذاهبهم كما يحاولون ضم أكبر عدد إلى صفوفهم لديهم قدرات مالية هائلة و شبكة علاقات عالمية تمكنهم من ارتكاب مختلف أنواع الهجوم في مختلف الأماكن.

---

[22] **محمد دباس الحميد ،ماركو ابراهيم نينو ،"** حماية أنظمة المعلومات" ، دار الحامد للنشر و التوزيع ،الطبعة الأولى ،2007 ،ص 73.

[23] **Robert Longeon ,Jean-luc Archimbaud ,"** guide de la sécurité des systèmes d'information à l'usage des directeurs" , Centre National de la Recherche Scientifique (CNRS) , Paris ,1999 , p12.

[24] **محمد بن عبد الله بن علي المنشاوي ، "**جرائم الانترنت في المجتمع السعودي" ، رسالة ماجستير في العلوم الشرطية ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ، 2003 ، ص 38 .

[25] **دياب موسى البداينة ، "**الجرائم الالكترونية : المفهوم و الأسباب "، الملتقى العلمي : الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية و الدولية ، عمان ، الأردن ، 2014 ، ص 21

5- الجواسيس

يشاركون في الحرب الاقتصادية ، يعملون لحساب دولة أو لحساب منافس ، صبورين و محفزين ، يتقنون الحفاظ على سر نجاحهم من أجل عدم إثارة الشكوك و إتمام أعمالهم في الظل ، يتحركون غالبا من داخل المؤسسة ، إما عن طريق ايجاد وسيلة للاختراق ، أو بشراء شخص لديه صلاحية الوصول إلى الأجهزة ، هدفهم سرقة المعلومات أو القضاء على المعطيات الاستراتيجية للمؤسسة ، في كل الأحوال الجواسيس لديهم مستوى هائل في التحكم بالذات ، إضافة إلى قدرة كبيرة في التأقلم مع المحيط.[26]

و أخيرا يمكن القول أن القراصنة المعلوماتيين لا يمتلكون أساليب سحرية تفتح لهم كل أبواب أنظمة المعلومات ، و إنما يتمتعون بخصائص تسمح لهم بذلك ، منها:[27]

- المعرفة الجيدة بثغرات أنظمة الاستغلال.
- التحلي بالصبر من أجل التقاط المعلومات في تحضير الهجمات.
- امتلاك الأدوات.
- ضعف وسائل الحماية.

الفرع الثاني : دوافع الهجوم

في الحياة الواقعية العديد من الدوافع تدفع الأشخاص إلى ارتكاب الجرائم ، و لعل الدافع المالي أهمها ، و لكن في عالم المعلوماتية هناك دوافع إضافية على هذا الدافع[28] ، و تختلف دوافع الهجوم حسب طبيعة هذا الأخير ، فنجد الدوافع العامة التي تكون بين دول أو مؤسسات او جماعات و نجد الدوافع الشخصية التي يقوم بها فرد واحد أو أكثر لأسباب شخصية.

[26] Menaces sur les systèmes informatique « Guide N 65 », op cit , p9

[27] **Eric Léopold, Serge Lhoste**, « la sécurité informatique », éditions Puf, 3éme édition, Aout, 2007 , p50.

[28] **George Sadowsky, et autres**, Information Technology Security Handbook , the International Bank for Reconstruction and Development, Washington, 2003, p24.

1- **الدوافع العامة** : من بينها نذكر:

الدوافع الاستراتيجية :

بالنسبة للدولة ، الهجمة الاستراتيجية تهتم بالمعلومات المتعلقة بأمن الدولة ، و المعلومات التي تخص الإرث الوطني، سواء ذات طابع علمي ، تقني ، صناعي ، اقتصادي أو دبلوماسي ، فالتهديد الاستراتيجي يمكن أن يعيق اتاحة أنظمة المعلومات التي يعتبر عملها المستمر ضروري للسير الحسن و العمل العادي للمؤسسات. أما بالنسبة لمؤسسة أو منظمة ، التهديد الاستراتيجي يكون هدفه الحصول على كل معلومة حول أهداف و نشاط هذه المؤسسة من أجل استقطاب زبائنها ،كشف أساليب الانتاج ، نتائج البحث و التطوير ، و هذا يكون غالبا من فعل المنافسين.[29]

الدوافع الإيديولوجية :

الدوافع الايديولوجية يمكن أن تكون محركات للأعمال المتطرفة ، فهذا التهديد يمكن أن يهتم بالملفات المعلوماتية التي تتضمن معلومات ذات طابع خاص حول الأشخاص ، فبعض التيارات الفكرية كالعديد من القراصنة لهم قناعة أن المعلومات ملك الجميع و ليست حكرا على جهة معينة.[30]

الدوافع الارهابية :

الارهاب المعلوماتي هو فعل تدمير أو شراء أنظمة معلوماتية بهدف اخلال توازن بلد أو الضغط على حكومة ،[31] فالتهديد الإرهابي هو كل النشاطات المنافسة التي تؤثر على توازن الأنظمة المقامة، و النشاطات التي تدخل في هذا الصنف يمكن أن تأخذ طابع عنيف كالتدمير المادي أو التلاعب بالمعلومات الحساسة، و الدوافع الارهابية تكمن في تحقيق نتائج خارقة من أجل إحداث ضجّة عالمية و إحداث الحرب السيكولوجية ، و تخويف الناس.[32]

[29] Menaces sur les systèmes informatique « Guide N 65 », op cit , p10.
[30] Ibid , p10.
[31] **Didier Godart** , op cit ,p34.
[32] Menaces sur les systèmes informatique « Guide N 65 », op cit , p10.

الدوافع السياسية

الدوافع السياسية تكمن في خلق حدث خاص يجعل وسائل الاعلام تنتبه إليه و تركز حوله ، فالدوافع السياسية هي القيام بمختلف النشاطات كتلفيق الأخبار ، التزوير...من أجل تشويه صورة الدولة المستهدفة أو المذهب المستهدف.[33]

الدوافع المالية :

الدافع المالي يمكن أن يكون الدافع الأكبر حصة من مجموع دوافع ارتكاب الهجمات الالكترونية نظرا للفائدة التي يعود بها على الجهة المنفذة ، سواء باختراق أنظمة المؤسسات و خاصة المالية منها و سرقة ما يمكن سرقته، و إما بالتسبب في خسائر للضحية مما يعود بالنفع على الجهة المهاجمة كحصة سوق أو عروض تجارية أو إفقاده مصداقيته.

و من أجل توضيح مدى و قدر الأرباح المحققة عند النجاح في ارتكاب الجريمة الالكترونية يقول أحد المجرمين المحترفين في سجن كاليفورنيا : " لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية ، و بإمكاني أن أكرر ذلك في أي وقت ، لقد كان شيئا سهلا فأنا أعرف أسلوب عمل جهاز حاسوب الضرائب و قد وجدت ثغرات كثيرة في نظامه يمكن أن تمدني بمبالغ طائلة لو لم يكن سوء الحظ قد صادفني "[34]

كما يمكن ادراج تحت الدافع المالي ما تقوم به بعض الشركات المتخصصة بإنتاج الحلول الأمنية للمؤسسات حيث تقوم بإطلاق هجمات إلكترونية على شكل برمجيات خبيثة عبر الشبكة بشكل سري و تقوم بعد ذلك بفترة بإعلان أنها قامت بإنتاج مكافح أو معطل قادر على حماية النظام من هذه البرمجيات فتتهافت الشركات و المؤسسات لشراء ذلك المكافح مما يعود بالنفع على الشركة المنتجة بالربح.[35]

[33] Menaces sur les systèmes informatique « Guide N 65 », op cit , p10.

[34] **نهلا عبد القادر المومني** ، "الجرائم المعلوماتية" ، دار الثقافة للنشر و التوزيع ، الطبعة الاولى ، عمان ، 2008 ، ص91 عن : صغير يوسف ، الجريمة المرتكبة عبر الانترنت ، رسالة ماجستير ، جامعة مولود معمري تيزي وزو - 2013 ،ص 39.

[35] **أسامة سمير حسين** ، "الاحتيال الالكتروني - الأسباب و الحلول – "، الجنادرية للنشر و التوزيع ، الطبعة الأولى ،2011 ، ص 97.

2- **الدوافع الشخصية** : و نذكر منها :

دافع الانتقام :

الانتقام يكون من قبل عمال اتجاه أنظمة المؤسسة التي يعملون بها ، و هو حافز كبير يجعل العامل ينفذ هجمات ضد نظم المعلومات ، كأن يحس العامل أنه ليس مقدّر على قدر كفاءته ، أو أن يشعر أنه سيفقد عمله ، أو المعاملة معه سيئة ، كل هذه العوامل تدفعه للانتقام لذاته و تبعث البهجة في نفسه.

التسلية و اثبات المهارات الفنية:

فاعلو هذا التهديد ينشطون برغبة في التسلية أو زيادة في التعلم ، فهم يعتبرونها تسلية و لعب أكثر منها جريمة حقيقية ، دوافعهم هي تحقيق انتصارات تقنية [36]، فالكثير من الأشخاص يشعرون بالفخر على قدرتهم على تنفيذ هجمات الكترونية و اختراق مواقع و الوصول إلى قواعد بيانات محمية ، و لكن في الواقع أغلبية هؤلاء لا يملكون معرفة حقيقية بشن الهجمات الالكترونية و لكن هناك برامج جاهزة يسهل استخدامها في مهاجمة أنظمة المعلومات دون تطلب معرفة كبيرة بالحاسوب أو الشبكات ،و يسمي المتخصصون في مجال أمن المعلومات هذا الصنف أطفال البرامج الجاهزة.[37]

اثبات ضعف نظم الحماية :

فهناك هجمات تشن فقط لإثبات أن أنظمة الحماية المتخذة ضعيفة و يمكن اختراقها، فقد قامت عصابة هاكرز متكونة من 5 أشخاص:4 مصريين وفرنسي الاستيلاء على حسابات بطاقات خاصة بعملاء البنوك، لكن الشاب الفرنسي"**جان كلود** "استطاع تصميم بطاقة صرف آلي و سحب بها مبالغ من إحدى البنوك ثم ذهب إلى البنك وأعاد إليه المبالغ وأخبرهم أنه فعل ذلك ليؤكد لهم أن نظام الحماية بالبنك ضعيف و يمكن اختراقه، و لكن هذا لم يمنع الشرطة الفرنسية من القبض عليه و محاكمته.[38]كما قامت مجموعة من الشباب الأمريكي أطلقوا على

[36] Menaces sur les systèmes informatique « Guide N 65 », op cit , p11.
[37] " Internal threat-Risks and countermeasures", 15/12/2001 in :
خالد الغثبر،مهندس القحطاني،أمن المعلومات بلغة ميسرة،مرجع سابق عن http://www.sans.org/rr/papers/60/475.pdf
[38] **أسامة سمير حسين** ، مرجع سابق ، ص 101.

أنفسهم"**الجحيم العالمي** "اختراق مواقع البيت الأبيض، و المباحث الفدرالية، والجيش ووزارة الداخلية، لكنهم لم يخربوا تلك المواقع بل اقتصر دورهم على اثبات ضعف نظم الحماية في تلك المواقع، إلا أنهم حوكموا أيضا.[39]

و عليه فان دوافع ارتكاب القراصنة لهجمات الكترونية عديدة و متعددة ، فهناك الدوافع العامة كالدوافع المالية و السياسية و الايديولوجية ...، و الدوافع الخاصة كدافع التسلية و الانتقام و اثبات المهارات....و تختلف طريقة تنفيذ التهديد و خطورته من نوع لآخر ، و سنتعرف على أنواع التهديدات من خلال المطلب الموالي.

المطلب الثالث : أنواع التهديدات على المعلومات و نظم المعلومات

إلى جانب التهديدات التقليدية ، تهديدات جديدة ظهرت بفعل تطور أساليب عمل المنظمات ، فتطور الاعتداء و تقنيات الاعتداء أصبح أمرا مقلقا ، إذ أصبحت هذه التقنيات في تطور سريع مما يعمل على إحداث خسائر كبيرة . من خلال هذا المطلب سنقوم بشرح مختلف أنواع التهديدات سواء الناتجة عن اعتداءات أو تلك الناتجة عن الأخطاء و الثغرات الأمنية.

الفرع الأول : التهديد الناتج عن الاعتداءات

و من تقنيات الاعتداء نجد : زرع البرامج الضارة، القرصنة المعلوماتية أو الاختراق ، الاعتداء المادي.

أولا : البرامج الضارة (الخبيثة)

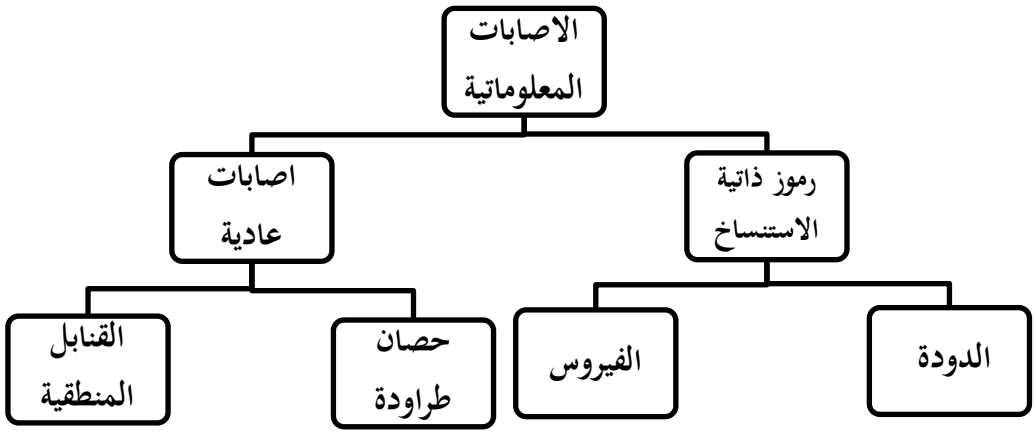
و هي كل برنامج يدخل في النظام و يكون عمله ضارا و خبيثا.

و تعرف أنها كل البرامج التي و بدون علم المستعمل تُوجَّه لتشويش ، تعديل أو القضاء على كل أو جزء من العناصر الضرورية للعمل الطبيعي للحاسب.[40]

[39] **عبد العال الديربي ، محمد صادق اسماعيل ، "**الجرائم الالكترونية – دراسة قانونية قضائية –**"** ، المركز القومي للإصدارات القانونية ، الطبعة الأولى ، 2012 ، ص 175.

[40] Les virus informatiques, Espace menace-groupe virus, CLUB de la Sécurité des Systèmes d'Information Français (CLUSIF), 2005, p06. Vu sur le site : http://www.leprovostjm.com/docs/virusinformatiques.pdf Le 25/01/2016 à : 05.57

الشكل (2.1): ترتيب الاصابات المعلوماتية



Source : Eric Filiol , les virus informatiques : théorie, pratique et applications , deuxième éditions , Springer , Paris , 2009, p111.

و من بين هذه البرامج نذكر :

1- الفيروسات Virus

أ- تعريفها

التعريف الذي يمثل المرجعية في عالم الأمن هو تعريف [41]« Fred Cohen » الذي عرف الفيروس على أنه : " برنامج له القدرة على إصابة برامج أخرى عن طريق تعديلهم بطريقة تجعلهم يحتوون على صورة منه ".[42] و كان Fred Cohen أول من تداول أو أخرج مصطلح "الفيروس المعلوماتي " سنة 1984.[43]

و تعرف الفيروسات على أنها :برمجيات خبيثة بطبيعتها ، تؤثر سلبا في الحواسيب بشكل مباشر ، و في غير الحواسيب بشكل غير مباشر ، فالفيروس عندما يحذف ملفات مهمة للعملاء فإن التأثير يتعدى الحاسوب إلى العملاء و سمعة الشركة ، و الفيروسات لها تأثيرات منها ما يقوم بحذف ملفات أو برامج أو تعطيلها عن العمل ، و منها ما يقوم بزراعة برامج خبيثة أخرى قد تكون تجسسية، و منها ما يعطل الجهاز بالكلية ، و هناك أنواع

[41] « un virus est programme capable d'infecter d'autres programmes en les modifiant de manière à ce qu'ils contiennent une copie de lui-même, parfois évoluée »
[42] **Michel Lafitte**, « Sécurité des systèmes d'information et maitrise des risques », édition Revue Banque, 2003, p90
[43] Les virus informatique, CLUSIF , 2005 , op cit, p01.

للفيروسات منها ما يكون مكون من أجزاء متعددة ، و منها ما تتغير صفاته بشكل دوري ، ومنها ما يكون متخفيا حتى من برامج مكافحة الفيروسات.[44]

هذا التعريف يبين أولا الآثار الجانبية و غير المباشرة للفيروس و المتمثلة في نتائج تدمير البرمجيات و الملفات ، و إضافة إلى ما ذكره التعريف من آثار كخسارة العملاء و السمعة يمكن أن تخسر المؤسسة أموالا طائلة أو تخسر وقتا ، و كل هذا قد يؤدي إلى الإفلاس ، ثانيا يبين التعريف و يذكر مختلف تأثيرات الفيروس.

كما يعرف الفيروس المعلوماتي على أنه برنامج مقرصن ، يرتبط ببرامج أو ملفات من أجل تنفيذه ، و غالبا ما يكون ذلك بدون تصريح من المستخدم ، أغلب الفيروسات المعلوماتية تحتوي على نشاط ، هذا النشاط قد يكون حميد ، مثل تعليمات من أجل كشف رسالة أو صورة ، أو يكون جد مدمر، مدمر للبرامج ، معيق للذاكرة ، مثير لإعادة مسح القرص الصلب ، أو استعمال سيئ للبرامج ، و عادة ما ينتشر الفيروس من حاسب لآخر عند القيام بإرسال ملفات مصابة كقطع إضافية عن طريق البريد الالكتروني.[45]

هذا التعريف له نظرة مختلفة قليلا للفيروس ، فهو يقسم نشاط الفيروس إلى قسمين ، قد يكون حميد و ليس ضارا، و قد يكون مدمرا.

كما يمكن اعتبار أن الهدف الوحيد للعديد من الفيروسات هو الاستنساخ ، و بالتالي لا يكون هناك أضرار و نتائج كارثية ، و لكن السمعة السيئة للفيروس تأتي بفعل تأثيراته الثانوية ، بمعنى النشاطات المنفذة من قبل برنامج الفيروس تختلف حسب أهداف مصممي الفيروس ، فبعضهم لا يقوم إلا بطلب من المستخدم أن يتمنى له عيد ميلاد سعيد من خلال كتابة بعض الكلمات، و البعض الآخر تكون نتائجه أكثر خطورة كالمسح أو تزييف المعطيات.[46]

من خلال التعريفات السابقة و الإطلاع على عديد المراجع تخرج الباحثة بالتعريف التالي : "الفيروس برنامج خبيث ، تم تصميمه من قبل أحد المبرمجين لتحقيق بعض الأهداف من وراء ذلك ، و حسب هذه الأهداف تكون النتائج ، قد تكون عادية غير مضرة كإظهار بعض الصور و الإعلانات مثلا ، قد تكون خطيرة نوعا ما كتعديل جزء من البرامج ، و أغلبها يكون مدمر كتعطيل و تدمير البرامج و الأجهزة كلية ، و من سمات الفيروس

[44] خالد الغثبر، مهندس القحطاني،مرجع سابق ، ص 65 ، ص 66.

[45] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p352

[46] **Eric Léopold, Serge Lhoste**, op cit , p43.

قدرته على ربط نفسه بالبرامج و نسخ نفسه بنفسه دون علم المستخدم إضافة إلى قدرته على التخفي و الانتشار السريع .

ب– آلية عمل الفيروس

آلية عمل الفيروس تكون عن طريق بحث الفيروس عن هدف معين عن طريق انتقاء برامج أو ملفات ذات حجم معين أو بنية محددة ، يقوم بالانتشار السريع على مستواها و إعادة نسخ نفسه ، و بالتالي يضمن نسخة منه على مستوى الهدف و من ثم يطلق هجومه[47] . فالفيروسات دائما ما تستتر خلف ملف آخر ، و لكنها تأخذ زمام السيطرة على البرنامج المصاب، بحيث أنه بمجرد تشغيل هذا الأخير يتم تشغيل الفيروس أيضا.[48]و بالتالي يكون عمله مشابها لعمل الفيروس البيولوجي الذي يصيب جسم الإنسان لهذا سمي باسمه ، فمثل ما أن الفيروس البيولوجي يدخل في الجهاز الوراثي لخلية من أجل أن ينسخها ، الفيروس المعلوماتي يدخل في رمز البرنامج باحثا عن تعليمات التي بمجرد تنفيذها تبدأ عملية الانتشار و الهجوم.[49]و لكن اليوم نشاط الفيروس لم يعد محصورا في إعادة النسخ و إطلاق الهجوم بل هناك نشاط إضافي يجب أخذه بعين الاعتبار و هو ضمان بقائه ، إذ أصبح الفيروس يخفي تواجده باختلاطه مع ملفات ضرورية لعمل الأنظمة[50]، و في نفس السياق و لزيادة تعقيد اكتشاف الفيروس ظهر مؤخرا ما يسمى ب polymorphisme و هي قدرة الفيروس على أخذ عدة أشكال من أجل تضليل برامج مكافحة الفيروس إضافة إلى ظهور ورشات خلق برامج فيروسات بسمح بإضافة على الفيروسات الموجودة قدرات تشفير ليصبح تحديدها أكثر تعقيدا.[51]و بالنسبة لطريقة الفيروسات في عملية التدمير فإن الفيروس الذي يدمر المعطيات بطريقة جد فورية و سريعة فرص بقاءه و انتشاره جد ضعيفة إذا كانت هناك عملية تخزين جيدة ، و بالعكس ، الفيروس الذي يدمر المعطيات بطريقة جد تدريجية يمكن أن يبقى بطريقة خفية لوقت طويل.[52]

[47] **Michel Lafitte**, op cit , p91.

[48] أسامة سمير حسين ، الاحتيال الالكتروني ، مرجع سابق ، ص 124

[49] **Eric Léopold, Serge Lhoste**, op cit , p42

[50] **Didier Godart , sécurité informatique**, op cit ,p59

[51] **Eric Léopold, Serge Lhoste**, op cit , p42

[52] **Eric Léopold, Serge Lhoste**, op cit , p43.

2- الديدان Vers

الديدان عبارة عن برامج مستقلة تنتقل من حاسب لآخر داخل الشبكة دون الحاجة لتدخلات بشرية ، و تنتشر بسرعة أكبر من الفيروس ، و يمكن أن تخفي معطيات و برامج و اتلافها ، و إعاقة عمل شبكة معلوماتية[53]، فالديدان المعلوماتية تستقر في ذاكرة أنظمة المعلومات بنفس الطريقة التي تستقر فيها الدودة البيولوجية في تفاحة، و على عكس الفيروس ، فهي قادرة على نسخ نفسها بدون تدخلات داخلية أو خارجية ، إذ أنها لا تحتاج إلى تحميل ملف ، وثيقة أو بريد أو منفذ من أجل أن تنتشر ، فهي تنتج نفسها بفعل الشبكة باستغلال الثغرات الموجودة في النظام المتصل ، و نسل هذا البرنامج قادر على العيش منفصلا عن أصله على نظام آخر و يبقى على اتصال معه.[54]

كما تعرف الديدان على أنها : "برامج أو عمليات طفيلية تستغل موارد أنظمة المعلومات(ذاكرة حية ، شبكة ..) و أخطاء أنظمة التشغيل للآلات المتصلة بالشبكة المعلوماتية من أجل الانتشار و إصابة برامج أخرى ".[55]

و عليه يمكن تعريف الديدان على أنها برامج حاسوبية مضرة ، تنتقل بين الحواسيب بعدة طرق ، تعمل على نسخ نفسها ذاتيا سواء على الأقراص أو على الشبكات ، و تنتشر بسرعة هائلة ، عملها ليس ضار بصفة مباشرة و لكن سرعة تكاثرها و انتقالها السريعان يؤثران سلبا في فعالية الحاسوب و شبكة المعلومات.

و بالنسبة لتحقيق الدودة فهو أمر صعب و لكن بمجرد النجاح في ذلك تحدث خسائر كارثية ، و أكبر دليل هو الدودة المعروفة تحت اسم Slammer و هي أشهر دودة عبر التاريخ ، ففي 25 جانفي 2003 انتشرت الدودة عبر الانترنت و أصابت أكثر من 90% من أنظمة المعلومات العالمية في 10 دقائق.[56]

[53] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p352
[54] **Didier Godart** , op cit ,p69
[55] **Eric Léopold, Serge Lhoste**, op cit , p.48
[56] **George Sadowsky**, et autres, Information Technology Security Handbook op cit, 2003, p22.

3- حصان طراودة Chevaux de Troie

أ- تعريفه

مصطلح حصان طراودة مستعار من قصة النزاع الأسطوري بين اليونانيين الأوائل و شعب مدينة Troie، ففي الرواية التقليدية "باري" ابن ملك Troie ، هرب مع " هيلين" زوجة "Ménélas" de Sparte" ، فقام أخ Ménélas بإطلاق بعثة عسكرية يونانية ضد Troie ، الحرب التي دامت طيلة 10 سنوات انتهت أخيرا بخدعة انسحاب اليونان الذين تركوا وراءهم حصان خشبي عملاق تاركين بداخله جماعة من الجنود المهاجمين ، و عندما أدخل شعب Troie الحصان إلى المدينة ، خرج اليونان منه و فتحوا الأبواب لأصحابهم و دُمِّرت المدينة بأكملها.[57]

و من خلال هذا التشبيه يظهر لنا أن البرنامج يعتمد على الخدعة في عمله ، و عليه يعرف حصان طراودة على أنه : " رمز خبيث يختفي داخل برنامج ، مُظهرا بذلك براءته عن طريق تمثله في لعبة صغيرة أو بطاقة رغبات أو برنامج مشاهدة صور من أجل أن ينفذ لاحقا عمليات غير شرعية ".[58]

فهو " برنامج غير خطير في الظاهر ، و لكن تصرفاته غير متوقعة ، ليس فيروس لأنه لا يتكاثر ، و لكن يمكن أن يمرر فيروسات و رموز خبيثة أخرى من أجل أن يضمن دخوله في النظام المعلوماتي ".[59]

بمعنى أنه برنامج حاسوبي ظاهره بريء و مفيد لكنه يضمر جزءا ماكرا يتمثل في أعمال خبيثة و مضرة ، ينشط هذا الجزء بمجرد تشغيل البرنامج ، فيقوم بالسيطرة على الجهاز أو اتلافه ، أو التجسس على الحاسوب و جمع ما يمكن من معلومات سرية أو شن هجمات على حواسيب أخرى من خلال الحاسب المسيطَر عليه ، و هذا النوع من البرامج الخبيثة لا يتكاثر.

ب- طريقة عمله

يقوم المهاجم بزرع برنامج مستقبل أو خادم على جهاز الضحية بعدة طرق ، و يفتح منفذا خاصا به للاتصال عن طريق الانترنت ، ثم يقوم البرنامج بإرسال عنوان جهاز الضحية على الانترنت (IP) للمهاجم ، بعد ذلك

[57] **Didier Godart** , op cit ,p65
[58] Ibid, pp 65-66.
[59] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p352

يقوم المهاجم بالاتصال بذلك البرنامج ليبدأ التحكم بجهاز الضحية.[60] ببساطة يمكن أن يبعث لك شخص خبيث بريد يقول فيه : " مرحبا ، كيف حالك ، أنظر إلى هذا الملحق " و عند فتحه تجد لعبة أو رسوم متحركة تبدأ تنشط ، و عندما تكون تمضي وقتا ممتعا ، حصان طراودة يكون يستقر في أحشاء الحاسوب ليسيطر عليه ، فهذا النوع من الرموز يسمح برؤية ضربات لوحة المفاتيح ، رؤية الشاشة بأكملها ، اطلاق برامج بدون علم المستخدم ، الوصول إلى معلومات مخزنة في القرص الصلب و كذلك شبكة المنظمة التي يتصل بها المستخدم ، و يمكن أيضا التصنت على المحادثات و فقد السيطرة على لوحة المفاتيح.[61]

4- القنابل المنطقية Bombe logique

القنبلة المنطقية هي برنامج خبيث ، يستقر في النظام و ينتظر حدث معين (تاريخ ، نشاط ، معلومة معينة ...) و هذا مل يسمى بالزناد لينفذ نشاطه الهجومي.[62]

كما أنها تعرف على أنها برنامج يحتوي على وظيفة مدمّرة مخفية ، أُضيفت بطريقة محظورة إلى برنامج مضيف و الذي سيحتفظ بمظهره الطبيعي و عمله الصحيح إلى غاية الوقت الذي يختاره المبرمج الخبيث.[63]

و نجد نوعين من القنابل :[64]

- **القنبلة المنطقية المحددة** : يركب المبرمج داخل برنامج أجور المؤسسة مثلا وظيفة مدمرة تنفذ في حال لم يظهر اسمه في ملف الأجراء.
- **القنبلة المنطقية العمياء** : يركب المبرمج داخل برنامج عمومي موزع مجانا على الانترنت وظيفة و عادة مدمرة تنفذ مثلا كل 1 أفريل.

و لمعرفة خطورة هذا الرمز فقد قام "**تيموتي آلن ليود** "اطلاق قنبلة الكترونية ألغت كافة التصاميم و برامج الانتاج لأحد أكبر مصانع التقنية العالمية في **نيوجرسي** التي تعمل لحساب وكالة الفضاء NASA والبحرية الأمريكية[65].

---

[60] خالد الغثبر، مهندس القحطاني، ،مرجع سابق ، ص70.

[61] **Didier Godart** , op cit ,p65

[62] **Eric Filiol** , « les virus informatiques : théorie, pratique et applications » , deuxième éditions , Springer , Paris , 2009, p127

[63] Les virus informatique, CLUSIF , 2005 , op cit, p07

[64] Ibid, p 07.

[65] أسامة سمير حسين ، الاحتيال الالكتروني ، مرجع سابق ، ص 101.

ثانيا : القرصنة المعلوماتية (التجسس على أنظمة المعلومات)

القرصنة تعمل على كشف نقاط ضعف نظم الحماية لمواقع الانترنت و الأنظمة المعلوماتية ، و غالبا ما يتم استغلال مختلف وظائف الانترنت التي تحوله إلى نظام مفتوح سهل الاختراق.[66]

و عليه هذا النوع من تقنيات الاعتداء يتمثل في محاولة اقتحام أنظمة المعلومات و الحصول على المعلومات السرية بأي طريقة ، و سنقوم خلال هذا الجزء بذكر أكثر الطرق انتشارا .

1- التصنت L'Ecoute

التصنت يكمن في التموقع على شبكة معلوماتية أو شبكة التواصل عن بعد ، و من ثم تحليل و تخزين المعلومات العابرة ، و ترجمة التآمرات و كل ما يدور داخل الشبكة المعلوماتية.[67] فأغلبية أنظمة المعلومات تضع تحت تصرفها أدوات اتصال عن بعد من أجل وضع عدة حواسب على الشبكة ، و الاتصال عن بعد يتطلب بث الاشارة الذي يأخذ في أغلب الأحيان شكل موجة كهرومغناطيسية ، هذه الموجة يمكن أن تنتشر عن طريق الفضاء أو تكون موجهة عن طريق سلك الكتروني، و تمر في أغلب الحالات على مناطق يمكن أن تكون خارج مراقبة المجموعة المشاركة في الاتصال ، و عليه هناك خطر رؤية الاتصالات العارضة بفعل بثها من قبل شخص موجود في مجال الاشارة ، و هذا ما يضع سرية المعلومات العابرة في خطر ، فمعرفة كلمات المرور مثلا يمكن أن يهدي القراصنة باب للدخول في نظام المعلومات ،[68] إذ أنه و على مستوى الاتصال بالشبكة أو الانترنت العادية 99.9% من المعلومات التي تدور ليست مشفرة ، و يمكن اعتراضها من قبل أي أحد.[69]

و من أكثر البروتوكولات عرضة للتصنت بروتوكول (TCP/IP[*][**])[70] ، و من الأدوات المستخدمة لتنفيذ التصنت برامج تحليل الشبكات و بروتوكولاتها كبرنامج " Sniffer " و الذي يعرف على أنه برنامج أو تطبيق

---

[66] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p354

[67] Menaces sur les systèmes informatique « Guide N 65 », op cit , p13

[68] **Eric Léopold, Serge Lhoste**, op cit , p55

[69] **Jean-Marc Royer** , » Sécurisé l'informatique de l'entreprise : enjeux , menaces , prévention et parade » , édition ENI , p23.

[70] بروتوكول (TCP/IP) : هو اللغة الأكثر استخداما في الانترنت للتخاطب و تبادل المعلومات

[*] بروتوكول (IP) (Internet Protocol) : هو نوع من بروتوكولات التواصل للشبكة المعلوماتية ، يستعمل عن طريق الانترنت ، يقدم خدمة تحويل المعطيات تسمى datagrammes من العنوان المصدر نحو عنوان المستقبل ، أين المصدر و المستقبل هم آلات معرفة بعناوين ذات طول محدد ، و هذا البروتوكول لا يقدم ضمان للاستقبال الجيد و لا مراقبة المرور ، هذا من اختصاص بروتوكولات أخرى مثل .TCP

[**] بروتوكول TCP (Transmission Control Protocl) : مهمته عرض خدمة جد موثوقة في ارسال المعطيات نقطة بنقطة على مستوى شبكة معلوماتية ، و هو قادر على تحويل معطيات القاعدة و تحديد و تصحيح أخطاء الارسال و مراقبة المرور ، اقامة روابط متزامنة بين المرسل و المستقبل و تسيير التواصلات ، و هو يعمل تحت بروتوكول IP عن طريق اتصال بين عمليتين على حاسبين متباعدين

التصنت الالكتروني الذي يراقب المعلومة المنقولة داخل الشبكة، هذا النوع من البرامج يمكن أن يخدم عملية تشخيص المشاكل أو النشاطات غير المرغوب فيها داخل الشبكة ، و كلما استعمل لأهداف غير شرعية يمكن أن يحدث أضرار و من الصعب اكتشافه.[71]

فهذا البرنامج التجسسي يسمح بالتصنت على الحركة على الشبكة المعلوماتية التي تتصل مباشرة بالحاسب ، و من أولوياته البحث عن تحديد الحزم التي تضم كلمات login أو password .[72]

و هناك أيضا برامج لالتقاط المعلومات و هو : Keyloggers أي برنامج تسجيل نقرات لوحة المفاتيح و هو برنامج يزرع في الجهاز و يسجل كل ما يكتب على لوحة المفاتيح من رسائل ، دردشات ، كلمات مرور... و يُرسل إلى المهاجم.[73] أغلب هذه الآليات غير مرئية ، فضربات لوحة المفاتيح هي عموما مكتوبة داخل ملفات مؤقتة مشفرة و مرسلة آليا عن طريق البريد الالكتروني إلى المتجسس.[74]

فحتى لو كان التصنت لا يعني بالضرورة استخدام هذه المعلومات المتحصل عليها من هذه العملية بطريقة سيئة لكن بمجرد خروج المعلومة من اطارها الشرعي و استملاكها و معرفتها من قبل أشخاص غير مخولين فإن هذا يعتبر تهديد حقيقي يمس عنصر خصوصية المعلومة.

2- سرقة الهوية l'usurpation d'identité

سرقة الهوية أو التنكر هو من أنواع السبل غير الشرعية ، تتعلق بهجمة معلوماتية تكمن في انتحال شخصية أو هوية شخص آخر و الاستفادة من امتيازاته و حقوقه عن طريق اغتصاب هويته ، فالشخص يُعرَّف إما بما لديه (بصمة ، صوت ..) ، ما يملك (بطاقة تعريف ، بطاقة ائتمان ، شريحة ...) ، أو ما يعرف (كلمة سر ، تاريخ ميلاد...)، و من أجل انتحال شخصيته ، المتعدي عليه الاستيلاء على العديد من العناصر الخاصة به ،[75] و هذا يكون غالبا إما من أجل شراء سلع أو الاستفادة من خدمات أو الحصول على قرض...باسم الضحية.

و ملفات القرض هي من أهم أهداف القراصنة ، و تطور الانترنت و ظهور التجارة الالكترونية سهّل من مهمة سارقي الهوية ، إذ أن مواقع التجارة الالكترونية هي أحسن مصدر للحصول على المعلومات السرية للزبائن ،

[71] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p354
[72] **Eric Léopold, Serge Lhoste**, op cit , p53
[73] خالد الغثبر، مهندس القحطاني،مرجع سابق ، ص76
[74] Les virus informatique, CLUSIF , 2005 , op cit, 08
[75] Menaces sur les systèmes informatique « Guide N 65 », op cit , p19

و بمجرد أن يستطيع المتعدي الحصول عليها ينتحل الشخصية و يطلب قرض أو يشتري سلعة لأن الشراء على الانترنت لا يتطلب مقابلة شخصية .[76]

أهم تقنية خداع مستعملة هي هجمة مسماة " par spoofing "تسمح لهيئة ما أن تكون مشابهة لتلك الأصلية عن طريق بريد مظهره يوحي أنه عنوان موثوق بهدف الوصول خفية إلى تطبيقات و معلومات حساسة.[77] بمعنى هؤلاء القراصنة يقومون إما بخلق موقع مزور مشابه ، أو ارسال رسائل الكترونية يبدو عنوانها المرسلة منه هو ذلك الخاص بالمنظمة الحقيقة أي لا مجال للشك فيه ، و يطلب منك في هذه الرسائل إما الموافقة على ملف أو تحديث بيانات أو الموافقة على إجراءات جديدة للحماية عن طريق إدخال رقم بطاقة الائتمان أو كلمة مرور أو رقم بطاقة الضمان الاجتماعي ، و عليه تكون قد وضعت المعلومات السرية و الثمينة في موقع مزور.

3- رفض الخدمة

أ- تعريفها

هجمة رفض الخدمة حتى و إن كان ظاهرها غير مخيف و غير مخرب لنظم المعلومات إلا أن تأثيرها كبير و يؤدي إلى خسائر كبيرة و يمكن تعريفها كالتالي:

- هي نشاط خبيث يترجم بانشغال أو عدم اتاحة مؤقت أو دائم لعدة مكونات نظام الاتصال عن بعد.[78]
- هجمة رفض الخدمة هي تلك التي تعرقل و تمنع خدمة تطبيق ما و جعلها أحيانا غير مفيدة للمستعملين الشرعيين ، باختصار هجمة رفض الخدمة تعمل على ازعاج الضحية ، و لكن أيضا يمكن أن تتسبب في خسائر كبرى.[79]

ب- طرق تنفيذ هجمة رفض الخدمة

رفض الخدمة يمكن أن يتسبب فيه العديد من العوامل إما تكون طبيعية أو مفتعلة.

العوامل الطبيعية : كالمشاكل المادية و المنطقية التي تحدث في مكونات النظام مثل :تسرب الموارد ، عطل في القرص الصلب ، الاستعمال السيئ ، انتهاء صلاحية برنامج....

[76] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p355
[77] **Michel Lafitte**, op cit , p85
[78] Ibid , p88.
[79] **Tom Gallaghe et autres**, « Chasser les failles de sécurité , les meilleures pratiques pour tester la sécurité de vos logiciels » , édition microsoft ,Janvier 2007, p375.

العوامل المفتعلة : و التي تكون بفعل المعتدين ، و من الطرق التي يستعملونها ما يلي:

استهلاك موارد النظام : الحواسب قدرتها لا تحمل إلا موارد محددة : قدرة الأقراص الصلبة ، مساحة الذاكرة ، قدرة عناصر الشبكة...[80] و عن طريق استهلاك المعتدي أكبر جزء ممكن من هذه الموارد فان هذا سيحدث خنق و قطع لعمل التطبيق[81] ، فتعبئة منطقة التخزين يؤدي إلى مرحلة يصبح لا يمكن استعمالها.

- **اجتياح النظم و الضغط عليها** :

– اجتياح خادم الشبكة : فاجتياح خادم الشبكة أو خادم الويب بطلبات خاطئة يثير عطل الشبكة[82]، فكل خادم لا يستطيع ضمان الخدمة إلا في نطاق محدد ، و الضغط بمعنى عدد الطلبات بوحدة الزمن يجب أن تبقى في إطار الحدود ما يمثل واحد من خصائص الخادم.[83]

– **اجتياح خادم الرسائل** : هذا النوع من التعدي يستعمل خادم الرسائل لموقع ما من أجل ارسال رسائل غالبا تكون إشهارية و غير مرغوب فيها لعدد كبير من الجهات عن طريق إخفاء هويته ، إلى غاية تعبئة البريد بالرسائل الإلكترونية ، و بالتالي تعطيل خدمة رسائل الموقع.[84]

- **فيروس bot**: هذا الفيروس لا يعمل سوى أنه ينتشر ، و لكن في ساعة محددة أو إشارة معطاة آلاف أو ملايين الآلات المصابة تتصل بنفس الخادم المستهدف و تثير انهياره.[85]

كما يطلق عليه اسم شبكة الروبوتات أو البوت نت (botnets) و يتمثل خطرها في سيطرة شخص أو مجموعة يعرف بالمتحكم (Master) ، على شبكات ضخمة من الأجهزة الحاسوبية ربما يبلغ عددها الآلاف بل حتى الملايين ، و يمكن لذلك المتحكم أن يطلب من تلك الأجهزة القيام في توقيت محدد عن طريق برنامج تحكم يطلق عليه برنامج السيطرة و التحكم بتنفيذ أوامر معينة لأغراض تجارية أو تخريبية ، و تتم كل هذه الأمور بشكل خفي و من الصعب جدا اكتشافها من مستخدمي الأجهزة.[86]

[80] **Eric Léopold, Serge Lhoste**, op cit , p56
[81] **Tom Gallagheret autres**, op cit , p376.
[82] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p354
[83] **André Vaucamps**, op cit , p14.
[84] **Robert Longeon ,Jean-luc Archimbaud**, op cit , p13.
[85] **André Vaucamps**, op cit , p14.
[86] **مأمون العزب** ،" أمن المعلومات في فضاءات انترنت الأشياء " ، مجلة التقدم العلمي ، العدد 99 ، مؤسسة الكويت للتقدم العلمي ، أكتوبر 2018 ، ص 14.

ت– تأثيرات هجمة رفض الخدمة

هجمة رفض الخدمة حتى و إن كانت لا تستطيع تدمير المعلومة أو الوصول إلى مناطق ممنوعة داخل نظام معلومات المؤسسة ، إلا أنها يمكن أن تؤدي إلى إغلاق موقع الويب ، فمثلا بالنسبة لمواقع التجارة الالكترونية ، هذه الهجمات هي جد ضارة ، لأن المستهلكين لا يمكنهم القيام بعملية الشراء بما أن الموقع خارج الخدمة[87] ، و كذلك إذا كان هناك مثلا موقع ويب لمزايدة إذا أصبح غير متاح بسبب هجمة رفض الخدمة فالموقع يمكن أن يضيّع جزء مهم من المداخيل[88].

و عليه فإن هذه الهجمة مضرة بالنسبة للمستعملين الذين يعتمدون على تطبيقات أو مواقع أو أنظمة عليها العمل باستمرارية ، و التي قد يؤدي تعطيلها و لو لمدة معينة إلى خسارة مداخيل ، خسارة سمعة ، تضييع زبائن ، تضييع مصالح...

4– التزوير أو التعديل

تزييف و تعديل المعطيات خلال الارسال بتدخل خبيث يحدث مشكل التكامل ، فالتكامل المضمون عن طريق بروتوكولات النقل (TCPمثلا) تضمن أن يكون جريان المعطيات المستقبلة مماثلة تماما لجريان المعطيات المرسلة[89]، و بالتدخل بينهما و تعديل الرسائل المرسلة لا تكون هذه الأخيرة نفسها هي المستقبلة ، أما التعديل في البرامج يجعلها تؤدي عملها بطريقة مختلفة تلبية لمصالح المهاجم.

ثالثا : التهديدات المادية

رغم أن موضوع البحث هو أمن المعلومات و التهديدات المعلوماتية إلا أنه من الضروري معرفة التهديدات المادية التي تمس أجهزة الاعلام الآلي ، لأن تهديد هذا الأخير يعني تهديد أمن المعلومة التي يحتويها ، و المساس بخصائص هذا الأمن التي هي الخصوصية ، التكامل ، و خصوصا التوافر. و من بين أهم التهديدات المادية نذكر:

[87] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p355
[88] **Tom Gallagher**, et autres,, op cit , p377
[89] **André Vaucamps**, op cit , p14.

1- السرقة

السرقة يمكن أن تستهدف الحواسب الآلية و التحاميل و كل ما يتعلق بأنظمة المعلومات ، إذ أن سرقة أجهزة الاعلام الآلي أصبحت عملية جد منتشرة ، و هذا بسبب صغر حجمها و خفتها مما يسهل عملية سرقتها.

فسرقة الجهاز لبيعه كون هذه الأجهزة ثمينة و تسيل لعاب اللصوص فهذا بحد ذاته مشكلة نظرا للخسارة المتمثلة في ثمن الجهاز ، و لكن المشكلة الحقيقية هي قيمة المعلومات التي يحملها الجهاز و التكاليف المتكبدة في خسارتها، و تتمثل هذه التكاليف في :[90]

- تكلفة تجميع المعلومات و انشاءها من مال و جهد و وقت.
- الخسائر المترتبة عن انتشار المعلومات.

و تشير إحدى الدراسات أن منظمة الضرائب الأمريكية فقدت 2332 جهاز من أجهزة الحاسب المحمول خلال ثلاث سنوات.[91]

2- الوصول و التدمير المادي

مجرد الوصول إلى الأجهزة المعلوماتية بحد ذاته خطر أمني ،كما يمكن للمهاجم تدمير إراديا التجهيزات و تخريبها.

3- الهندسة الاجتماعية

الهندسة الاجتماعية هي شكل من أشكال الاستحواذ غير الشرعي للمعلومات و الاحتيال الذي يستغل الثغرات البشرية و الاجتماعية للبنية المستهدفة من أجل الحصول على ممتلك ، خدمة أو معلومات.[92] و قد صنفتها GARTNER[93] سنة 2011 كأكبر خطر في العالم الرقمي للعقد المقبل.[94]

هذه التقنية تعتمد على التحكم و التلاعب بالأفراد للتمكن من آليات الأمن باعتبار أن العامل البشري هو الحلقة الضعيفة في نظام المعلومات مستغلين بذلك سذاجة و جهل الشخص.[95] فالهندسة الاجتماعية هي من أسهل

---

[90] **Eric Léopold, Serge Lhoste,** op cit , p34

[91] خالد الغثبر، مهندس القحطاني،مرجع سابق ،ص 184.

[92] **Pierre-Luc Réfalo** , « la sécurité numérique de l'entreprise « l'effet papillon du hacker » » , groupe Eyeolles , Paris, p49

[93] GARTNER : est une entreprise Américaine de conseil et de recherche dans le domaine technique.

[94] Ibid , p 49.

[95] **Philippe Atelin** , « Réseaux informatiques-notions fondamentales » , troisième édition , édition ENI , France , 2009 , p 314.

الطرق للحصول على المعلومات مقارنة بالطرق الأخرى التي ذكرناها ، فهي تعتمد على وسائل بسيطة و حيل و خداع ، و من بين طرق الحصول على المعلومات بالهندسة الاجتماعية ما يلي :

- التفتيش في النفايات:فسلاَّت المهملات غنية جدا بالأوراق التي تظهر أنها غير مهمة و لكنها تحمل كم هائل من المعلومات الاستراتيجية ، فقد تتم مثلا طباعة بريد مهم و رمي الورقة ، أو محاولات لكلمات مرور ...[96]
- سرقة الطبعات و الوثائق المنسية فوق المكاتب و آلات النسخ أو المنتشرة في الأماكن العامة للمنظمة.[97]
- الدخول للمؤسسة عن طريق تظاهر المهاجم أنه أحد الموظفين أو عمال النظافة أو الصيانة من أجل جمع ما يمكن من كلمات السر.
- خداع شخص و استغلال ضعفه من أجل الوصول إلى المعلومات.
- التظاهر بالسلطة.

و عليه من مميزات هذه الطريقة أنها سهلة و لا تتطلب وسائل تقنية لتنفيذها فهي تعتمد فقط على المناورة و الخدع النفسية، و المهاجم الذي يستعمل هذه الطريقة يحصل على الكثير من المعلومات المهمة دون لفت الانتباه.

الفرع الثاني : التهديدات الناتجة عن ثغرات أمنية

1- تعريف الثغرة الأمنية

تعرّف الثغرة الأمنية على أنها نقطة ضعف في تصميم أو تهيئة البرمجيات أو قواعد تخزين المعلومات أو الأجهزة التي تحفظ فيها المعلومات ، أو معدات أو برامج تشغيل الشبكات التي تمر المعلومات خلالها ، و نقاط الضعف هذه هي الثغرات التي يتسلل المهاجم من خلالها لإحداث الدمار الذي يريده .[98]

و تُعرّف أيضا أنها : ضعف في إجراءات الأمن ، مراقبة الأمن التقني أو إجراءات الاستغلال أو الادارة المستعملة داخل المؤسسة ، فهي تعتبر عموما ضعف في حماية النظام و الذي يمكن استغلاله من قبل تهديد.[99]

[96] **Pierre Mongin et Franc Tognini** , « petit manuel d'intelligence économique » ,2e édition , Ed Dunod , Paris,2015 ,p38

[97] Menaces sur les systèmes informatique « Guide N 65 », op cit , p14

[98] **خالد الغثبر، مهندس القحطاني**، أمن المعلومات بلغة ميسرة،مرجع سابق ،ص 24.

[99] **Jean –François Carpentier**,op cit , p23 , p31.

كما تعتبر الثغرة الأمنية عبارة عن فجوة أو ضعف على مستوى نظام المعلومات، و من الممكن استغلالها من طرف عناصر مهددة باستعمال مختلف طرق الهجوم.[100]

و عليه الثغرة الأمنية هي عبارة عن ضعف أو خطأ في نظام معين أو طريقة حماية معينة يتم استغلالها من قبل المهاجم لإحداث أضرار مختلفة.

2- أنواع الثغرات الأمنية

الثغرات الأمنية عديدة و متعددة، و لكي يتم تعدادها بصفة شاملة، و حسب عدة معايير و مدارس مثل : BS7799, EBIOS GMITS من الممكن تجميعها في ثلاث عائلات كالتالي : الثغرات الأمنية على المستوى التنظيمي(الادارة)، الثغرات الأمنية على المستوى المادي، الثغرات الأمنية على المستوى التكنولوجي [101]

أ- الثغرات الأمنية على المستوى التنظيمي

غياب التسيير الصحيح لأي نظام معلوماتي يمكن أن يعرضه بسرعة للخطر،و من بين الثغرات على هذا المستوى:

- نقص الموارد البشرية و الأفراد الأكفاء[102] في مجال تقنيات أمن المعلومات.
- عدم توفير التدريب المناسب للعاملين في مراكز المعلومات على استخدام برامج و تقنيات الوقاية من الاختراقات.
- عدم وضوح القواعد الواجب اتباعها ، و غياب التحكم في نظم المعلومات و الاتصال ، إذ يجب تكييف موارد بشرية خاصة بمراقبة أنظمة المعلومات و معالجة أي انحراف.[103]
- عدم التوافق بين السياسة الأمنية و المخاطر ، التقييم الحقيق للمخاطر الخالية قليلا ما يتحقق بطريقة صحيحة و عليه معايير الأمن المتخذة غالبا ما لا تتناسب مع المخاطر الموجودة و المتوقعة.[104]
- غياب المراقبة الدورية ، و غياب توثيقات الاجراءات المتخذة في المؤسسة.[105]

[100] Menaces sur les systèmes informatique « Guide N 65 », op cit , p20
[101] Vulnérabilités , fiche thématique 013 , CASES , Cyberworld Awareness and Security Enhancement Structure , Luxembourg , www.cases.lu
[102] **Jean –François Carpentier**,op cit , p26.
[103] Vulnérabilités , fiche thématique 013 , CASES ,op cit.
[104] Ibid.
[105] **Jean –François Carpentier**,op cit , p26.

– الفشل في إلزام المعنيين بتطبيق السياسة الأمنية:حتى و إن كانت إجراءات أمن نظم المعلومات موجودة ، غالبا ما أنها لا تصل أو لا تصل بشكل جيد للمستخدمين و المسيرين ما يزيد من احتمالية تعرض المؤسسة للخطر.

ب– الثغرات الأمنية على المستوى المادي

هذا النوع يتعلق بكل ضعف أو نقص على مستوى التجهيزات المادية ، و من بين الثغرات على هذا المستوى :

– نقص الموارد على مستوى التجهيزات مما يتسبب في انقطاع الخدمات و يكون لعدة أسباب :

- تقادم الأجهزة المخصصة لحفظ البيانات.
- الأعطال و التلف في أجهزة الاعلام الآلي بسبب الاستعمال التعسفي ، إضافة إلى التجهيزات السيئة أو التغييرات غير المرخصة.[106]
- ضعف تجهيزات الاعلام الآلي مما يجعلها دائما حساسة لمحيطها ، فأكبر أنظمة المعلومات تحتاج أن تعمل في ظل شروط حرارة و تكييف خاصة ، و عدم احترام هذه الشروط يمكن أن ينتج عنه أعطال كبيرة و استنزاف مبكر للأجهزة ، إضافة إلى حساسيتها لمخاطر الحرائق التي تتسبب في التدمير المباشر للآلات ، كما أن الارتفاع غير العادي لدرجات الحرارة و آثار التدخين و تسريبات المواد السائلة يمكن أن تكون نتائجه كارثية.[107]

– غياب تأمين و مراقبة الوصول إلى العناصر المادية : الوصول إلى قاعات الاعلام الآلي ، الأجهزة الموصولة أو عناصر أخرى يجب أن يكون محدود لتجنب التلاعب (غير) الارادي ، كما يمكن أن يتسبب ذلك في الضياع الكامل لقاعات الاعلام الآلي.[108]

– غياب تسيير الموارد و سوء استراتيجية حفظ المعطيات[109]، و يتمثل ذلك في[110]:

- الحماية السيئة لتحاميل التخزين التي غالبا ما تخزن في قاعات المعلوماتية ما يجعلها معرضة للأخطار.
- التسيير السيئ للموارد التي يجب أن تكون مراقبة عن قرب.
- غياب تسيير الأسلاك ما يسبب انقطاع تواصل متكرر.

[106] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p348
[107] **Eric Léopold, Serge Lhost**e, op cit , p33
[108] Vulnérabilités , fiche thématique 013 , CASES ,op cit.
[109] **Jean –François Carpentier**,op cit , p25.
[110] Vulnérabilités , fiche thématique 013 , CASES ,op cit.

ث- الثغرات الأمنية على المستوى التكنولوجي

و تتمثل غالبا في:

- **أخطاء البرمجة** : أخطاء البرمجة و الثغرات الأمنية على مستوى البرامج تسمح بالتعدي على النظام و الوصول إلى المعلومات السرية و بالتالي اختراق النظام ، مما يسمح بتنفيذ و شنّ مختلف الهجمات ، هذه الأخطاء تسبب ضياع انتاجية غير محددة ، فحسب NIST[111] لمديرية التجارة للولايات المتحدة فان أخطاء البرامج تكلف كل سنة كثيرا الاقتصاد الأمريكي.[112]

- **سوء إدارة المواقع** : القراصنة يبحثون بانتظام عن المواقع سيئة الادارة باستعمال مسح على الانترنت عن طريق تطبيقات تسمى " scan " ، هذه التطبيقات تكشف عن بعد كل محطات الشبكة المحلية و تفحص وجود " الطبعات القديمة " للبرامج الشبكية على هذه المحطات مع فجوات أمنية معروفة.[113]

- **استخدام عنوان انترنت دائم** : عندما تكون شبكة المؤسسة متصلة مع الانترنت ، فأنظمة معلوماتها تصبح أكثر حساسية للتدخلات الخارجية ، فالحواسب المتصلة دائما بالانترنت هي أكثر عرضة للتدخلات لأنها تستعمل عنوان انترنت دائم يسهل تعارفاتهم ، فعنوان انترنت دائم يهدي القراصنة هدف ثابت.[114]

- **سوء استخدام الرسائل الالكترونية** : الاستعمال المنتشر للبريد الالكتروني و الرسائل الفورية تزيد من حساسية نظم المعلومات ، فهذه الرسائل يمكن أن تكون معرّضة للقراءة من قبل دخلاء خلال ارسالها بالانترنت.[115]

- **تعقد القواعد على الجدران النارية و المحركات** : وضع التصفيات و قواعد الوصول بالطلب تجعل رؤية الجميع شبه مستحيلة.[116]

- **عدم وجود تحديثات لأنظمة التشغيل و التصحيحات** ، و عدم وجود مراقبة كافية للبرامج الخبيثة[117]، إضافة إلى اهمال الاهتمام بطرق الحماية من الاختراق ، و اهمال تحديث برامج مكافحة الفيروسات.

و حتى و إن وجدت اليوم طرق تسمح بالحد من مخاطر الأخطاء إلا أنه يمكن اعتبار أنه لا يوجد برامج معفاة من الأخطاء ، و التي تكون نتائجها مختلفة سواء مشاكل خصوصية ، تكامل أو مشاكل توافر.[118]

---

[111] NIST : National Institute of Standard and Technology.
[112] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p357
[113] **Robert Longeon ,Jean-luc Archimbaud** , op cit , p12.
[114] **Kenneth Laudon et Jane Laudon**, 2006, op cit , p349
[115] Ibid , p 350.
[116] Vulnérabilités , fiche thématique 013 , CASES ,op cit.
[117] **Jean –François Carpentier**,op cit , p26.

فمثلا في 2 ماي 2000 ، إعصار عالمي انتشر من الفلبين في شكل بريد جذاب " **أحبكم**" يحث على فتح ملف مرافق ، الرسالة تتضمن فيروس و تحديدا عبارة عن دودة مهمتها الأساسية هي إعادة إرسال الرسالة الأصلية إلى كل دفتر عناوين المستلم ، مستغلة ثغرة في outlook أصابت 3 ملايين حاسب في 4 أيام فقط، و هذا ما سمح بتحديث أنظمة الرسائل قبل بداية اليوم.[119]

بظهور الاعلام الآلي ظهرت التهديدات المعلوماتية التي تختلف مصادرها سواء الطبيعية أو البشرية ، الداخلية أو الخارجية و دوافع ارتكابها التي تكون إما لأسباب عامة أو لأسباب شخصية إضافة إلى طرق تنفيذها المتعددة ، لذا على المؤسسة التيقظ و الانتباه لمختلف هذه النقاط و دراستها جيدا حسب نوعية محيطها من أجل القدرة على حماية نفسها ، إذ أن العالم اليوم يدفع ثمنا باهظا بسبب الهجمات الالكترونية كل عام ، حيث تكلف الجرائم الالكترونية اقتصاد العالم نحو 575 بليون دولار سنويا ، و عليه فان الأمر ليس بالهين أو الهامشي بل أصبح أولوية.

المبحث الثاني : وسائل تحقيق أمن المعلومات

تحقيق الأمن المعلوماتي يتطلب منظومة حماية متكاملة من كل الجوانب التي يمكن أن تمس المعلومة، و من خلال المبحث الأول سيتم التطرق لكل جوانب التهديدات المعلوماتية ، لكن معرفة التهديد لا يكفي ، و إنما هو مجرد قاعدة لبناء أعمدة الحماية ، و تحقيق الحماية و الأمن للمعلومات و الأنظمة التي تحملها يتطلب طرق و وسائل متعددة، و من كل الجوانب الممكنة لتكون الحماية فعالة، و حسب الاطلاع على عديد المراجع استنتجنا أن أفضل تحقيق للأمن المعلوماتي يعتمد على ثلاث أنواع من الوسائل : وسائل الحماية البرمجية و التي يكون الاعتماد فيها على كل أنواع البرامج المطبقة على الحواسب و التي تضمن سرية التعاملات و منع التدخلات غير الشرعية ، و وسائل الحماية المادية التي هي عبارة عن كل الاجراءات الأمنية المادية من أمن موقع المنظمة و تجهيزات نظم المعلومات و حماية تحركات الأفراد،و أخيرا حقوق الملكية الفكرية و التي من خلالها تتحقق الحماية القانونية للممتلكات غير المادية مع التركيز على المصنفات المعلوماتية محل الحماية.

[118] **Eric Léopold, Serge Lhoste**, op cit , p33

[119] **Pierre-Luc REFALO** , « la sécurité numérique de l'entreprise « l'effet papillon du hacker » » , Groupe EYROLLES , Paris , 2013 , p43.

المطلب الأول : الحماية البرمجية للمعلومات و أنظمة المعلومات

الحماية البرمجية تتمثل في استخدام كل البرامج المتاحة و التي توفر حماية للمعلومات المنتقلة عبر الشبكات أو المخزنة في الحواسيب ، سواء عن طريق منع الدخول أو التشفير أو مكافحة الفيروس... ، و تعتبر الحماية البرمجية أهم و أول خطوة في تحقيق الأمن ، و من خلال هذا المطلب سنتطرق لكل طريقة و كل برنامج على حده و تبيين أهميته و الطرق المثلى لاستخدامه.

الفرع الأول : الجدار الناري Pare-feux

يعود مصطلح الجدار الناري إلى أكثر من قرن ، حيث أن العديد من البيوت بنيت من طوب موضوع في الحائط بشكل يوقف النيران المحتملة ، و سمي هذا الطوب ب " **الحائط الناري** "، أما تقنية الجدار الناري فقد ظهرت في أواخر الثمانينات عندما كانت الانترنت تقنية جديدة نوعا ما من حيث الاستخدام العالمي ، الفكرة الأساسية ظهرت استجابة لعدد من الاختراقات الأمنية الرئيسية لشبكة الانترنت في أواخر الثمانينات.[120]

و يمكن تعريف الجدار الناري على أنه : " كل آلة موضوعة في شبكة معلوماتية و قادرة على تحقيق غربلة على التواصلات الداخلة و الخارجة ".[121]

و يعرف أيضا أنه : " جهاز أو برنامج يفصل بين المناطق الموثوق بها في شبكات الحاسوب ، و يكون أداة مخصصة أو برنامج على جهاز حاسوب آخر الذي بدوره يقوم بمراقبة العمليات التي تمر بالشبكة و يرفض أو يقرر أحقية المرور ضمن قواعد معينة ".[122]

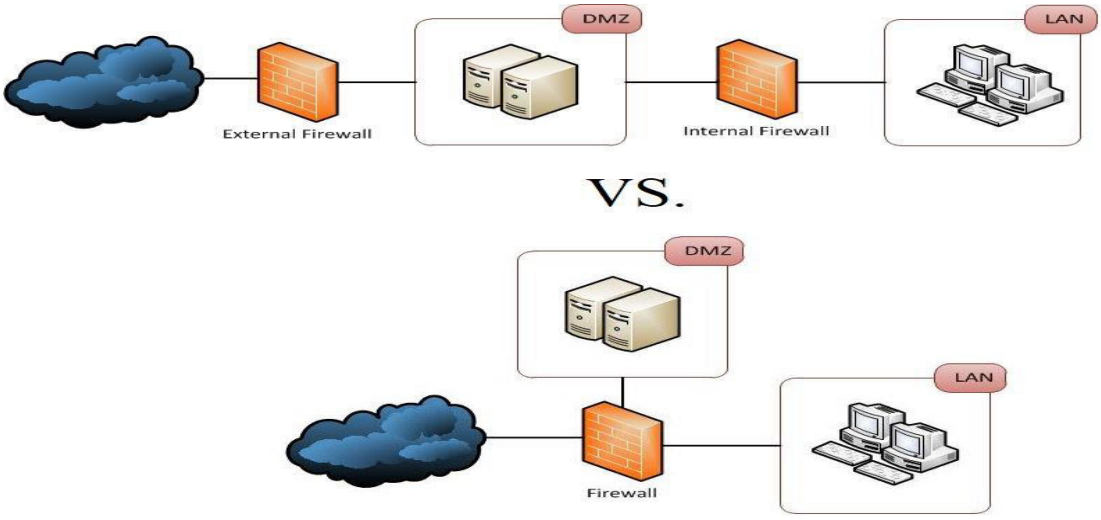
و عليه نستنتج أن الجدار الناري و كأنه حارس أو شرطي ينظم حركة مرور المعلومات داخل الشبكة المعلوماتية ، فهو يتحقق ممن له صلاحية الدخول و الخروج بين الشبكات المتعددة ، و التي تتمثل في الشبكة الخارجية " الانترنت " و هي منطقة عديمة الثقة و الشبكة الداخلية و هي منطقة عالية الثقة ، و هناك منطقة DMZ " منطقة منزوعة السلاح " و هي متوسطة الثقة و تتواجد بين الشبكة الخارجية و الشبكة الداخلية.

[120] أسامة سمير حسين ، الاحتيال الالكتروني ، مرجع سابق ، ص 193.

[121] **Eric Léopold, Serge Lhoste**, op cit , p85

[122] أسامة سمير حسين ، الاحتيال الالكتروني ، مرجع سابق ، ص 192.

الشكل (2.2): مكانة الجدار الناري و المنطقة منزوعة السلاح



Source : Layered DMZ Network Security Architecture Design , February 2018 , voir: https://www.sunnyhoi.com/layered-dmz-network-security-architecture-design/

فالجدار الناري يعمل على اختبار بطاقات تعريف كل مستعمل قبل الموافقة على دخوله الشبكة ، فهو يراجع و يدقق الأسماء ، عناوين بروتوكولات الانترنت (IP) ، التطبيقات و الخواص الأخرى لحركة المرور الداخلة ، و يقارن هذه المعلومات مع قواعد الدخول التي برمجها مدير الشبكة في النظام ، و هو يمنع كل الاتصالات غير المسموح لها التي تريد الدخول أو الخروج من الشبكة سامحا للمنظمة بتطبيق سياسة أمن على حركة المرور التي تدور بين شبكتها و شبكات أخرى غير آمنة.[123]

و لكن من دون الاعداد الجيد للجدار الناري يصبح عديم الفائدة ، و هناك طريقتين في إعداده :

- **السماح أولا** : بمعنى أنه مسموح لكل شيء المرور إلا ما تم منعه بشكل تخصيصي ، و هي طريقة غير آمنة تجعل من الجدار الناري غير فعال.
- **المنع أولا** : أي كل شيء ممنوع مروره إلا ما تم السماح له بشكل تخصيصي ، و هي الطريقة المثالية لتحقيق الأمن و جعل الجدار الناري فعالا.

أما بالنسبة لأشكال الجدار الناري ، فهي تأتي على نوعين :[124]

[123] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p372
[124] **Jean-Marc Royer**, op cit , p61.

- **برامج** : و هنا يكون الجدار الناري عبارة عن برنامج يتم تنزيله على الحاسب الخادم الذي يحتوي على الأقل على بطاقتين أو مخرجين لتوصيل الشبكة ، و يكون هذا الحاسب مسخرا للاستعمال الخاص بالجدار الناري ، و يُتجنب استعمالها لتطبيقات أخرى.
- **أجهزة** : و هو عبارة عن علبة أو صندوق مزود بواصلين اثرنت ، هاته العلبة تضم في نفس الوقت حاسب و برنامج جدار ناري ، و بالتالي لا يتم الانشغال بتركيب البرنامج لأنه قد تم شراء زوج من الجهاز و البرنامج.

و لتحقيق فعالية الجدار الناري يتم الاعتماد على أربعة مبادئ :[125]

- أن يكون بسيط : كلما كانت طريقة وضعه بسيطة كلما كان الجدار الناري مؤمّن و مُدار بطريقة سهلة.
- استعمال أجهزة جد ملائمة مع المحيط و مع وظيفته الأساسية : في أغلب الأحيان الجدار الناري الهجين هو أفضل الخيارات لأنه موجه لهذه الوظيفة.
- خلق دفاع في العمق على عدة طبقات بدلا من واحدة : إذا كان ضروري يتم استعمال عدة جدران نارية ، محركات تستطيع تحقيق مراقبة الدخول أو الغربلة أو عدة خوادم مجهزة بجدار ناري حسب حاجة الحماية.
- التفكير الجيد في التهديدات الداخلية : الدخيل الذي يستطيع الدخول بطريقة أو بأخرى للشبكة الداخلية المحمية وراء الجدار الناري له كل التسهيلات للوصول لكل الشبكة.

الفرع الثاني : برامج مكافحة الفيروسات Anti virus

أصبحت الفيروسات اليوم تشكل شبحا يهدد الحواسيب التي تشكل نواة أنظمة المعلومات ، و برامج مكافحة الفيروسات هو السلاح الفعال لمواجهتها إذا تم استعمالها بالطريقة المناسبة.

فبرنامج مكافحة الفيروس يتحقق من الأقراص و الأنظمة من أجل تحديد تواجد فيروسات معلوماتية ، هذه البرامج تستطيع عموما تنظيف المنطقة المصابة ، فمعظم برامج مكافحة الفيروسات تكون فعالة فقط مع الفيروسات المعروفة وقت وضع البرنامج ، لذا و من أجل أن يبقى البرنامج فعال يجب أن يُحدّث باستمرار.[126]

و لتكون طريقة عمل البرامج في البحث عن قطع الرموز الخبيثة و التي هي الفيروسات جد فعالة يجب توافر شرطين :[127]

[125] **Jean –François Carpentier**,op cit , p47.
[126] **Kenneth Laudon et Jane Laudon** , 2006, op cit , p373

- **إمضاء الفيروس** : بمعنى قطعة رمز الفيروس يجب أن تكون معروفة من قبل برنامج مكافحة الفيروس ، و لكن من الصعب جدا المعرفة الأوتوماتيكية للخواص التخريبية و الجانب الهدام لأي برنامج لأن وظائفه الحقيقية لا تظهر إلا عند التنفيذ.

- **الإمضاء يجب أن يكون ثابت** : و هنا نفهم مشكل الفيروس متعدد الأشكال الذي يقدم في حالتين مختلفتين رموز جد مختلفة ، لذا يجب أن تُحدّث مكتبة امضاءات الفيروسات بانتظام من أجل السماح بإدماجها ، و الاكتشافات اليوم أظهرت أن هناك برامج ذكية تعفي من كل تحديث.

و عليه فإن برامج مكافحة الفيروس مكلفة بالتحليل المستمر للحاسب للبحث عن فيروس قد تم تعريفه مسبقا أو عن طريق إمضاءه، و لكن اليوم أصبحت هذه البرامج أكثر تطورا ، و تحتوي على محركات تحليل ارشادية و هذا يعني أنه يبحث على تحديد كل تصرف غير عادي للآلة.[128] و عليه فان البحث الارشادي عن طريق هذه المحركات لا يعتمد على المعرفة الخاصة لمجموع المتغيرات لنفس الفيروس بل على بنية الملفات المحللة و على وجود عدد معتبر من التدخلات المهمة لمجموعة عائلة فيروسية ، و أصبحت هذه الطريقة موثوق بها رغم الانذارات الخاطئة التي تطلقها أحيانا.[129]

أظهرت دراسات في ديسمبر 2007 أن فعالية برامج مكافحة الفيروسات قلت كثيرا عما كانت عليه منذ سنوات وخصوصا ضد الهجمات المجهولة ، و تضخمت المشكلة بفعل تغير أهداف مصممي الفيروسات ، من قبل كان الهدف التدمير و كان مصممي الفيروسات هواة ، و لكن الفيروسات الحديثة غالبا ما تكون مصممة من قبل محترفين و تمولهم منظمات اجرامية ليس في مصلحتهم جعل الفيروسات أو برمجيات الجريمة واضحة ، و إذا كان المستخدم المصاب لديه منتج مكافحة الفيروسات قليل الفعالية و الذي يقول أن الحاسب نظيف ، قد لا يكتشف الفيروس.[130] لأنه من الضروري التيقن أنه ليس لمجرد عدم وجود أي اشعارات بإصابة الحاسب أنه سليم، لا يوجد شبكة سليمة 100% لأنه لا يوجد أي مكافح فيروسات يحمي 100% لذا بات لزاما على المؤسسات التفكير في منظومة حماية متكاملة و برامج حماية مرافقة لهذا البرنامج لكي يعطي مفعوله.[131]

---

[127] **Eric Léopold, Serge Lhoste** , op cit , pp67-68.

[128] **Tanguy HUGUES**, « protéger mon ordinateur : manuel de sécurité informatique » , 1er édition , édition Lulu , 2009 , p23.

[129] Les virus informatique, CLUSIF , 2005 , op cit, 39.

[130] أسامة سمير حسين ، مرجع سابق ، ص ص 187-188.

[131] **Nicolas Moinet** , op.cit , p 121.

الفرع الثالث : التشفير Chiffrement

تاريخ التشفير قديم فقد استعمله " **سيزار** " امبراطور الرومان من أجل ضمان سرية الرسائل ، و في ذلك الوقت الرسائل السرية تستعمل تقنية أساسية في حلول المراسلة بين الحروف : A تصبح D ، B تصبح T....و عند عكس المدخلات نجد الرسالة الحقيقية ، و الآن مع تطور الرياضيات و الجبر خاصة سمح بتجاوز التطبيق الوحيد للتشفير إلى تشفير المعلومة بفتح إمكانات الإمضاء و المصادقة على تكامل الرسائل المرسلة.[132]

و قديما كان التشفير يعتبر سلاح ثوري حتى سنة 1999 ، و اليوم حتى و إن كانت التطبيقات العسكرية لازالت متواجدة ، لكن التشفير بدأ يتحول تدريجيا من كونه علم الأسرار إلى علم الثقة بفعل ظهور تطبيقات جديدة خاصة تطور شبكة الانترنت و التجارة الالكترونية مما خلق تحدّ كبير و هو القدرة على العثور على أدوات تسمح بالتواصل عن بعد بطريقة مؤمّنة.[133]

و من تعريفات التشفير ما يلي :

- " فن التشفير هو فن حماية المعلومة عن طريق مثلا تحويلها إلى معلومات سرية عن طريق تعليمها باستعمال السر و هو المفتاح ، و فن فك الشفرات هو مجموع الإجراءات المتخذة من أجل مهاجمة الإجراءات المتخذة في عملية التشفير ."[134]
- "هو مجموع التقنيات التي تهدف إلى تحويل بفعل اتفاقيات سرية معلومات أو إشارات واضحة إلى معلومات أو إشارات غير واضحة من أجل تحقيق الفرضية المعاكسة عن طريق وسائل مادية أو برامج متخصصة لذلك".[135]
- " هو الاعتماد على خوارزمية من أجل تحويل المعطيات الواضحة إلى معطيات مشفرة من أجل جعلها غير واضحة لشخص دخيل "[136] ، و الهدف من التشفير هو جعل كل الملفات الرقمية الموجودة على التحاميل غير صالحة الاستعمال لمن لا يملك مفتاح الرمز[137] .

---

[132] **Eric Léopold, Serge Lhoste**, op cit , p75
[133] **Alain Yger , Jacques-Arthur Well** , Mathématique L3-Mathématique appliquées ,ED Pearson, France , 2009, p435
[134] Ibid , p435.
[135] **Eric Léopold**, op cit , p72
[136] **Arnaud Pelletier et Patrick Cuenot** , « Intelligence Economique ,mode d'emploi –Maitrisez l'information stratégique de votre entreprise » , édition Pearson , France ,2003 , p 35.
[137] Ibid , p35.

يمكن استنتاج مما سبق أن التشفير هو عبارة عن استخدام تقنيات أو برامج عملها هو تغيير شكل و مظهر المعلومات من معلومات واضحة يسهل فهمها إلى معلومات سرية يصعب فهمها ، و ذلك بالاعتماد على :

- خوارزمية أو صيغة التشفير : و هي الصيغة الرياضية المطبقة على المعلومات المراد تشفيرها.
- المفتاح التشفيري : و هو السر أو الأداة المستعملة في تشفير أو فك شفرة المحتوى.

و التشفير بالنسبة للمعلومات المنتقلة عبر الشبكة بكل مستوياتها (أدنى ، متوسط ، أعلى) هو عبارة عن حماية ضد تهديد التصنت ، فبما أنه لا يمكن منع الاعتراض و منع التصنت الاحتيالي للرسائل بين المرسل و المستقبل فالحل هو التشفير ، و بالتالي ضمان سرية التبادلات[138] ، أما بالنسبة للمعلومات السرية المخزنة فعلى الملف الذي يحويها أن يُشفَّر[139].

و من أنواع التشفير نجد :

- **التشفير المتماثل**

هذه الطريقة قديمة و جدّ مستعملة، تعتمد على مفتاح واحد فقط الذي يعتبر ضروري لعملية التشفير و فك التشفير و يجب أن يبقى سري خصوصا عند انتقاله بين المرسل و المستقبل، إذ تتم عملية التبادل قبل التواصل[140]

الشكل (2.3) : التشفير المتماثل

المصدر : التشفير–وانواعه https://mustafasadiq0.com/2014/09/30/

[138] **André Vaucamps**,op cit , p14.
[139] **Philippe Atelin** , op cit , p327.
[140] Ibid , pp 327-328.

- **التشفير غير المتماثل**

و يسمى أيضا ب " التشفير بالمفتاح العام " ، و الذي ظهر سنة 1976 عن طريق Whitfield Diffie et Martin Hellman و من خلاله تم كسر مقاربة التشفير المتماثل عن طريق الخروج من مبدأ تواجد نفس المفتاح المشترك لشخصين إلى الاعتماد على زوج مفاتيح (biclé) مرتبطين رياضيا : مفتاح عام متاح للجميع و الذي يسمح بتشفير رسالة ، و مفتاح خاص (سري) يسمح بفك شفرة الرسائل المشفرة بالمفتاح العام المشترك[141] .

الشكل (2.4) : التشفير غير المتماثل

المصدر : **التشفير**-وانواعه /https://mustafasadiq0.com/2014/09/30/

و عليه التشفير وسيلة لحماية سرية المعلومات ، فلا يطلع عليها من ليس مخول بذلك ، و يوجد عدد كبير من البرامج و المعدات التي تقدم خدمة التشفير و هي في متناول المستخدم و استخدامها لا يتطلب معرفة عميقة بتقنيات المعلومات ، و توفر قدرا معقولا من الحماية ضد المهاجمين العاديين.[142]

الفرع الرابع : مراقبة الدخول وأنظمة كشف التدخل

أولا : مراقبة الدخول (Contrôle d'accès)

مراقبة الدخول هي كل السياسات و الإجراءات المتخذة من قبل مؤسسة من أجل ايقاف أو إعاقة الدخول للأنظمة من قبل أشخاص ممنوعين في الداخل و الخارج ، و للاستفادة من الدخول على الشخص أن يُسمح له و بالتالي عليه أن يُعرَّف ، إذن الدخول إلى النظام يتطلب التعريف بالهوية + التحقق من الهوية.

[141] **Alain Yger , Jacques-Arthur Well** , op cit ,p 435.

[142] خالد الغثبر، مهندس القحطاني ، مرجع سابق ،ص 120.

أ– التعريف بالهوية

آلية التعريف ترتكز على معرفة عنوان IP ، و هي لا تسمح لأي مقر أو مستعمل بعبور الجدار الناري في حين آلية التحقق من الهوية هي التي تسمح بذلك.[143]

ب– التحقق من الهوية

التحقق من الهوية هي القدرة على التحقق من أن الشخص هو نفسه الذي يجب أن يكون.[144]

بمعنى هي عبارة عن عملية التأكد من أن الشخص الذي يحاول الدخول للنظام مخول لذلك أولا ، و إذا كان مخول ما هي حدود صلاحيته ، جزئية أو كلية ، و هل له صلاحية القراءة فقط ، أو التعديل ، او الحذف...

و عليه فان هذه الآلية تسمح لمدراء النظام بمعرفة أي مستخدم أو مجموعة مستخدمين لهم حق عبور الجدار الناري للوصول إلى المعطيات ، و بالتالي فهي تسمح بضمان هوية المستخدم الذي قام بالطلب ، و على هذا الأساس يكون السماح بالمرور أو لا.[145]

و يكون التحقق من الهوية من خلال 4 اشكال :[146]

- "ما أعرفه " : مثل كلمة مرور ، و التي تعتبر الوسيلة الأكثر استعمالا للتحقق من الهوية.
- " ما أملك " : تحميل مادي.
- " ما لدي " : اختبار خصائص البشرية.
- " ما أعرف عمله " : مثل إمضاء يدوي (مع وجود شاشة كتابة).

و لعل التحقق البيومتري هو أفضل وسيلة ، فهو تكنولوجيا جديدة تستعمل خطوط هيئة كل شخص ، فهي تقارن خصائص الشخص مثل بصمة الأصابع ، ملامح الوجه أو صورة قدحية العين مع قاعدة البيانات المخزنة

[143] **Philippe Mathon et Frédéric Esnouf** , « ISA server 2004 : protégez votre système d'information » , éditions ENI , France , 2005 , p 140.
[144] **Kenneth Laudon et Jane Laudon , Eric Fimbel , Serge Costa** , « Management des systèmes d'information » , édition Pearson , 11éme édition , 2010 , p317.
[145] **Philippe Mathon et Frédéric Esnouf**, op cit , p 140.
[146] **Philippe Atelin** , op cit , p320.

في الذاكرة و التي تحوي مجموع هذه الخصائص، و بعدها يوضح النظام إذا كان هناك خلاف بين هذه الخصائص و بين قاعدة البيانات ، و إذا كان موافق يتم السماح بالدخول ، و لكن هذه الطريقة مكلفة.[147]

ثانيا : أنظمة كشف التدخل IDS Intrusion Detection Systems

أنظمة كشف التدخل هي عبارة عن أدوات مراقبة مستمرة موضوعة في أماكن أو نقاط الدخول الأكثر حساسية لشبكات المؤسسة من أجل كشف التدخلات ، و من ثم يطلق النظام إنذار في وقت حقيقي في حال حدث مريب أو غير عادي.[148]

و تعرف أيضا على أنها مكونات لهندسة تسمح في مكان محدد بتحديد طلبات الشبكة المعتبرة كمحاولات تدخل، و هي أنظمة معقدة الضبط تتطلب معرفة شاملة بالتدفقات المسموح لها بالعبور على منطقة الشبكة ، و ليست كل محاولة تدخل مكتشفة من خلال أنظمة كشف التدخل هي بالضرورة هجمة على الشبكة.[149]

و تعتبر أدوات كشف التدخل مكملة لوظائف الجدران النارية عن طريق مراقبة هوية الطلبات التي تدور داخل الشبكة ، هذه الأدوات تعمل أيضا على اكتشاف الطلبات سيئة النية و الاعلام عنها و في العديد من الحالات تستعمل من أجل منع الدخول غير المسموح أو التدخلات داخل الشبكة.[150]

و يوجد نوعين من أنظمة كشف التدخل :[151]

- **أنظمة كشف التدخل المرتكز على المضيف** : يجب أن يُركب على كل آلة يجب حمايتها ، فهو في العموم مُدمج مع نظام الاستغلال الذي يحميها ، هذا النوع من أنظمة كشف التدخل مخصص لتحديد التهديدات ذات مستوى عالي من الحماية.
- **نظام كشف التدخل المرتكز على الشبكة** : هو موضوع كمحلل ذكي للبروتوكول، يراقب حركة مرور الشبكة على المستوى المادي، و يعتبر هذا النظام نظريا أكثر فعالية من السابق لأنه نظام واحد يمكن أن يراقب عدة موارد.

[147] **Kenneth Laudon et Jane Laudon ,** 2006, op cit , p371
[148] Ibid , p373.
[149] **Philippe Mathon et Frédéric Esnouf** , op cit , p 178.
[150] **Jean –François Carpentier**, op cit , p78.
[151] Ibid , p79.

و عليه فإن أنظمة كشف التدخل تستطيع مراقبة نشاط الشبكة ، مراقبة الحزم ، تعريف امضاءات الهجمات الالكترونية المعروفة و التعديات من أجل إنذار الشخص المعني في حال اكتشاف مثل هذه النشاطات ، فتكنولوجيا كشف التدخل تتيح للمنظمة معرفة صاحب التدخل و تكرار هجماته.[152]

الفرع الخامس : الشبكة الافتراضية الخاصة VPN Virtuel Private Network

الشبكة الافتراضية الخاصة هي تكنولوجيا حديثة نسبيا على مستوى سوق الحماية المعلوماتية ، تقدم تقنيات جديدة و متطورة في تحسين مستوى الأمن ، و عن طريق هذه الشبكة يتم حماية تبادل المعطيات بين موقعين متباعدين على الأقل ، ضامنة بذلك هويات المرسل و المستقبل ، إضافة إلى ضمان عدم انتهاك المعطيات و تكاملها و تأكيد عملية ارسالها و استقبالها.[153]

شبكة VPN تشفر حركة مرور الشبكة الحساسة عن طريق خوارزمية تشفير قوية و معروفة ، و تفرض تحقق من الهوية قوي عن طريق استعمال نظام بعاملين : اسم مستعمل و كلمة مرور.

عمل هذه الشبكة يتم من خلال خادم VPN الذي يعتبر الآلة التي تمثل مقر المراقبة داخل المؤسسة و الذي يجب أن يكون موضوع على الشبكة في منطقة DMZ[154] المخصصة ، و بالتالي يكون محمي بقواعد الجدار الناري ، فهذه الشبكة تعمل مرتبطة مع الجدار الناري [155]، و يمكن ايجادها على ثلاث أشكال :[156]

- تكون كخدمة جدار ناري.
- نظام مستقل موضوع قبل الجدار الناري.
- نظام مستقل موضوع خلف الجدار الناري.

[152] **Pierre E.Edorh** , « Sécurisation globalisée des systémes d'information de gestion , 4-Modules-T97 » , 2006 , p214.
[153] Ibid , p 208.
[154] DMZ : هي محيط تحت شبكي متموقع بين شبكة داخلية موثوقة و شبكة خارجية غير آمنة .
[155] **Jean –François Carpentier** ,op cit , p72.
[156] Ibid , p72

الفرع السادس : التحديثات

التحديثات هي عملية ضرورية لفعالية البرامج على المؤسسة الانتباه إلى أهميتها و الخطورة الناتجة عن اهمالها. و نجد نوعين من التحديثات : التحديث التلقائي أو الآلي و يكون ذلك عن طريق قيام البرنامج المثبت في الحاسوب الاتصال بالشركة الأم للتحقق من وجود أي تحديثات، فإن وُجد أي منها بادر البرنامج بتنبيه المستخدم إلى ذلك، و يتطلب هذا اتصال الحاسوب بالانترنت، أما الثاني فهو التحديث اليدوي و الذي يكون بمبادرة من المستخدم الذي عليه الذهاب إلى الموقع الالكتروني للشركة المصنعة للبرامج و يقوم بتحميل التحديثات اللازمة.[157]

و تمس التحديثات كل البرامج الحساسة كنظام التشغيل ، متصفح الانترنت ، برامج مكافحة الفيروسات ، الجدران النارية...

فمثلا إذا لم يتم تحديث نظام التشغيل ضد الأخطاء و الثغرات الأمنية بعد تركيب جدار ناري يمكن لأي مقرصن نشيط التنبه و استغلال الثغرة قبل تنبه المؤسسة و مهما كان نوع الجدار الناري.[158]

كما أن الإجراءات الآلية للتحديث الدوري لبرامج مكافحة الفيروس الموضوعة من قبل مصمم البرنامج يسمح بتوليد ردة فعل قوية ضد التهديدات الحالية.[159]

تعتبر الحمايات البرمجية المقدمة ضرورية لكل مؤسسة ترتكز في مجال عملها على الأنظمة الآلية ، و لا يعني تركيب أحدها الاستغناء عن الآخر ، بل من الضروري اعتمادها مجتمعة ، لأن لكل نوع منها دور مختلف عن الآخر .

المطلب الثاني : الحماية المادية لممتلكات المؤسسة المادية (الأمن المادي)

تحقيق الأمن المعلوماتي لا يكون بحماية المعلومات داخل الحواسب فقط ، بل من الضروري تحقيق الأمن الخارجي و المادي للمنظمة و موقع المنظمة و التجهيزات التي تضمها ، فالتهديدات المادية التي تتعرض لها هذه الأخيرة هي الأخطر من بين أنواع التهديدات إذ تدمر كل شيء و لا تترك مجالا للإصلاح ، لذا لا يجب التغافل أبدا عن الحماية المادية لما لها من أهمية لا تقل عن أنواع الحماية الأخرى.

[157] خالد الغثبر، مهندس القحطاني ، مرجع سابق ،ص ص 99-100.

[158] **Pierre E.Edorh** , op cit , p213.

[159] Les virus informatique, CLUSIF , 2005 , op cit, 35.

الفرع الأول : أمن موقع المنظمة

أمن المنظمة يعني تحقيق الأمن المادي لموقع المنظمة و السيطرة الخارجية للبناية و حمايتها من كل تدخل طبيعي أو متعمد ، و هذا يعتبر كخطوة استباقية لضمان و حماية نشاط المؤسسة و استمرارها و يتحقق ذلك من خلال عدة إجراءات :

- **الاختيار الأمثل لموقع المنظمة** : فالمؤسسة التي تقع في محيط أو منطقة مدنية و قريبة من الطريق العام ، و تعم فيها الحركة ليلا و تستفيد من الإضاءة العمومية هي أقل عرضة للمخاطر من تلك الموجودة في منطقة معزولة أو منطقة ريفية يسودها الظلام منذ غروب الشمس.[160]
- **تحديد نطاق المؤسسة** : يجب تحديد موقع نشاط المؤسسة باستعمال دلالات ظاهرة.
- **تقسيم المواقع الواجب حمايتها** : إذ يجب ترتيب المناطق الواجب حمايتها و تكييف معايير الحماية حسب حاجة كل منطقة[161]، بوضع آليات الحماية و أنظمة الكشف بالداخل و الخارج بين المستخدمين المسؤولين[162] ، و يكون هذا عن طريق مسؤول أمن أنظمة المعلومات و يكون لكل منطقة أمن خاص و شروط دخول محددة.[163]
- **تشييد آليات منع الدخول** : و يكون عن طريق :

– إحاطة الموقع : فوضع سور أو سياج للموقع يمنع الاقتراب من الموقع يعتبر أول حاجز مادي يحمي من التدخلات .[164]

– وضع الأبواب المغلقة بالرموز أو الأبواب الدوارة[165]، و يمكن استعمال منطقة خاصة بالنباتات كحاجز طبيعي إذا كان الموقع يسمح.[166]

– تركيب أجهزة إنذار في حال التدخل غير المسموح[167] أو في المناطق التي تضم تجهيزات حساسة للسرقة.

---

[160] **Nicolas Moinet** , « la boite à outils de la sécurité économique », ED Dunod , Paris , 2015 , p19.
[161] La sécurité économique au quotidien en 22 fiches thématiques , Délégation interministérielle à l'intelligence économique , Avril 2014 , Fiche 4.
[162] **Eric Delbecque** , op cit , p 95.
[163] Politique de sécurité des systèmes d'information de l'état , version 1.0 , Agence National de la Sécurité des Systèmes d'Information , Paris , 2014 , p20.
[164] **Nicolas Moinet**, op cit , p 19.
[165] **Eric Delbecque** , Jean-Renaud Fayol, op cit , p 95.
[166] La sécurité économique au quotidien en 22 fiches thématiques, op cit , fiche 4.
[167] Sécurité Economique « les bonnes pratiques pour votre entreprise », Comité Opérationnel Défensif de l'Intelligence Economique de Lorraine , DRIRE Lorraine , p05.

- الإضاءة الأوتوماتيكية .[168]
- المراقبة المستمرة للبناية عن طريق الحراس 24/24 ساعة ، 7 أيام / 7 أيام طول السنة.[169]
- إغلاق حظيرة السيارات التي توصل إلى البنايات كل مساء على الساعة التاسعة مساءا و في الإجازات. [170]

- **مراقبة الدخول المادي** : الدخول الى المناطق الداخلية (المصرح بها فقط لعمال مركز المعلوماتية أو أشخاص مرافقين) يجب أن يُحدد ضمن آليات مراقبة الدخول المادية عن طريق استخدام وسائل تسمح بتعريف و ضمان هوية الشخص[171]، و بالنسبة للمحلات الحساسة كالمخبر و قاعات أجهزة الاعلام الآلي... الدخول يكون مقيد و محدد بناءا على مبدأ الترخيص الدائم أو المؤقت حسب الحاجة في إطار العمل ، و دخول أي هيئة أخرى إلى المحلات (كمقابلة ، تهيئة مكاتب ، تصليحات...) يجب أن تكون تحت مراقبة مستمرة من طرف شخص مسموح له بالدخول.[172]
- **مراقبة هوية كل من يدخل المؤسسة** و إعطاءه البطاقة المناسبة لمهمته (زائر ، متدرب ..) و كتابة معطيات الهوية في سجل الزيارات و وقت المجيء و الذهاب.
- **وضع كاميرات مراقبة** : و تكون على كافة الموقع لمراقبة الحركة داخل المؤسسة . و تركيب نظام فيديو حماية ملائم لهيئة المؤسسة (داخليا و خارجيا) و عدم رؤيتها إلا عند الضرورة و الاستعلام عن التشريع ساري المفعول الخاص بفيديو المراقبة و تطبيقه و أجل تخزين الصور ...[173]
- **استخدام أجهزة كشف** الدخان و أجهزة الإطفاء الآلي للوقاية من الحريق و مكافحته عند وقوعه .

[168] Sécurité Economique « les bonnes pratiques pour votre entreprise » , op cit , p5.
[169] **Jean Menthonnex** , « Sécurité et Qualité informatiques-Nouvelles Orientation » , CERSSI , Presses Polytechniques et Universitaires Romandes , Suisse , 1995 , p339.
[170] Ibid , 339.
[171] Politique de sécurité des systèmes d'information de l'état , version 1.0, op cit, p20.
[172] **Philippe Gloaguen** , « Le guide de l'intelligence économique » , Le guide du routard, Hachette Livre , 2012 ,pp 50-51.
[173] La sécurité économique au quotidien en 22 fiches thématiques, op cit , fiche 4.

الفرع الثاني : أمن تجهيزات نظم المعلومات

أ- الحماية المادية لقاعات و أجهزة المعلوماتية

- **مراقبة الدخول للأنظمة** : الوصول المادي للتجهيزات يجب أن تكون ضمن سياسة مراقبة المداخل و معرفة حاجات و مستويات السرية المسموح بها لكل مستخدم في المؤسسة لتجنب أي تشويه للمعلومات ، سرقة الأجهزة أو تحاميل المعطيات[174]، فالأجهزة المعلوماتية للمؤسسة يجب أن تكون محمية ضد كل دخول غير مسموح و ضد كل ضياع أو كارثة التي يمكن أن تكون بصفة مقصودة أو غير مقصودة[175]، و بالتالي تكون الحماية المادية للأجهزة عن طريق إغلاق قاعات الخوادم و المعلوماتية و المكاتب و كل الأجهزة المتحركة التي تضم معلومات مهمة يمكن انتشالها.[176] و في هذا السياق يمكن انشاء ما يسمى بالغرفة التقنية للموقع و هي عبارة عن مكان يحوي النظام العصبي المعلوماتي للمؤسسة و الذي يجب أن يحظى بالحماية القصوى سواء من التدخلات البشرية أو من الكوارث الطبيعية .[177]
- **حماية الكابلات الكهربائية و كابلات التواصل** : يجب حماية أسلاك الشبكة ضد الأضرار أو ضد اعتراض الاتصالات المنتقلة ،كذلك لوائح الربط و الوصل وقاعات الكابلات يجب أن تتموقع خارج المناطق العامة و الدخول إليها يجب أن يراقب.[178]
- **التهوية** : يجب أن يكون هناك آلية تهوية موضوعة في خدمة أجهزة أنظمة المعلومات ، و إجراءات تفاعل في حال الأعطال للوقاية من كل ارتفاع حراري للتجهيزات التي يمكن أن تتسبب في ضياع الخدمات.[179]
- **وضع إجراءات لحماية الحواسب المحمولة** عند السفر و عند حضور المؤتمرات و الندوات كتجنب ترك الأجهزة في الحقيبة الخلفية للسيارة لأن ذلك يعرضها للعوامل الحيوية كالحرارة المرتفعة التي قد تتلف الدوائر الالكترونية في الحاسوب ، أو البرودة الشديدة التي تؤدي إلى عطب الشاشة أو يتعرض للسرقة.[180]
- **الحماية ضد السرقة** عن طريق وضع سلك الأمان الذي يربط في موضع خاص بالحاسوب المحمول و يثبت الكابل بهذا الموقع ، كما يثبت طرفه الآخر بجسم ثقيل أو ثابت.[181]

---

[174] **Jean –François Carpentier**,op cit , p39.
[175] Politique sur l'accès , la sécurité de l'information et la protection des renseignements personnels , Québec , 2010 , p4.
[176] **Philippe Atelin** , op cit , p320.
[177] **Nicolas Moinet** , op.cit , p137.
[178] Politique de sécurité des systèmes d'information de l'état , version 1.0, op cit, p20.
[179] Ibid , p21.
[180] خالد الغثبر، مهندس القحطاني ، مرجع سابق ،ص 191.
[181] نفس المرجع ، ص 192.

- **تركيب أنظمة اكتشاف** للحماية ضد الحريق و الفيضان و تسرب المياه.[182]
- حماية التحاميل ، أقراص التخزين ، آلات الطباعة و النسخ عن طريق وضع إجراءات مراقبة كل مستعمل لها إلى غاية إرجاعها.
- **الخزانة القوية** : هي خزانة أمنية توفر مقاومة قوية ضد السطو و السرقة ، موجهة من أجل ضمان أفضل حماية للوثائق و التجهيزات الحساسة ، و تكون مجهزة إما بمفتاح أمني يتم وضعه في مكان غير مكان الخزانة أو برمز الفتح يتم تحديثه دوريا[183]

ب– الحماية الفنية لأجهزة نظم المعلومات

- كلمات المرور : الدخول إلى أجهزة العمل و الوسائل المتحركة يجب أن تُؤَمَّن عن طريق كلمات المرور التي تتضمن معلومات سرية و يجب أن تكون صعبة ، و لا يجب افشاءها و تركها دون أمن[184].كما يمكن استخدام أدوات تعريف أخرى معتمدة على الخواص البيولوجية للمستخدم.

– تغيير كلمة السر كل 6 أشهر أو سنة بالأكثر و استخدام 10 أحرف متنوعة من أحرف كبيرة وصغيرة و أرقام و رموز صعبة لتصعيب اكتشافها.[185]

- تركيب مراقب سري على شاشات الحواسب المحمولة ، اللوائح ، الهواتف ذات الاستعمال المهني ، و في حال استعمال الويفي و البلوتوث في الأجهزة كثيرة التنقل يجب التذكر أن أي ارتباط يمكن أن يعرضها للخطر.[186]
- تحميل برنامج خفي يسهل متابعة الجهاز بحيث يقوم هذا البرنامج الاتصال ببرنامج آخر كلما ارتبط المحمول بشبكة الانترنت ، فعندما يريد السارق استخدام الجهاز للاتصال بالانترنت يجري البرنامج الموجود في المحمول اتصال بالبرنامج الموجود في الخادم و يمرر معلومات عن موقع الجهاز المسروق أو أي معلومات تساعد في ايجاده.[187]

[182] **Jean –François Carpentier**,op cit , p39.
[183] **Nicolas Moinet**, op cit , p 29.
[184] **Joseph ILLAND**, « politique de sécurité des systèmes d'information(PSSI), document d'orientation de sécurité des systèmes d'information », Centre National de la Recherche Scientifique (CNRS),2006,p20
[185] **Arnaud Pelletier et Patrick Cuenot** , op cit , p 42.
[186] La sécurité économique au quotidien en 22 fiches thématiques, op cit , fiche 5.
[187] خالد الغثبر، مهندس القحطاني ، أمن المعلومات بلغة ميسرة ، مرجع سابق ،ص 192.

الفرع الثالث : انتباه العنصر البشري لتحركاته و تصرفاته (حماية المعلومات الحساسة)

العامل الأساسي في تسيير أمن المعلومات الاستراتيجية يتموقع بين الكرسي و لوحة المفاتيح ، ليس الآلة ، إنما العامل البشري ، لذا فمن المهم جدا أن ينتبه كل شخص في المؤسسة و ليس المسؤولين فقط لكل التصرفات اليومية البسيطة و اعتماد العادات الجيدة لحماية المعلومات الحساسة.[188]

1- تدابير الحماية داخل المؤسسة

أ- التدابير اليومية : و هي انتباه العامل أو المسؤول عن كل تصرفاته و تحركاته طوال اليوم العملي و من بين التدابير ما يلي :

- **حماية التوثيق الداخلي للمؤسسة**[189] : يجب ترتيب و أرشفة الوثائق بطريقة جيدة و تعريف الوثائق الخاصة بالمؤسسة عن طريق تعليمها بقلم خاص فوق غلاف التقارير الورقية ، و برمز مرئي على شاشات الأجهزة الالكترونية ، و هذا التعليم يمكن أن يشمل : الوثائق المؤقتة و العابرة كالمحاولات و الملاحظات أو الوثائق الدائمة كمخططات العمل.
- عدم ترك المعلومات الناتجة عن الاجتماع مهما كان ما سجلت عليه (ورق ، تحميل) ، و الانتباه أنه يجب سحق الوثائق المهمة عند رميها لأنه يمكن استرجاعها.[190]
- النسخ و التخزين الاحتياطي : يجب نسخ المعطيات الاستراتيجية للمؤسسة في موقع مختلف كتأمينهم مثلا في مؤسسة خارجية متخصصة في أرشفة الاعلام الآلي.[191]

و من شروط التخزين ما يلي :[192]

- تحديد المعطيات الواجب تخزينها ، و مدة التخزين ، و مراجعة دورية لمحيط الخزن.
- تعديد أماكن الحفظ و التخزين في عدة تحاميل.
- تأمين أماكن التخزين و الحفظ الشهري و السنوي للتحاميل خارج المؤسسة.

[188] **Arnaud Pelletier et Patrick Cuenot** , op cit , p p42-41 .
[189] **Philippe Gloaguen** , op cit ,pp 49-50.
[190] Sécurité Economique « les bonnes pratiques pour votre entreprise », op cit , p12.
[191] **Philippe Gloaguen** , op cit ,p55.
[192] **Sylvie Domenech , Manuel Marciaux et Dominique Charnassé** , « Guide des bonnes pratiques en matière d'intelligence économique », Service de Coordination a l'Intelligence Economique , 2009,p26.

ب– التدابير الخاصة : تكون التدابير الخاصة عند دخول أشخاص غرباء للمؤسسة كالمتدربين ، الزوار بكل أشكالهم....مما يتطلب الحيطة و الحذر و التيقظ لكل تصرفاتهم و تحركاتهم ، و أخذ كل التدابير الوقائية ، و من بين التدابير ما يلي :

- **التدابير المتخذة مع العمال الجدد** : أهم و أول خطوة تقوم بها المؤسسة مع العمال الجدد هو الإمضاء على بند السرية في عقد العمل ما يمنع المستخدم من إفشاء أي معلومة حساسة و استراتيجية في حياة المؤسسة[193]

- **التدابير المتخذة مع المتدربين (المستخدمين المؤقتين)** : المستخدم المؤقت هو شخص له مهمة محددة داخل المؤسسة ، و من الصعب تحديد نواياه الحقيقية ، و هل فعلا تواجده داخل المؤسسة بهدف انجاز المهمة ، أو له أهداف خبيثة لذا يجب القيام بعدة تدابير وقائية منها :

– التحقق الجيد لمسار المستخدم المؤقت المستقبلي قبل أن يأتي ، هذه العملية يجب أن تتضمن الشخص نفسه و محيطه أيضا خاصة محيط العمل[194]، و دراسة السيرة الذاتية جيدا و الاتصال بالجهات المعنية للتأكد من صحة المعلومات المدونة فيها.

– تحسيس المستخدم المؤقت منذ وصوله بمعايير الأمن المطلوبة في المؤسسة ، و إجباره على حمل شارة خاصة مختلفة يمكن تمييزها عن بعد.[195]

– تعيين مسؤول مكلف بتأطير المتدرب و عدم تركه يصل بمفرده إلى التجهيزات و المعلومات الحساسة عن طريق فرض رقابة عليه عند كل استخدام لشبكات الاعلام الآلي ، التحاميل ، آلات النسخ ...

– وضع بند السرية و منع نشر معلومات المؤسسة دون موافقة منها في العقد ، و التأكد من التزامه به .

- **التدابير المتخذة مع الزوار** : عند فتح أبواب المؤسسة لزيارات منتظمة يجب التفكير جيدا بالأشخاص الفضوليين ، فهناك من يأتي خصيصا بهدف جمع المعلومات الاستراتيجية [196]،لذا يجب اتخاذ بعض التدابير الوقائية:

– التحضير المسبق لعملية استقبال الزوار ، و اعلام جميع المستخدمين و توصيتهم بالحيطة و الحذر، مع التحديد المسبق لمسار الزيارة حسب الحاجة ، و الابتعاد عن المناطق الخاصة و السرية.[197]

[193] **Nicolas Moinet** , op.cit , p58
[194] La sécurité économique au quotidien en 22 fiches thématiques, op cit , fiche 6.
[195] Ibid , fiche 6.
[196] **Pierre Mongin et Franck Tognini** , op.cit , p30
[197] **Nicolas Moinet** , op.cit , p61

- التأطير الجيد و الصارم لأي تسجيل صوتي أو تصوير أو تسجيل فيديو ، و التيقظ لأسئلة الزوار التي تكون أحيانا مفخخة.[198]

- فتح سجل زيارات لتدوين المعلومات الخاصة بالزوار و اجبارهم على حمل البطاقات الخاصة.[199]

- المرافقة الدائمة للزائر خلال كل الزيارة في حدود المعايير المطلوبة.[200]

- اغلاق الملفات التي يمكن أن تكون في الحاسب أو فوق المكتب ، و اخفاء الوثائق المهمة عند الزيارات لأنه قد يقوم الزائر بالتصوير بطريقة غير شرعية.[201]

- ايقاف نشاط كل التحاميل و الحواسب الموجودة في المسار و تحضير حاسب مسبقا غير متصل بالشبكة يسمح باستقبال مفاتيح و تحاميل الزوار.[202]

- استقبال الزيارات مع أشخاص مجهولين في قاعة الاجتماعات ، و ليس في المكتب أين توجد المعلومات الحساسة.[203]

2- تدابير الحماية خارج المؤسسة : تتضمن الحماية خارج المؤسسة إما الأماكن العامة أو المهمات المهنية.

أ- التحركات المهنية : من التدابير المتخذة في سفرات العمل ما يلي :

- تحديد إطار محدد لمهمة العمل ، و أخذ فقط المعلومات و الأجهزة الضرورية و عدم استخدام الأجهزة المتاحة في أماكن العمل.[204]

- التحفظ و تجنب المحادثات المهنية.

- عدم الوثوق بأي صداقات جديدة.

- الحذر خلال الملتقيات و المؤتمرات:إذ يوجد أشخاص موكلين فقط للحضور في مثل هذه التجمعات من أجل جمع ما يمكن جمعه من معلومات استراتيجية ، و عليه من الضروري التأكد من هوية الشخص الذي تحدّثه.[205]

ب- الأماكن العامة : نقصد بالأماكن العامة وسائل النقل ، المطاعم ، المقاهي ... ،ففي هذه الأماكن قد يأخذ الفرد راحته في الكلام دون الانتباه لعواقب ذلك مما قد يعرضه للخطر ، لذا يجب التيقظ جيدا لخطر هذه الأماكن ، و من التدابير الممكن اتخاذها ما يلي :

[198] **Nicolas Moinet** , op.cit , p61.
[199] Sécurité Economique « les bonnes pratiques pour votre entreprise », op cit , p13.
[200] **Philippe Gloaguen** , op cit ,p50.
[201] Ibid , p50.
[202] La sécurité économique au quotidien en 22 fiches thématiques, op cit , fiche7.
[203] **Arnaud Pelletier et Patrick Cuenot** , op cit , p43
[204] Sécurité Economique « les bonnes pratiques pour votre entreprise », op cit , p13
[205] **Pierre Mongin et Franck Tognini** , op.cit , p 27.

- تفادي التكلم في مواضيع العمل في الأماكن العامة فقد تتعرض لخطر التصنت من منافس يجلس بقربك.
- تفادي قراءة الملفات المهنية بصوت مرتفع أو فتح شاشات الحاسوب في مكان عام ، مما قد يعرضك لاستراق النظر من شخص ما.
- عدم التكلم مع شخص مجهول عن أمر متعلق بالعمل ، فقد يكون يعمل لدى المنافس.
- تفادي استعمال الويفي و البلوتوث خلال التنقل لتفادي أي ارتباط.

من خلال النقاط المذكورة يتبين لنا الدور الذي تلعبه الحماية المادية التي يتغافل الكثير عن أهميتها ، فحماية موقع المنظمة و تجهيزات الاعلام الآلي يعتبر نصف الطريق نحو أمن المعلومات ، إضافة إلى الاهتمام بكل تحركات العامل البشري خلال رحلة عمله التي في أغلب الأحيان تكون هي سبب الكوارث.

المطلب الثالث : الحماية القانونية للممتلكات غير المادية (حقوق الملكية الفكرية)

تعتبر الملكية الفكرية ضمانا حقيقيا للمصنفات المعلوماتية من التزوير و التقليد ، و تختلف طبيعة حقوق الملكية من مصنف لأخر حسب شكله و محتواه ، فهناك ما يحمى بحقوق المؤلف ، و هناك ما يحمى ببراءة الاختراع

و هناك ما يحمى بحقوق منتج قواعد البيانات...

الفرع الأول : ماهية حقوق الملكية الفكرية

لقد انتقل الاهتمام بحقوق الملكية الفكرية من المرحلة المحلية لكل دولة إلى مرحلة العالمية ، فلقد تعددت الاتفاقيات التي نظمت حقوق الملكية الفكرية عموما و براءة الاختراع بصفة خاصة بداية من اتفاقية " **برن** " انتقالا إلى اتفاقية المنظمة العالمية للملكية الفكرية (WIPO) ، و أخيرا اتفاقية " **التربس** ".[206]

و لكن رغم ذلك تبقى حقوق الملكية الفكرية تختلف من بلد لآخر ، إذ أن هناك علاقة بين الملكية الفكرية و البنية الاجتماعية و الاقتصادية للبلد ، و المفاهيم الفلسفية و العادات الثقافية. و عليه كل دولة لها ميزتها الخاصة في التعريف على مستوى الاقليم الذي تمارس فيه سلطتها العليا، و بالتالي حقوق الملكية الفكرية لها طابع

[206] **عمر محمد حماد** ، الاحتكار و المنافسة غير المشروعة ، دار النهضة العربية ، 2009 ، ص 288.

اقليمي و يجب أن تُسيَّر بقانون البلد الذي طُلبت به الحماية ، و عليه لا يوجد حقوق على الابتكارات الفكرية التي لها فعالية عالمية.[207]

و حسب المنظمة العالمية للملكية الفكرية (OMPI) مصطلح الملكية الفكرية يعني " نتاج العقل ، الاختراع ، النتاجات الأدبية و الفنية و الرموز ، الأسماء ، الصور و الرسومات و النماذج المستعملة في التجارة " ، فهي تمثل حماية الابداعات الفكرية ، التصدي ضد نشاطات التزوير ، و الأعمال غير القانونية ، اثراء رأس المال المادي للمؤسسة و خلق مصدر مداخيل حقيقي (تنازلات الشهادات ، تراخيص الاستخدام ..) ، ابقاء شهرة المؤسسة أمام الزبائن ، و تنمية مصداقيتها أمام شركائها.[208]

1- حقوق الملكية الأدبية و الفنية (حقوق المؤلف)

لقد أخذت الحماية الدولية لحق المؤلف تاريخيا شكل نصوص يتم تضمينها في القوانين الوطنية تلزم الدول بوجوب المعاملة بالمثل ، و كانت أول اتفاقية دولية متعددة الأطراف في مجال حماية حق المؤلف اتفاقية " **برن** " عام 1886 ، و أصبحت فيما بعد إحدى الاتفاقيات التي تشرف عليها المنظمة العالمية للملكية الفكرية ، ثم أبرمت الاتفاقية العالمية لحقوق المؤلف تحت إشراف اليونسكو ، و ترتبط حقوق المؤلف عادة بالجهود الابداعية للأفراد و الدول مما أدى إلى توسيع نطاق المصنفات التي تحميها حقوق المؤلفين.[209] و تحمي حقوق المؤلف المواد المكتوبة كالكتب، و المواد الشفهية كالمحاضرات ، و المصنفات الفنية الأدائية كالمسرحيات و الموسيقى و التمثيل الايمائي ، و المصنفات الموسيقية، و المصنفات الفنية الأدائية كالأشرطة السينمائية و المواد الاذاعية السمعية ، و الفنون التطبيقية كالرسم و النحت و الصور التوضيحية و الخرائط و التصميمات و المخططات و الأعمال المجسمة المتعلقة بالجغرافيا و الخرائط السطحية للأرض ، و برامج الحاسوب و قواعد البيانات ، و طوبوغرافيا الدوائر المتكاملة ، و هذا القسم يعرف بحقوق المؤلف ، و يلحق به ما أصبح يطلق عليه الحقوق المجاورة لحق المؤلف المتمثلة بحقوق المؤديين و العازفين و المنتجين في حقل الفونجرامات (التسجيلات الصوتية) و حقل الاذاعة.[210]

---

[207] **Dario Moura Vicente** , « La propriété intellectuelle en droit international privé , Adagp : Académie de droit international de la Haye » , Paris , 2009 , p23.

[208] **Eric Delbecque , Jean-Renaud Fayol** , op cit , p167.

[209] **مجد الدين خمش** ، "العولمة و تأثيراتها في المجتمع العربي "، 2011 ، ص 54

[210] **يونس عرب** ، "نظام الملكية الفكرية لمصنفات المعلوماتية "، الدليل الالكتروني للقانون العربي ، ArabLawInfo ، ص 15 أنظر : www.arablawinfo.com

و بالتالي حق المؤلف هو الحق المطلق الإستئثاري الذي يحظى به مؤلف أي مصنف ليتصرف فيه كما يشاء ، بحيث يمكن أن يكتب عليه اسمه أو يعلن أنه صاحبه ، و يعد حق المؤلف بمعناه الواسع حقا ذهنيا لذلك فهو يعرف بأنه حق الملكية المعنوية المتعلقة بتأليف ما[211]، و التي هي ملك مؤلف النتاج لمدة 70 سنة بعد وفاته.[212]

و عليه حقوق المؤلف تحمي كل " نتاج عقلي " مهما كان نوعه ، شكله ، التحميل الذي يوجده أو الوجهة مع إقصاء الأفكار و المفاهيم .[213] بشرط أن يستوفي هذا النتاج شرطي الأصلية ، و التثبيت على تحميل مادي.

2- حقوق الملكية الصناعية

الملكية الصناعية هي إحدى عناصر الملكية الفكرية ، و تعرّف حقوق الملكية الصناعية بأنها " الحقوق التي ترد على مبتكرات جديدة مثل : المخترعات و الرسوم و النماذج الصناعية ، أو على إشارات مميزة تستخدم إما في تمييز المنتجات و السلع كالعلامة التجارية أو في تمييز المنشآت التجارية كالاسم التجاري بحيث تمكّن صاحبها من الاستئثار باستغلال ابتكاره أو علامته التجارية أو اسمه التجاري في مواجهة الكافة ".[214]

و حددت **اتفاقية باريس** لحماية الملكية الصناعية المفهوم بمعناه الواسع فجاء فيها : " تطلق الملكية الصناعية على المعنى الأكثر اتساعا ، فلا يقتصر تطبيقها على الصناعة و التجارة بمعناها الحرفي ، و إنما تُطبق أيضا على مجال الصناعات الزراعية و الاستخراجية و جميع المنتجات المصنعة أو الطبيعية مثل : الأنبذة و الحبوب و أوراق التبغ و الفواكه و المواشي و المعادن و المياه المعدنية و البيرة و الزهور و الدقيق " .[215]

فالملكية الصناعية تأخذ أشكال متعددة ، كبراءة الاختراع التي تحمي إبداع أو اختراع تقني مدة 20 سنة[216] العلامة التجارية لحماية اشارات المنتجات و الخدمات و التمييز بينها ، و التي بمجرد ايداعها يتحصل صاحبها على احتكار استغلال مدة 10 سنوات متجددة[217]، و الاسم التجاري لحماية المؤسسة و تمييزها عن غيرها ،

---

[211] **نايل الحجايا** ، "التحول الالكتروني في الجامعات و أثره في التعليم الالكتروني" ، المؤتمر الدولي الأول لتقنيات المعلومات و الاتصالات في التعليم و التدريب ، الحمامات ، تونس ،7-2012/05/10 ، ص98.

[212] **Ghilhem Fabre** , « Propriété Intellectuelle , contrefaçon et innovation – les multinationales face à l'économie de la connaissance -» , Publication des Universités de Rouen et du Havre , 2009 , p 15.

[213] Guide Pratique du MEDEF , La Protection des Informations Sensibles des entreprises , Paris , janvier 2013 , p19.

[214] **سميحة القليوبي** ، "الملكية الصناعية" ، دار النهضة العربية للطبع و النشر و التوزيع ، القاهرة ، 2005 ، ص 11 عن سائد أحمد الخولي ، حقوق الملكية الصناعية ،دار مجدلاوي ، عمان ، 2004، ص 21.

[215] Comprendre la propriété industriel , Organisation Mondiale de la Propriété intellectuelle WIPO , op cit , p5.

[216] **Phillippe Gloaguen** , op cit , p45

[217] **Eric Delbecque , Jean-Renaud Fayol**, op cit , p171

و الذي تنشأ ملكيته بمجرد تقيده في السجل التجاري[218]، و الرسومات و النماذج الصناعية لحماية الابتكارات الزخرفية و التي هي عبارة عن المظهر الزخرفي أو الجمالي لسلعة ما ، و تكون فترة الحماية 5 سنوات مع امكانية تجديدها إلى 25 سنة كحد أقصى[219] ، إضافة إلى الاشارات الجغرافية و حماية الأصناف النباتية و الأسرار التجارية. و قد تحقق في اتفاقية " **تربس** " إرساء قواعد ملزمة و فعالة لحماية حقوق الملكية الصناعية بحيث جمعت كل الوثائق السابقة و القوانين و دُمجت معا لتشكل نظاما متكاملا للحماية منها ، و تلزم الاتفاقية الدول بشكل واضح بتعديل تشريعاتها لتتلاءم مع أحكام هذه الاتفاقية.[220]

الفرع الثاني : حماية المصنفات المعلوماتية

1- **حماية برامج الحاسوب :**

تعد برامج الحاسوب أول و أهم مصنفات المعلوماتية أو تقنية المعلومات التي حظيت باهتمام كبير من حيث وجوب الاعتراف و توفير الحماية القانونية لها[221]، و من أجل توفير حماية مناسبة للبرنامج يجب أولا إعطاء تعريف محدد له ، و قد تم تعريفه كالآتي:

- البرنامج هو مجموع الأنظمة ، الإجراءات ، القواعد ، و التوثيقات المتعلقة بمعالجة المعلومات[222].
- و يعرف أيضا على أنه : مجموع الأوامر المرتبة التي تتيح للأجهزة المادية للكمبيوتر القيام بمهامها. و بدون البرمجيات تصبح الأجهزة المادية مجرد كتل حديدية و بلاستيكية بدون فائدة.[223]

و البرامج المحمية يمكن أن تكون برامج تشغيلية (Windows)، أو برامج تطبيقية(Word،Exel) ، و يمكن أن يكون برنامج عام أو تحت الطلب.[224]

و قد أثارت برامج الحاسوب جدلا واسعا بشأن طبيعتها و موضع حمايتها من بين تشريعات الملكية الفكرية ، و ترددت الآراء بين داع لحمايتها عبر نظم براءات الاختراع لما تنطوي عليه من سمة الاستغلال الصناعي ، و بين

---

[218] عمر محمد حماد ، مرجع سابق ، ص342

[219] الرسوم و النماذج الصناعية و اتفاق لاهاي ، منشور الويبو رقم (A) 429 ، المنظمة العالمية للملكية الفكرية.

[220] مجد الدين خمش ،مرجع سابق ص 55 .

[221] يونس عرب ، نظام الملكية الفكرية لمصنفات المعلوماتية ، الدليل الالكتروني للقانون العربي ، ArabLawInfo ، ص 19 أنظر : www.arablawinfo.com

[222] **Hubert Bitan** , « Droit des créations immatérielles –logiciels , bases de données , autres œuvres sur le web 2.0 » , éditions Lamy , France , 2010 , p21.

[223] يونس عرب ، مرجع سابق ، ص 5

[224] **Marie-Florc Célarier , Delphine Marie-Vivien** , « les droits de propriété intellectuelle :guide pratique » , éditions Cirad ,France , Janvier 2002 , p 31 .

من ذهب إلى حمايتها عبر نظم الأسرار التجارية إذ تنطوي في الغالب على سر تجاري يتجلى بالأفكار التي انبنى عليها أو الغرض من ابتكارها ، و بين داع لحمايتها عبر آلية الشروط العقدية التي تجد مكانها في رخص الاستخدام أو اتفاقيات الاستغلال ، لكن كافة هذه الآراء لم تصمد أمام الرأي الذي وجد في البرمجيات عملا ابتكاريا أدبيا ، يضعها ضمن نطاق مصنفات الملكية الأدبية ، إذ هي أفكار و ترتيب لخوارزميات تفرغ ضمن شكل ابتكاري ابداعي ، و صفاتها المميزة تتقابل مع عناصر الحماية لمصنفات الملكية الادبية[225] ، و بما أن البرنامج هو عبارة عن نتاج العقل ، فمن شروط حمايته هو اكتساء طابع " الأصلية " و الذي يكون تقييمه غالبا عرضة للجدال ، فعنصر الأصلية يعكس و يترجم تعبيرات شخصية المؤلف و بصمته ، وهذا يختلف حسب البرنامج.[226]

و بالنسبة لعناصر الحماية فإنه فقط الشكل محمي ، و كل فكرة أو مفهوم يجب أن يكتسي قدر من التطبيق المادي ، و تكون حماية البرنامج متعلقة بنتاج العقل مهما كان نوعه او شكل تعبيره ، استحقاقه أو توجهه ، و يوجد ثلاث أنواع من النتاجات: النتاجات الأدبية ، الفنية و العلمية ، و يكون التفريق بينها حسب المضمون لا الشكل ، فمثلا إذا كان محتوى البرنامج في المعظم تقني فسوف يقيم كنتاج علمي.[227]

و من الاجتماعات و الاتفاقيات التي ترسّم حماية البرامج كمصنفات أدبية هي سلسلة اجتماعات خبراء "**الويبو**" و منظمة اليونسكو عام 1983و 1985 التي أسفرت عن توجه عام لاعتبارها من قبيل الأعمال الأدبية، كما أن اتفاقية "**تربس**" أضافتها إلى المصنفات الأدبية و الفنية محل الحماية بموجب اتفاقية بيرن[228]، و في سنة 1988 تأسس الاتحاد الدولي لمنتجي برامج الكمبيوتر التجارية، و هو هيئة عالمية تمثل مطوري برامج الكمبيوتر و تطبيقات التجارة الالكترونية في 65 دولة في أنحاء العالم، و له شبكة مكاتب في الولايات المتحدة و أوربا و الشرق الأوسط و آسيا،هدفه مساعدة الحكومات في محاربة القرصنة عبر توعية مستخدمي الحاسوب بقوانين حماية حقوق الملكية الفكرية،و يدخل في عضوية هذا الاتحاد شركات عالمية في تقنيات المعلومات و البرمجيات[229].

---

[225] يونس عرب ، مرجع سابق ، ص 20

[226] **Hubert Bitan** , 2010 , op cit , p 30.

[227] Ibid , p 31.

[228] يونس عرب ، مرجع سابق ، ص 20

[229] **زايري بلقاسم ، بلحسن الهواري** ، "اقتصاديات الأفكار الرقمية و قضايا الحماية الفكرية لها "، الملتقى الدولي حول اقتصاد المعرفة ، كلية الاقتصاد و التسيير ، جامعة بسكرة ، نوفمبر 2005 ، ص224.

و تكتسب الحماية منذ ابتكار البرنامج دون أي اجراءات ، الشرط الوحيد هو " الأصلية " ، كما أن ايداع ملكية حقوق المؤلف ليس اجباري و لكن الايداع محبذ من أجل اقامة الحجة على تاريخ و ابتكار البرنامج ، و تكون مدة الحماية 70 سنة منذ نشره و تعطي لصاحب البرنامج حق حصري في : إعادة الانتاج ، الترجمة ، التكييف و الترتيب و التوزيع ، و منع إعادة انتاج البرامج جد صارم ، إذ أنه من الممنوع إعادة انتاج جزء أو كل البرنامج سواء بصفة مؤقتة أو دائمة ، و تحت أي شكل و إن كان لأغراض شخصية أو بيداغوجية ، و صاحب الحق على البرنامج حر في منح تراخيص استعمال البرنامج مجانية أو مدفوعة.[230]

استثنائيا ، البرنامج يمكن أن يكون محمي بحقوق البراءات :[231]

- إذا كان الاختراع المحصل على البراءة يضم برنامج ، فالبرنامج بصفة غير مباشرة يصبح محمي ببراءة اختراع.
- إذا كان البرنامج ينتج عنه نتائج تقنية ملموسة ، بمعنى يسمح بتحقيق منتج أو أسلوب ، و إذا كانت خصائص التسجيل مكتملة إذن يستطيع أن يحصل على براءة الاختراع .

2- حماية قواعد البيانات

البيانات أو المعلومات المخزنة في نظم الحواسيب ليست محل حماية بالنسبة للقوانين و الأنظمة ، لكنها متى ما أفرغت ضمن قاعدة بيانات وفق تصنيف معين و بآلية استرجاع معينة فإنها تتحول من مجرد بيانات إلى قاعدة معطيات.[232]

و تعرف قاعدة البيانات على أنها : كتب تحوي مقتطفات أدبية أو وثائق ، معطيات أو عناصر أخرى مستقلة ، منظمة بطريقة منهجية أو نظامية و سهلة المنال بوسائل الكترونية أو بأي وسيلة أخرى [233].

و الاعتراف لقواعد البيانات بالحماية جاء وليد جهد واسع لمنظمة الويبو و لمجلس أوروبا الذي وضع عام 1996 قواعد ارشادية و قرار يقضي بالنص على حماية قواعد البيانات ضمن قوانين حق المؤلف ، كما أن اتفاقية تربس نصت صراحة في المادة 2/10 على تمتع البيانات المجمعة سواء كانت بشكل مقروء آليا أو أي شكل آخر بالحماية القانونية متى ما كانت تشكل خلقا فكريا.[234]

---

[230] **Marie-Florc Célarier** , op cit , pp 31- 32.
[231] Ibid , p 31.
[232] يونس عرب ، مرجع سابق ، ص 20
[233] **Hubert Bitan** , « Protection et contrefaçon des logiciels et des bases de données » , éditions Lamy , 2006 , p224.
[234] يونس عرب ، مرجع سابق ، ص 21.

و حقوق منتج قواعد المعطيات أو حقوق Sui generis (حقوق موضوعة خصوصا لحماية قواعد البيانات) تحمي قاعدة البيانات منذ ابتكارها لمدة 15 سنة تُحسب منذ اتمام قاعدة البيانات أو منذ أول وضعها و إتاحتها للجميع.[235]

3- حماية موقع الانترنت

الحماية الفكرية المتعلقة بمواقع الانترنت متعددة ، حسب محتوى الموقع و الأدوات المرافقة له ، فإذا كان المحتوى نتاج عقلي يمكن أن يُحمى بعنوان حقوق المؤلف ، و إذا كان الموقع يحوي قاعدة معطيات يُحمى عن طريق حقوق Sui generis التي تحمي قواعد البيانات ، اسم المجال يمكن أن يحمى عن طريق حقوق العلامة.

حقوق المؤلف تحمي موقع الويب منذ ابتكارها إذا كان أصلي ، فالموقع يعكس شخصية المؤلف و تكون مدة الحماية 70 سنة منذ إعلانها إذا كان الموقع نتاج أدبي أو فني جماعي محقق من طرف عدة مؤلفين أين تكون المساهمة الشخصية غير بارزة عن مجمل مفاهيم الموقع ، أما بالنسبة لموقع ويب مؤلف واحد أو مؤلفين أين تكون مساهمته منفصلة بموضوع ما ، الحماية عن طريق حقوق المؤلف تذهب إلى غاية 70 سنة بعد موت المؤلف.[236]

4- طوبوغرافيا الدوائر المتكاملة

الدوائر المتكاملة هي المنتجات التي يكون الغرض منها أداء وظيفة الكترونية ، و قد حققت فتحا مميزا في صناعة الالكترونيات و تطوير وظائف التقنية العالية ، و مع تطور دمج الدارات الالكترونية على الشريحة للقيام بمهام الكترونية أصبح التميز و الخلق الابداعي يتمثل بآليات و ترتيب و تنظيم الدوائر المدمجة على شريحة شبه الموصل ، بمعنى أن طوبوغرافيا الشريحة انطوى على جهد ابداعي مكّن من تطوير أداء نظم الحواسيب بشكل متسارع ، و بالاعتماد على مشروع قانون الحماية الذي أعدته اللجنة الأوروبية أصدر مجلس أوروبا عام 1986 دليلا لحماية الدوائر المتكاملة ، و في عام 1989 أبرمت اتفاقية واشنطن بشأن الدوائر المتكاملة.[237]

[235] **Marie-Florc Célarier** , **Delphine Marie-Vivien**, op cit , p.34
[236] **Marie-Florc Célarier , Delphine Marie-Vivien**, op cit , p.34
[237] يونس عرب ، مرجع سابق ، ص 21

5- حماية المهارات

تستفيد المهارات على المستوى الأوروبي من تعريف نظامي حيث تعرف المهارات على أنها:[238] " مجموعة من المعلومات التطبيقية غير المسجلة ، تلخص الخبرة ، و هي :

أ- **سرية** : بمعنى أنها غير معروفة في العموم أو غير سهلة المنال.

ب- **أساسية** : بمعنى أنها مهمة و مفيدة في انتاج منتجات .

ج- **مُعرفة**: بمعنى انها موصوفة بطريقة كافية و كاملة من أجل السماح بالتحقق من أنها تلبي شروط السرية و الأهمية ."

المهارات لا يمكن حمايتها عن طريق البراءة فهي بطبيعتها غير الملموسة لا تدخل في معايير الاختراع، و كذلك صعوبة تبيين تقليدها من قبل شخص آخر دون موافقة صاحب المهارة تجعل من السرية أحسن حل فعال لحمايتها[239] ، إذ أنه من أبرز الصعوبات القانونية ضمن الاقتصاد الرقمي هو حماية سلعة ليس لها شكل ملموس ثابت كالأفكار و الحقائق ، ففي سوق الانترنت من حق الجميع تداول المعلومات التي تعبر عن الحقائق و الأفكار طالما تم الاعلان عنها و عرضها ، و قوانين الحماية الفكرية تحمي ما يعبر عن الأفكار و لا يحمي الأفكار ذاتها أو الحقائق مهما بذل المنشئ فيها جهدا فكريا و وقتا لاكتشافها و تطويرها ، فمع الانترنت يمكن تحويل الأفكار من عقل لعقول أخرى دون أن يكون لها وجود مادي.[240]

و المؤسسة عموما لها رأس مال من المهارات العمومية لا يمكن للزبون استخدامها دون أجر ، و المهارات يمكن أن تُمثل بعنصر الترخيص و الذي يعرف أيضا ب"تحويل التكنولوجيات " ، و غالبا ما يتعلق الأمر ببراءة الاختراع و المهارات ، لأن براءة الاختراع نادرا ما تكفي لتشغيل الانتاج ، إنما يجب أيضا أن تكون متصلة بمعلومات ، تعليمات ، توثيقات و تكوينات التي هي عبارة عن مهارات ، و أحيانا يتعلق الأمر بترخيصات للمهارات مستقلة عن براءة الاختراع.[241]

[238] Guide Pratique du MEDEF , La Protection des Informations Sensibles des entreprises , op cit , p17.

[239] **Marie-Florc Célarier , Delphine Marie-Vivien** , op cit , p 34

[240] زايري بلقاسم ، بلحسن الهواري ، اقتصاديات الأفكار الرقمية و قضايا الحماية الفكرية لها ، الملتقى الدولي حول اقتصاد المعرفة ، كلية الاقتصاد و التسيير ، جامعة بسكرة ، نوفمبر 2005 ، ص 221 ، ص 227.

[241] Guide Pratique du MEDEF , La Protection des Informations Sensibles des entreprises , op cit , p17.

الفرع الثالث : التزوير و التقليد

1- مفهوم التقليد

التقليد ظاهرة متشعبة تمس أوضاع اقتصادية و قانونية مختلفة، و من وجهة نظر قانونية مصطلح "تقليد" هو اغتصاب حق الملكية الفكرية، ويدل بصفة واسعة على مجموع أعمال التطفل، التقليد و المنافسة غير الشرعية.[242]

و يعرف التقليد أي تقليد نتاج العقل على أنه التعدي على الحقوق الحصرية للمؤلف ، خاصة استخدام نتاجاتها دون ترخيص.[243]

و حسب [244]Articles l.335-2 ,al.1 et 335-3 du CPI : "كل طبعة لكتابات ، قطع موسيقية ، رسم ، ألوان و كل نتاج آخر ، مطبوع أو منسوخ بأكمله أو جزء منه بدون مبالاة لحقوق و قواعد ملكية المؤلف هو تقليد ، و كل تقليد جريمة و تكون جريمة التقليد كل إعادة انتاج ، إعادة تقديم و نشر عن طريق أدوات مهما كانت ، لنتاج عقلي بسرقة حقوق المؤلف كما عرفها و نظمها القانون ".[245]

و عليه و من خلال التعريف يتبين أن التقليد يمكن أن يكون على عدة أوجه ، فهو عبارة عن تعدي على حقوق مؤلف النتاج عن طريق إما إعادة انتاج غير مرخصة ، توزيع دون رخصة ، النسخ ، و أيضا عن طريق إصابة حقوق الترجمة ، المطابقة و الترتيب .

أما بالنسبة للمقلد فهو كل شخص ساهم في عملية التقليد ، و أكثر تحديدا ، هو كل شخص أثار العملية ، قدم معلومات مساعدة ، أو أمد بوسائل من أجل اتمامها ، و من خلال الممارسة ، و خاصة في مجال البرامج ، الحقوق التي هي مرتبطة بالمستخدم تكون معروفة في عقد الترخيص ، و عندما لا يحترم المستخدم نصوص العقد و يتجاوز الحقوق الممنوحة له فهو مزور .[246]

و التقليد بصفة عامة يكون على وجهين :[247]

[242] **Eric Delbecque , Jean-Renaud Fayol ,** op cit , p179
[243] **Hubert Bitan ,** Droit des créations immatérielles , 2010 , op cit , p 346
[244] **CPI : Cour Pénael Internationale**.
[245] Ibid , p346.
[246] Ibid , p284.
[247] Ghilhem Fabre , op cit , p 15.

- **التقليد الأعمى** : و يكون إما لمنتج ، علامة ، براءة ، رسم أو نموذج ، وهذا يكون عبارة عن نشاط غير قانوني واضح ، و غالبا ما يكون خارج الاقليم الوطني من أجل ابطاء عملية اكتشافه ، و هنا غالبا ما تكون جودة المنتج أقل من الأصلي ، فالمؤسسة المقلِّدة لا تهتم بوفاء الزبائن ، و انما تبحث عن الربح السريع على المدى القصير ، عن طريق اغتصاب سمعة أخرى ، أما خسارة المؤسسة الضحية فتكون في مجال البحث و التطوير إضافة إلى خسائر مالية.
- **التقليد الذكي**: يأخذ شكل صورة بخداع العين، أي أنه لا يكمن اكتشافه بسهولة، و المؤسسة المقلدة تقدم منتج في نفس جودة المنتج الأصلي وأحيانا أحسن وأكثر تطور، تبحث عن وفاء الزبائن بدراسة رغباتهم لكسب حصة سوق وماركة منافسة للمؤسسة الضحية، و عليه فان التقليد الذكي يمس الميزة التنافسية للمؤسسة الضحية .

من خلال هذا التمييز بين نوعي التقليد يرفع أول ارتباك في معايير التقليد.

2- اجراءات التصدي لعملية التقليد

لمواجهة التقليد هناك نوعين من الإجراءات يمكن اتخاذها ، إجراءات وقائية أو احتياطية تقوم بها المؤسسة قبل وقوع التقليد و ذلك لتفاديه ، و إجراءات تصحيحية تتخذها بعد وقوع التقليد.

أ- الإجراءات الوقائية:

- تفعيل نظام يقظة : أفضل طريقة يمكن أن تعتمد عليها المؤسسة في حماية ممتلكاتها غير المادية هي تفعيل نظام يقظة شامل داخل الاقليم الوطني و خارجه للتأكد من عدم تقليد منتجاتها خصوصا على مستوى الانترنت، و طبعا قبل ذلك تكون المؤسسة قد سجلت حقوق ملكيتها الفكرية عند الجهة المعنية.
- حماية المؤسسة ممتلكاتها عن طريق السرية كإمضاء بنود سرية في عقود العمل ، و اعتماد معايير أمنية مشددة.

ب- الإجراءات التصحيحية:

بعد وقوع التقليد تقوم المؤسسة بالتالي :

- أول خطوة تقوم المؤسسة بالتأكد من أن حقوق ملكيتها مازالت سارية المفعول و لم تنته مدة الحماية الممنوحة
- إجبار المقلد على الكف و قطع شهادات التقليد عن طريق ارسال له بريد يذكره بعواقب اختراق حقوق الملكية الفكرية.[248]
- التواصل مع السلطات المعنية و ايداع طلب تدخل لدى الجمارك مع محاولة جمع أكبر قدر ممكن من الأدلة.

[248] Philippe Gloaguen , op cit ,p50.

- و من أجل تفادي إجراءات غير أكيدة ، المؤسسة يمكنها الدخول في تفاوض ودي مع المقلد و إعطاءه تعويضات تحت عنوان تصليحات ، و يمكن أيضا عرض على المقلد رخصة استخدام.[249]

و بالتالي فإن الحماية القانونية لمصنفات المعلوماتية أمر ضروري ، إذ يعتبر الوسيلة رقم واحد ضد التقليد و التزوير.

وسائل و طرق تحقيق الأمن المعلوماتي عديدة و متعددة ، و لكن الاستخدام الصحيح و التسيير الجيد لها هو سر نجاحها ، فكل مؤسسة تختار ما يناسبها من حماية حسب طبيعة نشاطها ، و محيط عملها ، كما أنه لا يجب الاستهانة بأي نوع من الحماية سواء البرمجية ، المادية أو القانونية ، لأن كل وسيلة أو كل نوع له أهميته و دوره في الوصول بالمؤسسة و الأنظمة المعلوماتية إلى بر الأمان.

[249] Eric Delbecque , Jean-Renaud Fayol, op cit , p180

خلاصة الفصل

من خلال ما سبق تم استنتاج أن أمن المعلومات هو استجابة و مواجهة للتهديدات المعلوماتية التي يصدرها الانترنت بالدرجة الأولى ، فكلما تطورت التهديدات تطورت معها طرق مواجهتها ، فتهديدات أمن المعلومات عديدة و متنوعة ، و تختلف هذه التهديدات حسب منفّذها ، أسباب الهجوم و طريقة التنفيذ ، فمن المنفذين نجد المحترف و الهاوي ، أما أسباب التهديد و الهجوم فهي متعددة ، إذ هناك من يهاجم لأجل الحصول على المال ، و هناك من يهاجم لأسباب ايديولوجية أو قضية يدافع عنها ،و هناك من يهاجم بدافع الانتقام ، كما نجد أيضا من يهاجم بدافع التسلية و إثبات المهارات ، و طرق التنفيذ لهذه الهجمات متنوعة ، فهناك التهديدات المادية التي تكون بالطرق التقليدية كالسرقة و التدمير ، و هناك التهديدات البرمجية التي تكون باستخدام وسائل التكنولوجيا ، و تكون إما بزرع البرامج الخبيثة و إما عن طريق القرصنة المعلوماتية ، أو عن طريق استغلال ثغرات الأنظمة لشن الهجومات ، و كلما تطورت التهديدات تطورت معها طرق الحماية ، فالتهديدات المادية أصبحت تواجَه بكاميرات المراقبة و أجهزة الانذار و البطاقات الممغنطة و الأبواب الدوارة .....أما التهديدات البرمجية فتواجَه ببرامج الحماية التي تركب على الأجهزة المعلوماتية ، كبرامج مكافحة الفيروس ، و الجدران النارية ، و الشبكات الافتراضية ، و أنظمة كشف التدخل.... ، إضافة إلى الاهتمام بالجانب البشري سواء من ناحية المراقبة و فرض العقوبات عند ارتكاب الأخطاء ، أو من خلال التوعية و التحسيس ، و لكن يبقى الأهم هو تعلم كيفية الوقاية منها قبل وقوعها و قبل حدوث الخسائر ، و يكون ذلك من خلال اليقظة الاستراتيجية التي تلعب دورا مهما داخل المؤسسة و في كل مراحل الحماية ، فتوفير كل وسائل الأمن المعلوماتي دون يقظة و دون دراسة للمحيط أمر غير مجد ، و هذا ما سيتم دراسته في الفصل الثالث الذي يشرح السياسة الكاملة لأمن المعلومات.

الفصل الثالث : استراتيجية أمن المعلومات في المؤسسة

المبحث الأول : الجانب التنظيمي لأمن المعلومات في المؤسسة

المطلب الأول : : السياسة الأمنية و وثائقها

المطلب الثاني : الجانب البشري في عملية أمن المعلومات

المبحث الثاني : عملية تسيير المخاطر

المطلب الأول : تحديد عناصر الخطر و تشخيص البنية التحتية

المطلب الثاني : تحليل المخاطر

المطلب الثالث : معالجة المخاطر و الفحص و التدقيق في برامج تسيير المخاطر

المبحث الثالث : نظام إدارة أمن المعلومات و الايزو 27001

المطلب الأول : معيار الايزو 27001

المطلب الثاني : نظام ادارة أمن المعلومات

المطلب الثالث : تطبيق الايزو 27001 حسب نموذج PDCA

تمهيد

تحقيق أمن المعلومات داخل المؤسسة يتطلب دراسة شاملة لكل الجوانب ، فالجانب المادي للأمن أساسي إذ من الضروري توفير كل الوسائل المادية و البرمجية من أجل التصدي لكل أنواع التهديدات الممكنة و حماية ممتلكات المؤسسة ، و لكن وضع أحسن و أحدث البرمجيات ، و توفير أحسن الحمايات المادية دون تنظيم و دراسة شاملة و استراتيجية لمفهوم الأمن و طبيعة النظام أمر غير مجد ، فالجانب التنظيمي للأمن هو أهم جانب على مستوى المؤسسة ، إذ أن عملية الأمن عملية دقيقة تتطلب خطة استراتيجية متمثلة أولا في تحضير السياسة الأمنية و وثائقها و تقسيم الأدوار و المسؤوليات و تحسيس و تكوين الموظفين في هذا المجال ، ثانيا من الضروري وضع خطة شاملة لكيفية التعامل مع المخاطر و التي تسمى بعملية تسيير المخاطر و التي من خلالها يتم تحليل بيئة المؤسسة و توقع المخاطر المحتملة و تحليلها باستخدام عدة أدوات و اقتراح معايير المعالجة الضرورية ، و أخيرا بما أن المعيار المتعلق بهذا المجال هو معيار ايزو 27001 فعلى المؤسسة التي تسعى لتطوير نفسها في مجال الأمن أن تكيف نظام ادارة أمن المعلومات لديها حسب شروط هذا المعيار من أجل الحصول على المصادقة.

و من خلال هذا الفصل سيتم توضيح الاستراتيجية الواجب على المؤسسة اتباعها لتحقيق أمن المعلومات ، ففي المبحث الأول سيتم توضيح الجانب التنظيمي لأمن المعلومات من خلال السياسة الأمنية و وثائقها و كيفية التعامل مع الجانب البشري من تقسيم المسؤوليات و إقام دورات التكوين و التحسيس ، أما المبحث الثاني فسيخصص لعملية تسيير المخاطر داخل المؤسسة ، من أول خطوة و هي تحديد عناصر الخطر و تشخيص البنية التحتية مرورا بتحليل المخاطر و أهم الطرق الخاصة بذلك إلى غاية كيفية معالجتها في حال وقوعها أما المبحث الثالث فيتم التطرق فيه لنظام ادارة أمن المعلومات و شهادة الايزو 27001.

المبحث الأول : الجانب التنظيمي لأمن المعلومات في المؤسسة

أمن المعلومات اليوم لم يعد مرتبطا بتركيب أحدث مضاد للفيروسات أو أقوى جدار ناري أو اعتماد أحدث أدوات المراقبة ، لأن نطاق الأمن توسع جدا و أصبح متعلقا بكل العمليات اليومية داخل المؤسسة ، و لا يمكن التحكم فيه و تحقيق مستوى أمن عالي إلا إذا كان تنظيم هذه العملية واضحا للجميع ، فالخطوة الأولى لتعزيز الأمن داخل المؤسسة هو إدخال سياسات و إجراءات أمن معلومات دقيقة و قابلة للتطبيق ، و إعلام الموظفين بمختلف جوانب مسؤولياتهم ، و تكوينهم و تحسيسهم ، و توضيح كيفية التعامل مع المعلومات الحساسة.

المطلب الأول : السياسة الأمنية و وثائقها

السياسة الأمنية هي عبارة عن خطة شاملة لعملية الأمن المعلوماتي و كيفية تطبيقه داخل المؤسسة ، تكون على شكل وثيقة تضم أساسيات الأمن ، يرافق هذه السياسة وثائق أخرى مفصلة كالدستور و القواعد و الاجراءات.

الفرع الأول : تحديد نطاق السياسة الأمنية

من غير المفيد المباشرة في عملية الأمن دون تحديد الأصول الواجب حمايتها و مستوى الأمن الحالي للمؤسسة :

1- تحديد الأصول الواجب حمايتها :

كل منظمة راغبة في حماية أنظمتها و شبكاتها يجب أن تحدد نطاق الأمن الذي يشمل الهيئات المادية و غير المادية.[1] هذه الهيئات خصوصا غير المادية تمثل البنية التحتية التي بدونها لا يمكن أن تتواجد نظم المعلومات ، اتاحة هذه البنية التحتية يجب أن تكون محمية ، و تشمل : الخوادم ، الشبكات ، قواعد المعطيات ، محطات العمل ، البرامج ...[2]

و أهم خطوة في تحديد الأصول و النطاق هو تصنيف المعلومات و تحديد المعلومات الحساسة ، هذه العملية كما أنها الحجر الأساسي لبناء سياسة أمنية إلا أنها يمكن أن تمثل نقطة ضعف سياسة الحماية لأنها عملية معقدة و خطرة ، إذ يمكن أن تقود المؤسسة إلى درجة نسيان الهدف الذي هو : حماية المعلومات الضرورية و الحرجة للمؤسسة ، و هذا إذا تم الخوض فيها أكثر من اللازم.[3]

---

[1] **Laurent Bloch , Christophe Wolfhugel** , « Sécurité informatique : principe et méthodes » , 3eme édition, ed Eyrolles, 2011,p10.

[2] **Laurent Bloch , Christophe Wolfhugel** , « Sécurité informatique : principe et méthode à l'usage des DSI ,RSSI et administrateurs » , 2eme édition, ed Eyrolles, paris 2009,p210.

[3] **Stéphane Rouhier** , étude « protection de l'information –enjeux, gouvernance et bonnes pratiques», Cigref, 2008, p17.

هذه العملية تكمن في تعريف و فهرسة المعلومات التي تحتاج إلى معايير حماية ، و هذا يتطلب العمل و الاتصال مع مختلف مصالح المؤسسة : التقنية ، مكاتب الدراسات القانونية ، الملكية الفكرية ، التجارية ، المالية....، و هذه المرحلة تتطلب تدوين المعطيات ، و كل مصلحة تدون المعطيات الحساسة لديها[4].

إذ يمكن القول أنه تعتبر معطيات حساسة يجب أن تخضع لمعايير حماية مكثفة كل المعطيات ذات نوع :[5]

– معطيات علمية غير منشورة مرتبطة بطلب البراءات، أشكال أخرى من تراخيص البحث أو المهارات الواجب حمايتها.

– المعطيات العلمية ، الإدارية ، وثائق العقود ، المعطيات المالية و المحاسبية ، المعلومات السياسية أو الاستراتيجية الداخلية و الوزارية.

و لتقييم و تصنيف مدى سرية و حساسية المعلومات بالمنشأة ، و لتحديد نوع و درجة الحماية الأمنية فان المحددات الممكن اعتمادها هي :[6] فائدة المعلومات ، أهمية و قيمة المعلومات ، عمر المعلومات ، حجم الخسائر التي قد تلحق بالمنشأة عند كشف المعلومات أو عند حدوث تعديل أو تلف بالمعلومات ، القوانين و اللوائح و المسؤوليات الخاصة بحماية المعلومات ، مدى تأثر الأمن بهذه المعلومات ، من المصرح له باستخدام المعلومات ، من الذي سيقوم بصيانة المعلومات ، أين ستحفظ المعلومات ، أي نوع من المعلومات يحتاج إلى تصنيف خاص.

2- تحديد مستوى الأمن :

لمعرفة المستوى الحقيقي لأمن نظم المعلومات يقوم مسؤول أمن المعلومات بالتعرف على أعوانه الأساسيين لتكوين رؤية مناسبة للمنظمة و نظم المعلومات ، و يطلب من كل واحد حسب نشاطه و كفاءته تحديد التطبيقات المطبقة في مجال الأمن ، بعد هذا كله يكون لديه العناصر الكافية لتحرير "التقرير" ، بمعنى وثيقة توضح الثغرات الأمنية في كل جانب من نظام المعلومات ، هذه الوثيقة تحدد المستوى الحقيقي لأمن نظم المعلومات.[7]

و يمكن عموما تقسيم مستويات الأمن إلى ثلاثة مستويات :[8]

[4] Guide pratique du Medef , la protection des informations sensibles des entreprises , paris, janvier ,2013 ,p7.

[5] **Laurent Bloch** , 2009 ,op.cit ,p 210.

[6] مقدمة عن سياسات و معايير أمن المعلومات ، المركز القومي للمعلومات – قسم الجودة و التطوير – الاصدارة الأولى ، فبراير 2010 ، جمهورية السودان - ص 09

[7] **Alexandre Fernandez-Toro** , « Sécurité opérationnelle , conseil pratique pour sécuriser le SI », Eyrolles, 2éme édition, 2016,p05.

[8] Ibid , pp 6-10.

أ- **منطقة الهوان** :هو المستوى الذي نجد فيه العديد من الثغرات المعروفة و سهلة الاستغلال من قبل المهاجمين ما قد يسمح لهم بالسيطرة الكلية على نظم المعلومات ، ما يؤدي إلى نتائج كارثية على المؤسسة. نظم المعلومات المتواجدة في "منطقة الهوان " تعتمد عموما إجراءات حماية أولية مثل : كلمات المرور ، برامج مكافحة الفيروسات، الجدران النارية ، و الإجراءات الأمنية غالبا تتوقف هنا.

ب- **مستوى الأمن الأساسي** : هذا المستوى أعلى و أحسن من منطقة الهوان ، و يسمح لنظام المعلومات الصمود في وجه الهجمات متوسطة الخطورة ، و لكن الاصابات الخطيرة على نظام المعلومات تبقى ممكنة.

ت- **مستوى الأمن المتطور**:في مستوى الأمن المتحكم فيه كل ما هو من المعقول تحقيقه بالوسائل و الوقت المتاح تم فعله، و لتعريض نظام في هذا المستوى للخطر على المهاجم تصور هجمات معقدة، و هذا يتطلب خبرة حقيقية.

الفرع الثاني : تعريف السياسة الأمنية

بعد تحديد نطاق أمن المؤسسة و المستوى الأمني الذي تقف عليه يأتي دور إعداد السياسة الأمنية المناسبة لنطاق و مجال المؤسسة ، فما هي السياسة الأمنية ؟ و ماذا تحتوي ؟

أ- **تعريف السياسة الأمنية** :

- السياسة الأمنية عبارة عن وثيقة رسمية تقدم القواعد التي يمكن أن تكون محررة تحت شكل تعليمات يجب تبنيها من أجل تطبيق جيد لأمن المعلومات، و تكون ملائمة و قابلة للاستعمال ، مطابقة للتشريعات ، دقيقة و مرنة في نفس الوقت.[9]
- سياسات أمن المعلومات هي قواعد عملية و فنية موثقة لحماية جهة ما من مخاطر أمن المعلومات التي تحدق بأعمالها و بنيتها التحتية التقنية ، و وثيقة السياسة الأمنية المكتوبة تقدم وصفا عاما للضوابط المختلفة التي ستستخدمها المؤسسة لإدارة مخاطر أمن المعلومات.[10]
- السياسات : عبارة عن قوانين تسيطر على نظام المعلومات و تزوده بمستوى حماية موثوق به ، تصدر هذه السياسة جهة مسؤولة تقر بمسؤوليتها تجاه أمن و حماية معلومات المنشأة من كل مصادر التهديد.[11]

[9] **Jean François Carpentier** , « la sécurité informatique dans la petite entreprise « état de l'art et bonnes pratiques » », éditions Eni , France , 2012, 2éme édition , p47 , pp49-51.

[10] إطار سياسات و إجراءات أمن المعلومات "الدليل الارشادي لسياسات و إجراءات أمن المعلومات للجهات الحكومية السعودية "، المركز الوطني الارشادي لأمن المعلومات ، الطبعة الأولى ، 1436 ، السعودية ، ص 13.

[11] المركز القومي للمعلومات ، السودان ، مرجع سابق ، ص 10 .

و بناءً عليه فان سياسة أمن المعلومات للمؤسسة هي عبارة عن وثيقة تصدرها جهة مسؤولة، تضم مجموعة من القواعد العملية ، بلغة بسيطة يفهمها الجميع من أجل تطبيق جيد لأمن المعلومات ، و يتم مراجعتها و تحديثها دوريا.

ب– أهمية السياسة الأمنية :

ترافق السياسة الأمنية تطور أهداف المؤسسة سواء كانت كبيرة أو صغيرة ، و خفض ثغراتها و مخاطرها إلى مستوى مقبول و مسيطر عليه[12] ، إذ أن سياسات أمن المعلومات تقدم إطاراً لأفضل الممارسات الممكن اتباعها من قبل جميع الموظفين ، و تساعد على التأكد من خفض المخاطر إلى الحد الأدنى ، و من أن الاستجابة تتم تجاه أية حوادث أمنية بصورة فاعلة ، كما تساعد السياسات على إشراك الموظفين في جهود الجهة المعنية لتأمين أصولها المعلوماتية ، و التنفيذ الملائم للسياسات يخفف المخاطر الناتجة عن أخطاء "العامل البشري ".[13]

و عليه فان سياسة أمن المعلومات التي تكون على شكل وثيقة رسمية أصبح أمرا ضروريا لكل مؤسسة، فهي بمثابة الخطة الإستراتيجية للمؤسسة في مجال أمن المعلومات، تطبيقها الجيد و الالتزام بقواعدها يقي المؤسسة من الوقوع بعدة مطبات.

ث– إطار و شكل السياسة الأمنية:

أول نقطة يجب الانتباه إليها في تحضير السياسة الأمنية أن تكون هذه الأخيرة ملمّة بكل النواحي الأمنية في المنظمة، بمعنى تغطي محيط واسع. **ثاني** نقطة و هي ضرورة توافق السياسة الأمنية مع الاستراتيجية العامة للمؤسسة و احترام ثقافة المؤسسة الحالية، ما يؤكد استحالة استخدام سياسة واحدة في عدة مؤسسات، و استحالة نقل سياسة أمنية من مؤسسة و تطبيقها على أخرى ، إذ أن السياسة الأمنية تعبر عن هوية المؤسسة في مجال الأمن.

" فسياسة أمن المعلومات تحدد أسلوب الجهة في التعامل مع المعلومات ، و تعلن داخليا و خارجيا أن المعلومات هي أحد أصول تلك الجهة ".[14]

و يجب أن تكون سياسات الأمن دقيقة و قابلة للتطبيق، و تصف معنى الاستخدام المقبول و ذكر الأنشطة المحظورة، و تبليغ الموظفين بالجوانب المختلفة من مسؤولياتهم و الاستخدام العام للموارد، و توضيح كيفية التعامل مع المعلومات الحساسة.[15]

---

[12] **Jérôme Del Duca , Alexandre Planche** , « la sécurité informatique « organisez la sécurité du SI de votre entreprise » » , éditions Eni , Janvier 2012 , France , p198.

[13] إطار سياسات و إجراءات أمن المعلومات "الدليل الإرشادي ، السعودية ، مرجع سابق ،ص 14 ، ص 35.

[14] نفس المرجع ، ص 14.

[15] نفس المرجع ، ص 35.

تعريف ، تطبيق و متابعة قواعد الأمن يجب أن تسير كمشروع حقيقي يضم إدارة المؤسسة ، الأشخاص المكلفين بتسيير الوسائل المعلوماتية و الاتصالية و ممثلي المستخدمين ، و تخص كل الأجهزة و التكنولوجيات التي تساهم في دوران و تخزين المعلومة ، و أيضا وسائل الاتصال.[16]

أما بالنسبة لمسؤولية السياسة ، فإن هذه الأخيرة يجب أن يكون لها " مالك " سواء مجموعة أو فرد ، و ينبغي تخويل " مالك " السياسة الأمنية السلطة و الموارد الكافيين ، و أن يكون مسؤولا عن استمرارها و مراجعتها بانتظام ، و أن تكون السياسة واضحة يقرأها و يفهمها الجميع ، و أن يتم توضيح عواقب عدم الالتزام بما جاء فيها ، و يزداد تعقيد السياسات كلما زاد حجم المؤسسة.[17]

الفرع الثالث : وثائق السياسة الأمنية

إن مشروع أمن المعلومات في المؤسسة يحتاج إلى توثيق ، أولها وثيقة السياسة الأمنية ، إلا أن هذه الأخيرة تمثل الإطار العام فقط ، و من أجل تفعيلها يجب أن تستكمل بمجموعة من الوثائق تكون أكثر تفصيل و بساطة و موجودة باتساع على مستوى المؤسسة، و تتمثل هذه الوثائق عموما في : الميثاق "الدستور" المعلوماتي، القواعد، الارشادات الاجراءات.

1- الدستور المعلوماتي :

الدستور المعلوماتي هو عبارة عن وثائق توضح حقوق و واجبات كل مستخدم داخل المؤسسة ، و كيفية تعامله مع كل ما يخص المعلوماتية ، و يعالج النقاط التالية : المحظورات ، الالتزامات ، التقييدات ، بمعنى أبسط : ما هو مسموح به و ما هو محظور.

و يعرف على أنه : أداة قانونية حقيقية تسمح بإضفاء صفة الرسمية على مجموع حقوق و واجبات المستخدمين و المسؤول فيما يخص أمن استخدام و مراقبة أنظمة المعلومات ، و العمل على حفظ مصالح المسؤول دون المساس بمصالح المستخدمين.[18]

الهدف من هذه الأداة هو التذكير بالإطار القانوني المتعلق باستخدام أجهزة المعلوماتية و وسائل الاتصال الالكترونية ، إضافة إلى شروط وضع مراقبة استخدامها من قبل المسؤول.[19]

---

[16]:Document « Maitrise et protection de l'information » ,CLUSIF – **CLU**b de la **S**écurité de l'**I**nformation **F**rançais - , Paris , 2006 , p27

[17] ضمان أمن المعلومات للمديرين التنفيذيين : " دليل تأمين شبكات و أنظمة معلومات المؤسسات التجارية الدولية طبقا لأسس منظمة التعاون الاقتصادي و التنمية 2002 نحو ثقافة أمنية " ، غرفة التجارة الدولية ، منظومة الأعمال العالمية ، باريس 2003 ، ص 22.

[18] **Nicolas Moinet** , op.cit , p48.

[19] Ibid , p49.

هذا الدستور لا يجب أن يكون ذو حجم كبير ، ما يصعّب عملية تحديثه و لا يشجع على قراءته ، و من المهم أيضا تجنب التفاصيل التقنية من أجل عدم إضجار المستعملين ، لأن هذه الوثيقة موجهة لكل العمال من أفراد المصنع إلى المهندس ، يكفي أن يكون مختصر ، و من أجل تسهيل الولوج إليه من قبل الكل يمكن وضعه على انترانت المؤسسة ، أو توزيعه مع التنظيم الداخلي.[20]

أما إذا لم يوجد بعد ميثاق معلوماتي في المؤسسة ، فالوسيلة الوحيدة الفعالة هي التنظيم الداخلي.

الميثاق المعلوماتي لا يجب أن يكون مقيدا أكثر من اللازم ، و شأنه شأن السياسة الأمنية لا يمكن أن يحرره مسؤول أمن نظم المعلومات باستقلالية عن باقي المؤسسة، تحريره يتطلب على الأقل إطارين مسيرين مهمين في المؤسسة .[21]

2- **القواعد** : القواعد هي مبادئ قيادة ، تعرف التصرف الجيد الذي يجب تبنيه من قبل العون بفعل المكان أو الحدث الذي يواجهه ، لا يتعلق الأمر بالقواعد التقنية ، و إنما بالسلوكيات و التحفظ.[22]

3- **الإرشادات أو الدلائل** : هي عبارة عن توصيات إجرائية و دليل تشغيل و تنفيذ عمل للمستخدمين من موظفي التقنية ، و مشغلي الحاسوب و الآخرين من ذوي العلاقة عندما لا تكون هناك سياسة أو مواصفات لتطبيقها ، و يستدل الموظف بالدليل لتنفيذ العمل، إذ أنه يتمتع بمرونة التطبيق على عكس المواصفات التي يجب تطبيقها بدقة.[23]

4- الإجراءات : قواعد الأمن هدفها تحديد "من" و "ماذا "، إجراءات الأمن تقوم بتفصيل "كيف" بمعنى المنهجية المتبعه من أجل تحقيق النشاطات المطلوبة.[24] فهي تكمن في وصف المراحل المفصلة التي يجب اتباعها من قبل المستخدمين، مسؤولي الأنظمة و كل الأشخاص الذين عليهم تنفيذ مهمة خاصة متعلقة بحماية الارث المعلوماتي.[25]

و تأتي الاجراءات بعد تحديد السياسات الأمنية و تطبيقها ، و هي أقرب إلى المستخدمين و الأجهزة من السياسة الأمنية ، لأنها توفر الخطوات التفصيلية المطلوب القيام بها لتحقيق هدف معين ، كما تحدد الاجراءات كيفية

[20] **Patrick Boulet** , « Management de la sécurité du SI » , ed Lavoisier , Paris , 2007 , p174.
[21] **Jérôme Del Duca**, op.cit , p121 ,p 122.
[22] Ibid , p123.
[23] المركز القومي للمعلومات ، جمهورية السودان ، مرجع سابق ، ص 11.
[24] **Patrick Boulet , op.cit , p177.**
[25] **Jean François Carpentier** , 2012, op.cit , p51.

تطبيق السياسات الأمنية و المعايير و التوجيهات على أرض الواقع ، و كيفية نقلها من الطرح النظري إلى اجراءات واقعية تنفذ في بيئة تشغيلية حقيقية.[26]

وثائق السياسة الأمنية المذكورة لا يمكن أن نجدها مجتمعة في كل المؤسسات ، فبعض المؤسسات تعتمد فقط على الإرشادات أو الإجراءات أو القواعد ، و هناك من تعتمد فقط على التنظيم الداخلي ، و لكن أفضل تطبيق للسياسة هو الاعتماد على كل وثائقها الضرورية لأن كل توثيق له دوره المناسب.

المطلب الثاني : الجانب البشري في عملية أمن المعلومات

بعد الاتفاق على جميع السياسات و إجراءات أمن المعلومات و تحضير الوثائق الخاصة بها يأتي دور التنفيذ الذي يعتبر المرحلة الأصعب من سابقتها ، إذ تحتاج إلى توزيع ملائم للمسؤوليات و تدريب و تعليم جيد للموظفين للتصرف بشكل آمن و تحسيسهم بأهمية الالتزام بكل العناصر الأساسية التي نصّت عليها وثائق السياسة الأمنية.

الفرع الأول : تقسيم المسؤوليات

لكي يتحقق أمن المعلومات بالصفة المرغوبة ، من الضروري أن تكون المسؤوليات واضحة ، و هذا يختلف من مؤسسة لأخرى ، ولا يوجد نموذج يتبعه الجميع و لكن عموما يمكن تقسيمها كالتالي بالتدرج من مستوى لآخر:

1- **مسؤولية الادارة العليا** : مسؤولية الادارة العليا هي وضع الإطار العام لسياسات الأمن ممثلة بالرئيس المدير العام الذي يعتبر المسؤول العام عن السياسة الأمنية بصفته سلطة مؤهلة لأمن نظم المعلومات ، كما أن ضمان الأمن يتطلب تدخل الادارة العليا و إصدار تعليمات واضحة من القمة.

2- مسؤولية إدارة نظم المعلومات : التنظيم العملياتي لأمن نظم المعلومات هو من تحريك مدير مديرية نظم المعلومات بالتنسيق مع مسؤول أمن نظم المعلومات ، ومن أجل التسيير الجيد لهذه المهمة العملياتية ، مدير مديرية أمن نظم المعلومات يرتكز على مستوى مديريته على مسؤول الأمن العملياتي الذي يعتمد على جانب البنية التحتية من جهة و على المسؤولين المعلوماتيين الجهويين و المسؤولين المعلوماتيين للمواقع من جهة أخرى.[27]

[26] **ذيب بن عايض القحطاني** ، "أمن المعلومات "، مدينة الملك عبد العزيز للعلوم و التقنية ، الرياض ، 2015 ، ص 201

[27] **Laurent Bloch** ,2009 , op.cit , p 214.

3- مسؤولية مسؤول أمن نظم المعلومات:

أ- خصائص مسؤول أمن نظم المعلومات :

- الاسم الأكثر تداولا له هو : مسؤول أمن نظم المعلومات (RSSI[28])، ويمكن تسميته عون أمن نظم المعلومات (ASSI[29]) أو ضابط أمن نظم المعلومات (OSSI [30]).[31]

يمكن سماع شكاوى حول صعوبة تواجد مسؤول أمن معلومات في كل مكان ، و لكن عادة ما يقال أن مسؤول أمن المعلومات هو فريق من رجل واحد ، يشغل العديد من الأدوار في الأعمال الموكلة إليه تحقيقها [32].

- تعريف مسؤول أمن المعلومات و مهماته يختلف حسب كل شخص ، حسب خبرته بعدد السنوات أو اختلافها ، حسب المسار الذي حققه على مستوى مؤسسته ، حسب ثقافة و طبيعة عمل المؤسسة.[33]

- يجب أن يمتلك كفاءات لوظيفته ، إذ من الممكن أن يتحصل على شهادات خاصة بأمن نظم المعلومات مثل: شهادة CISSP[34] (شهادة محترف أمن نظم المعلومات) المحررة من طرف الجمعية االدولية ISC التي تطلب معارف جيدة في كل مجالات أمن نظم المعلومات (التشفير ، تسيير الدخول ، البنى التحتية مؤمنة ، مخطط استئناف العمل....) و شهادة CISM[35] (شهادة مدير معتمد لأمن المعلومات)المحررة من طرف جمعية ISACA[36] جمعية مراقبة و تدقيق نظم المعلومات موجهة أكثر لإدارة و تسيير المخاطر ، و إضافة إلى المعارف التقنية يجب إضافة معارف قانونية ، فمن غير المقبول أن يكون مسؤول أمن المعلومات مكلف إذا كان لا يعرف نصوص قوانين " الإعلام الآلي و الحرية ".[37]

- يجب أن يمتلك الميزانية الكافية لتطبيق سياسته الأمنية و التصدي لأي تهديدات ، و امتلاك الاستقلالية التامة في تطبيق المهمات الموكلة إليه .

- مسؤول أمن المعلومات يجب أن يكون صبور من أجل تغيير ثقافة المؤسسة و العمل على إدخال الأمن في عادات كل واحد دون افزاع ، فعمله كعمل النملة على المدى الطويل.[38]

---

[28] **RSSI** : **R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation
[29] **ASSI : A**gent de la **S**écurité des **S**ystèmes d'**I**nformation
[30] **OSSI : O**fficier de la **S**écurité des **S**ystèmes d'**I**nformation
[31] **Patrich Boulet** , op.cit , p 38.
[32] **Bernard Foray** , « la Fonction RSSI « guide des pratiques et retours d'expériences » » , ed Dunod , Paris , 2010, p p 17,18.
[33] Ibid , p17.
[34] **CISSP : C**ertified **I**nformation **S**ystem **S**ecurity **P**rofessional
[35] CISM : **C**ertified **I**nformation **S**ecurity **M**anager.
[36] **ISACA : I**nformation **S**ystem**s** **A**udit and **C**ontrol **A**ssociation
[37] **Patrick Boulet** , op.cit , p 39 , p 53.
[38] **Bernard Foray** , op.cit , p p 19- 20 .

ب- فوائد مسؤول أمن المعلومات : هو مفيد على مستويين :[39]

- يسمح أولا بوضع و ضمان احترام استراتيجية الأمن ، و يضمن وضع و متابعة الاجراءات التقنية و التنظيمية، و الحفاظ على مستوى أمن المنظمة مع البقاء في الاستماع لتطور المشاكل و حلول الأمن.
- إضافة إلى هذه المهام فان تواجد مسؤول الأمن يسمح للمنظمة بالاستثمار الجيد للميزانية المخصصة لأمنها، هذا مع معارفه التي يمكن من خلالها أن يساعد المؤسسة باختيار أفضل الحلول التقنية و التخلي عن الحلول غير المجدية.

ت- **مهام و مسؤوليات مسؤول أمن المعلومات** : هو المسؤول المباشر عن عملية أمن نظم المعلومات داخل المؤسسة ، قبل شروعه في تحضير مخطط الأمن عليه معرفة عدة نقاط : احتياجات المصالح العملياتية في مجال الوصول للأنظمة و التطبيقات المعلوماتية ، المعوقات التنظيمية ، تنظيم الموارد البشرية ، الضوابط القانونية ، المخاطر المعروفة ، ضوابط الميزانية .....[40] بمعنى جرد البنية التحتية. و بعد نهاية هذا الجرد تأتي مجموعة من المهام قبل و خلال و بعد تطبيق السياسة الأمنية ، أهمها :

- نصح هيئة الادارة في اختيار المعايير المناسبة و التأكد من احترام القواعد الملقاة من طرفها.[41]
- تحضير الوثائق الخاصة بالسياسة الأمنية : وثيقة السياسة الأمنية ، الدستور المعلوماتي ، الاجراءات ، القواعد و الدلائل و محاولة نشرها بشكل فعال.
- تعريف متطلبات الأمن لمجموع أنظمة المعلومات على ضوء قاعدة سياسة الأمن العامة للمؤسسة.[42]
- التخطيط للنشاطات الخاصة بتطبيق سياسة أمن نظم المعلومات و مراقبة تطبيقها و نتائجها.[43]
- تحسيس المستخدمين بالقواعد الأساسية للأمن باحترامها و تذكرها المستمر و تكوينهم حول المنهجيات الواجب تطبيقها ، و الأدوات الواجب استعمالها بهدف تحسين مستوى الأمن.[44]
- المتابعة و المراقبة المستمرة و الاستجابة الفورية للحوادث الأمنية و معالجتها ، و وضع لوحات التحكم في مختلف المجالات.

---

[39] **Didier Godart** , op.cit , p176
[40] **Patrick Boulet** , op.cit. , p57.
[41] **Didier Godart** , op.cit , p176.
[42] **Bernard Foray** , op.cit , p 21.
[43] « Politique de sécurité des systèmes d'information de l'état – version 10 -»publication de l'agence nationale de la sécurité des systèmes d'information , 17/07/2014 ,paris , p14.
[44] **Patrick Boulet** , op.cit , p57.

– تعريف العائد على الاستثمار في المشاريع التي يقدمها ، فوظيفة الأمن مثلها مثل الوظائف الأخرى عليها تخفيض تكاليفها و رفع استثماراتها ، و قياس العائد على الاستثمار في الأمن هو عملية صعبة و تتطلب مجهود كبير من قبل مسؤول أمن المعلومات.

هناك مؤسسات صغيرة و متوسطة لا نجد فيها منصب مسؤول أمن نظم المعلومات ، هنا قد نجد أحيانا أن مدير مديرية نظم المعلومات هو من يتكفل بهذه الأنشطة داخل المؤسسة ، و قد يكون مسؤول أمن نظم المعلومات شخص واحد و قد تكون هيئة مسؤولة عن الأمن متكونة من عدة مسؤولين تختلف مهامهم من مؤسسة لأخرى.

4- مسؤولية مالكي الأصول المعلوماتية :

تؤول ملكية المعلومات و نظم المعلومات و أصولها إلى جهات أو أفراد داخل المنشأة ، و يكون المالك هو المسؤول المباشر عن كل ما يتعلق بتأمين المصادر تحت ملكيته[45]، عليه أن يدرك أن الوثائق و أنظمة المعلومات هي انشغال ضروري بالنسبة لموارده البشرية ، عليه تحسيس العمال و ضمان أن وسائل الأمن تستخدم بطريقة صحيحة ، فهو المسؤول الأول عن الأمن و عليه رؤية أن كل المعايير الأمنية المتخذة هي مطبقة[46]، بمعنى هو مسؤول عن ضمان أن الأمن المطبق المتناسق مع سياسة أمن المؤسسة مندمج في أنظمتهم المعلوماتية.[47]

5- مسؤولية المراسل المعلوماتي :

من أجل التطبيق الجيد لوظيفة أمن نظم المعلومات ، من الضروري أن تضم كل وحدة من وحدات المؤسسة مراسل معلوماتي للوحدة يكون في اتصال منتظم مع مسؤولي البنى التحتية و الشبكة[48]، و تختلف طبيعة الاتصال و التواصل بين المراسل و مسؤولي الأنظمة حسب طبيعة المؤسسة :[49]

– في مؤسسة جد مركزية و مهيكلة ، وظيفة المراسل المعلوماتي تعرف على شكل عملياتي ، و يكون هناك تعليمات محددة للتطبيق و يجب أن تعطي مردودية تطبيقها.

– في مؤسسة ذات بنية أكثر ارتخاء ، منظمة بحث مثلا : علاقات الاتصال تكون أقل قطعية ، و لكن مع ذلك من المهم تواجده و لو على شكل محادثات منتظمة بجانب جهاز القهوة.

طبيعة التواصل بين المراسل و مسؤولي الأنظمة تتكيف مع الوضعية المحلية للمؤسسة ، و تحمل العناصر التالية:[50]

---

[45] "مقدمة عن سياسات و معايير أمن المعلومات "، المركز القومي للمعلومات ، جمهورية السودان ، مرجع سابق ص 08

[46] **Marilyn Thibault , Guylaine Marcoux et autres** , politique sur l'accès , la sécurité de l'information et la protection des renseignements personnels , version du janvier 2010 , société d'habitation du Québec , p07.

[47] **Michael .P. Cangemi** et autres , Manager la sécurité de l'information , la revue n 85 , février.

[48] **Laurent Bloch** , 2009 , op.cit , pp 214 215.

[49] **Laurent Bloch** , 2011 , op.cit , pp 15-16.

[50] **Laurent Bloch** , 2009 , op.cit , p 215.

- ارتفاع المعلومات المتعلقة بحوادث الأمن.
- ارتفاع المعلومات المتعلقة بالحوادث التقنية.
- نشر التحديثات الأمنية للبرامج خاصة مكافحة الفيروسات.
- نشر انذارات و معلومات الأمن .

6- مسؤولية المستخدمين :

المستخدمين هم الأشخاص الذين يتعاملون مع البيانات و الأنظمة بشكل يومي ، و تكمن مسؤولياتهم في استخدام الأنظمة المعلوماتية في حدود صلاحياتهم ،كل حسب منصبه ، واحترام القوانين و التنظيمات الموجودة في المؤسسة و الخاصة بمجال عملهم ، واحترام كل توثيق خاص بالسياسة الأمنية تبنته المؤسسة سواء وثيقة سياسة أمنية ، دستور معلوماتي ، إجراءات ، قواعد ، دلائل ...و الابلاغ عن أي تهديد أو استخدام غير مشروع.

الفرع الثاني : التكوين و التحسيس

على الرغم من ضرورة الحفاظ على سرية الترتيبات الأمنية ، إلا أن العامل البشري يمثل الحلقة الأضعف في أمن المعلومة ، و من الضروري أن تتحقق لديه ثقافة أمنية تحسن من تصرفاته و ترفع من قدراته في مجال أمن المعلومات، و لا يتم ذلك إلا برفع الوعي و التحسيس و تكثيف التكوين.

1- **التحسيس** : عملية التحسيس هي أحد العوامل الضرورية لنجاح السياسة الأمنية داخل المؤسسة و تضم عدة نقاط نذكر :

- يجب أن يفهم كل موظف داخل المؤسسة دوره و مسؤوليته في مجال ضمان الأمن ، و مع من يتعامل.[51]
- اشراك الأفراد في الأمور المتعلقة بالوصول إلى معلومات حساسة ، و أن يكونوا واعين بما هو سري لأخذ الاحتياطات اللازمة عند أي تواصل خارجي لتفادي أي افشاء غير مقصود.[52]
- خلال حصة التحسيس من الضروري ترك فرصة للمستخدمين من أجل التعبير عن رأيهم و كشف الثغرات الأمنية بالمؤسسة ، و السماح لهم بإعطاء أفكار و حلول و مشاركتهم في عملية اتخاذ القرار.[53]
- تذكير المستخدمين بالإطار القانوني و العقوبات الناتجة عن التصرفات الطائشة.[54]

[51] ضمان أمن المعلومات للمديرين التنفيذيين : دليل تأمين شبكات و أنظمة معلومات المؤسسات التجارية الدولية ، 2003 ، مرجع سابق ، ص 20.
[52] Guide pratique du MEDEF, op.cit , p 11.
[53] **Nicolas Moinet , op.cit** , p53
[54] Ibid , p53

- **التواصل المباشر مع المستخدمين** من أجل تقييم الفجوة بين العملية الأمنية و فهمها و تطبيقها على الواقع، فتقديم دستور أو نشر إجراء هو أمر غير كافي للمصالح العملياتية[55] إذا لم يستكمل بالاحتكاك مع المستخدمين و شرح ما جاء في الوثائق الأمنية.

- **تحفيز المستخدمين** و توليد الاهتمام لديهم بمجال أمن المعلومات و إفهامهم بطبيعة المخاطر الأمنية و التهديدات التي قد تصادفهم ، ليس لإقلاقهم و انما لرفع الوعي و روح المسؤولية لديهم.

- **رفع فاعلية فرق التحسيس** : التحسيس ليس بالأمر الهين ، إذ يعتبر تحدي لأغلب مسؤولي أمن أنظمة المعلومات ، فالفرق الكلاسيكية يغيب فيها التأثير ، و لا تحقق أهدافها بفعل اعتمادها المطلق على نشر الرسائل التي لا تصل و لا تؤدي مفعولها و سرعان ما تنسى ، على عكس فرق التحسيس الحديثة التي تعتمد في طرق تحسيسها على بعض التصرفات الفعالة ما يرفع قدرة حفظ المعلومة في الذاكرة .[56]

و بالتالي ليس التحسيس عن طريق إلقاء المواعظ و نشر القواعد ما يحقق الفعالية ، و إنما التحسيس بالتطبيق و إعطاء الأمثلة التي يفهمها المستخدم البسيط هو ما تحتاجه المؤسسة.

- **تحسيس الادارة و أصحاب الاعلام الآلي** : هذه العملية جد مهملة ، مع أنها أساسية لأنهم هم الأكثر تعاملا مع الموضوع ، و لكن الأقل تحسيس بحقوقهم و واجباتهم[57] يجب رفع وعيهم بقيمة الأصول التي تحت أيديهم ، و أن مسؤوليتهم مضاعفة ، و تغيير وجهة نظرهم نحو العملية الأمنية التي أصبحت روتينا لديهم.

2- التكوين:

من أجل تفادي أن يكون المستخدمين الحلقة الأضعف في سلسلة الأمن فان تكوينهم ضروري ، إذ في كثير من الأوقات المعلومة البسيطة التي يتم نشرها لا تكفي ، و لمعالجة مواضيع حساسة و معقدة من الضروري القيام بحصص تكوين حقيقية ، و ادماج هذه الحصص في إطار التكوين المستمر لإعطاء فائدة إضافية ، و تعتبر أفضل الوسائل للمستخدمين من أجل اكتساب المهارات المطلوبة.[58]

يجب أن يتكيف التدريب مع السياسة الأمنية و مستوى الموظفين ، و أن يلتزم الموظفين بتلقي التدريب و التعليم الأمني الاختياري على المستوى المناسب لعملهم حسب نوع المعلومات التي يمكنهم الاطلاع عليها و احتياجات المؤسسة ، و ينبغي تقديم التدريب في بداية التوظيف و بعد ذلك يقدم دوريا.[59]

---

[55] **Patrick Boulet** , op.cit , p179.

[56] **Matthieu Bennasar et autres** , « Sensibilisation à la sécurité de l'information 2.0 » , livre blanc , Lexis , Paris , p2.

[57] **Stéphane Rouhier** , étude « protection de l'information- enjeux , gouvernances , et bonnes pratiques » , Cigref , 2008 , p22 ,p24.

[58] **Patrick Boulet** , op.cit , p179.

[59] ضمان أمن المعلومات للمديرين التنفيذيين ، مرجع سابق ، ص20.

و كما ذكرنا عن طريقة التحسيس الفعالة ينطبق ذلك على التدريب ، فالتدريب المثالي لا يقتصر على إلقاء النظريات فقط أو التطبيق المباشر دون مقدمات و إنما الطرح النظري يتبعه التطبيق.

و يشتمل التدريب و التوعية سواء كان يتم التعامل معهما كوحدة واحدة أو منفصلين على ثلاثة مستويات :[60]

- **المستوى الأعلى** : و هو مستوى عام و شامل يحتوي مواد تدريبية و توعوية ، قصيرة المدة ، عامة المفاهيم ، لمعرفة الخطوط العريضة لكل من السياسات الأمنية و المعايير القياسية و التوجيهات و الاجراءات ، دون الدخول في التفاصيل و يستهدف المستويات العليا من إدارة المنشأة.

- **المستوى المتوسط** : متوسط الشمولية ، و يحتوي مواد تدريبية و توعوية متوسطة المدة و متوسطة التفاصيل، و يستهدف المهندسين و الاستشاريين و رؤساء الأقسام.

- **المستوى الأدنى** : و هو مستوى تفصيلي يحتوي مواد تدريبية و توعوية طويلة المدة ، تحتوي معلومات تفصيلية عن كيفية تطبيق السياسات الأمنية و المعايير و الاجراءات خطوة بخطوة على أرض الواقع ، و يستهدف الأفراد و الجهات التنفيذية من فنيين و مستخدمين.

الفرع الثالث : مكانة مصلحة أو مسؤول أمن نظم المعلومات في السلم التنظيمي

تختلف مكانة ادارة أمن نظم المعلومات من مؤسسة لأخرى ، فمثلا المؤسسات الصغيرة و المتوسطة أغلبها لا يملك مصلحة أو مسؤول أمن معلومات معرّف ، و إنما توكل هذه المهمة إلى مدير نظم المعلومات ، أما المؤسسات الكبرى فغالبا ما نجد فيها مسؤول أو مصلحة خاصة بالأمن و لكن أين يمكن أن تتموقع هذه المصلحة أو هذا المسؤول؟

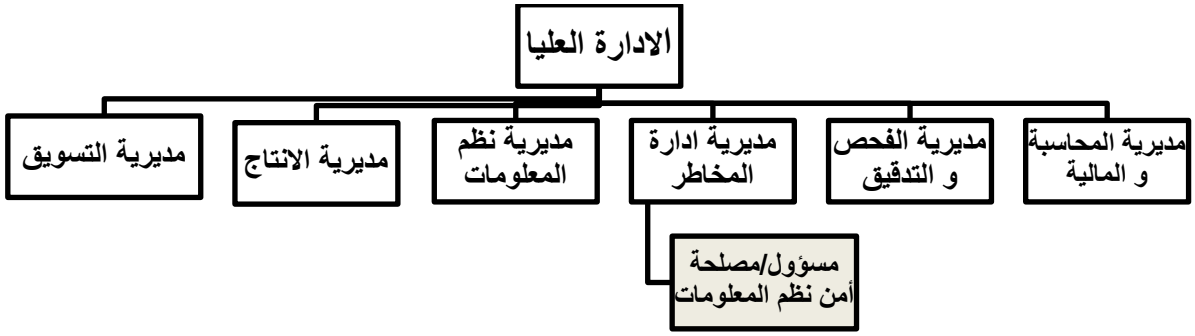
مسؤول أمن المعلومات يمكن أن يرتبط تسلسليا بعدة جهات من المؤسسة ، و قد يكون توجهه غالبا نحو ادارة مخاطر المؤسسة.[61]

قد يكون الهدف من هذا التوجه أن يكون المسؤول على دراية بكل التهديدات و المخاطر التي قد تتعرض لها الأنظمة و المعلومات ، و كيفية التعامل معها ليكون التحرك في الوقت المناسب.

[60] ذيب بن عايض القحطاني ، أمن المعلومات ، مرجع سابق ، ص ص 208 209.

[61] **Bernard Foray** , 2010 ,op.cit , p 21.

الشكل (3.1): مسؤول أمن المعلومات تابع لمديرية ادارة المخاطر



المصدر : من اعداد الطالبة بناءا على المعلومات المذكورة

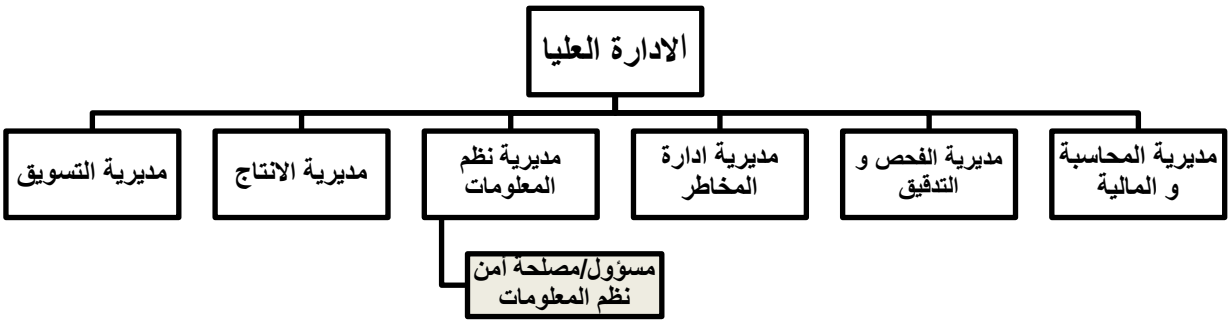
و حسب تحقيق Clusif فإن مسؤول أمن نظم المعلومات مرتبط بمديرية نظم المعلومات في 41 % من الحالات، بالإدارة العامة في 39% من الحالات و بمديرية وظيفية فيما تبقى.[62]

و بالتالي فان الأمر المعروف و الأكثر رواجا هو ارتباط مسؤول أمن نظم المعلومات بمديرية نظم المعلومات ،

و لكن لماذا هل هو صدفة أم خيار مدروس؟

مسؤول الأمن الموجود على مستوى مديرية نظم المعلومات له ضمان امتلاك كل المعلومات التقنية الضرورية لوظيفته لأنه سيكون في اتصال يومي مع المختصين في مجاله.[63]

الشكل (3.2) : مسؤول أمن المعلومات تابع لمديرية نظم المعلومات



المصدر : من اعداد الطالبة بناءا على المعلومات المذكورة

كل هذا منطقي ، و لكن ارتباط مسؤول أمن نظم المعلومات بمديرية معينة سواء ادارة المخاطر أو نظم المعلومات هل يعطي له الصلاحيات الكاملة و الحرية و الموضوعية لأداء مهامه على أكمل وجه ؟ إذ أنه من الممكن أن

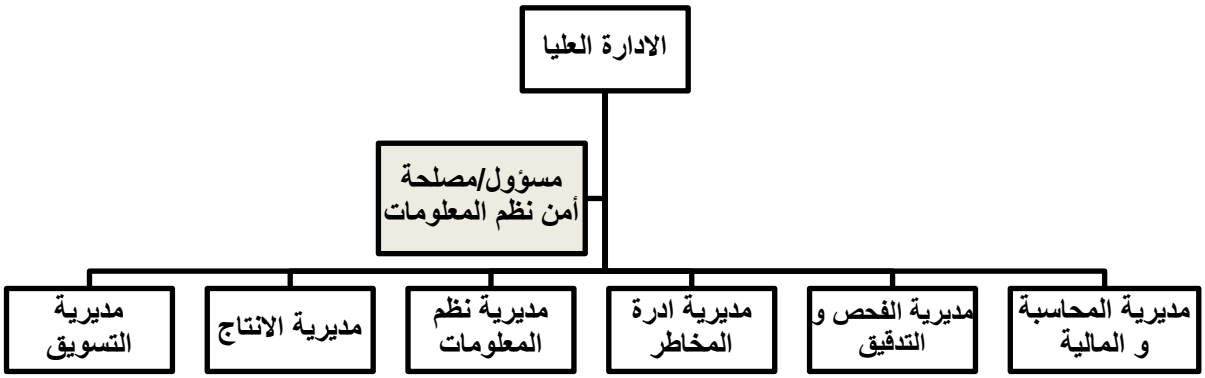
[62] **Patrick Boulet** , op.cit , p37.
[63] ibid , p37.

يتصادم رأيه حول مسألة مع رأي مديره الذي هو أعلى منه في السلم التنظيمي و بالتالي يكون هناك تقييد لعمله الذي قد يكون في غير صالح المؤسسة.

لتفادي المشاكل و الحساسيات التي قد تنتج بين مسؤول أمن نظم المعلومات مع مديريه ، نلاحظ اليوم رواجا كبيرا لارتباط مسؤول أمن نظم المعلومات بالإدارة العامة خصوصا في المؤسسات الكبرى ، و بالتالي تكون مهمته واضحة و قراراته مستقلة ، و يمكن ارتباطه بالإدارة العليا على شكلين:

أ- أن يكون متمركز على مستوى الادارة العليا:

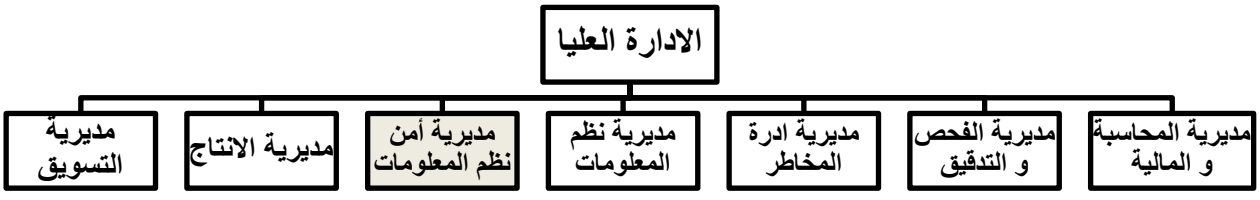
الشكل (3.3): مسؤول أمن المعلومات تابع مباشرة للإدارة العليا



المصدر : من إعداد الطالبة بناءا على المعلومات المذكورة

ب- **أن تكون مصلحة أمن نظم المعلومات مديرية مستقلة:**

الشكل (3.4) : مديرية أمن المعلومات مديرية مستقل



المصدر : من اعداد الطالبة بناءا على المعلومات المذكورة

المبحث الثاني : عملية تسيير المخاطر

عملية تسيير المخاطر هي جزء أساسي في الادارة الاستراتيجية للمؤسسة ، و هي الاجراءات التي تتبعها المؤسسة لمواجهة التهديدات المصاحبة لأنشطتها ، و أول خطوة في هذه العملية هي تحديد النطاق الواجب حمايته و عناصر الخطر الممكنة ، تليها عملية تحليل المخاطر ، من أجل الوصول أخيرا إلى معايير و أساليب المعالجة.

المطلب الأول : تحديد عناصر الخطر و تشخيص البنية التحتية

عملية تسيير المخاطر عملية دقيقة و حساسة ، و من أجل الوصول إلى النتائج المرجوة من الضروري القيام بتشخيص عام لبيئة المؤسسة و معرفة العناصر الأكثر عرضة للخطر و العناصر البعيدة عن الخطر لاتخاذ الاجراءات المناسبة ، كما أنه من الضروري معرفة أهم عناصر الخطر.

الفرع الأول :عناصر الخطر

أولا : تعريف الخطر و عملية تسيير المخاطر

أ- **الخطر** : الخطر هو توقع الأثر الذي يمكن أن ينتج عن استغلال ثغرة ممتلك من قبل تهديد ، و يعتبر مطابق في حالة تضمن ثغرة أو عدة ثغرات يمكن أن تستغل من قبل تهديد حقيقي ، و أيضا يتسبب في أثر غير مقبول.[64]

و يعرف أيضا بترتيب احتمالية الحدث و نتائجه : الخطر = التهديدات*الثغرات*الأثر ، و تعتبر هذه المعادلة الأكثر انتشارا في تسيير المخاطر ، و تمثل أساسا في تعريف و تقييم الخطر.[65]

ب- تسيير المخاطر

تعرف " ايزو " تسيير المخاطر كمجموع النشاطات المنسقة الهادفة إلى إدارة و قيادة المنظمة تجاه الخطر.

و تتكون عملية تسيير المخاطر من ثلاث أقسام : الممتلكات و الاحتياجات الأمنية ، ثم المخاطر المتعرضة لهذه الممتلكات ، و أخيرا المعايير المأخوذة لمعالجة المخاطر ، و بالتالي ضمان مستوى أمن معين.[66]

عملية تسيير المخاطر تكمن في تعريف التهديدات "الحقيقية" للنظام، و تتطلب فهم عالي لثغرات الممتلك و تحديد أثرها، الخسائر المحتملة، تقدير الأثر في حال الحوادث، إضافة إلى النتائج المباشرة لوضع معايير الحماية.[67]

ثانيا : عناصر الخطر

[64] **Didier Godart** , op.cit ,p 184

[65] **Nicolas Mayer , Jean philippe Humbert** , « la gestion des risques pour les systèmes d'information » , centre de recherche public Henri Tudor , Article paru dans le magasin MISC n24 , 2006 ,p3.

[66] ibid, p2

[67] **Didier Godart** , op.cit , p188.

لفهم الخطر يجب فهم مكوناته ، و لا يمكن أن يوجد الخطر إلا بتواجد مكوناته مجتمعة : و هي الممتلك ، التهديد ، الثغرة ، الأثر.

- الممتلك: هو المورد المتعرض للخطر ، و يتلخص في أقسام : بشرية ، تقنية ، معلومات ، شركاء ، و مادية[68]، وفي هذا السياق التركيز على ممتلكات النظام أكبر و المتمثلة في الممتلكات التقنية و الأجهزة، البرامج، التطبيقات، الخوادم، الشبكات...و أيضا الممتلكات البشرية (المستخدمين)، إضافة إلى المعلومات و محيط المؤسسة.
- التهديد : هو أصل و مصدر الخطر ، و يمكن أن يكون شخص أو حادث أصاب ممتلك من ممتلكات المؤسسة ، و تسبب في خسارة جزئية أو كلية للمورد بصفة مؤقتة أو دائمة.
- الثغرة : هي الضعف الأمني الموجود على مستوى ممتلك من ممتلكات النظام ، و تعتبر نوع من أنواع التهديد.
- الأثر : هو نتيجة استغلال الثغرة الموجودة على مستوى الممتلك من قبل التهديد ، و قد يكون هذا الأثر مقبولا أو غير مقبول.

الفرع الثاني : تشخيص البنية التحتية

أول مرحلة في عملية تسيير المخاطر تكمن في تعريف النطاق و الممتلكات و تحقيق فحص شامل لنظام المعلومات الموضوع. فهندسة نظام المعلومات متكونة من عناصر مادية و برمجية تمثل موارد على كل سياسة أمنية أخذها بعين الاعتبار ، حيث أن ضعف هذه الموارد يمكن أن يمنع نظام المعلومات من اتمام مهمته.[69] لذا يجب إحصاء مجموع الموارد التي تحتاجها المؤسسة من أجل أن تعمل ، و مقارنتها بكل الحوادث الممكنة التي حدوثها المفاجئ يحرمنا منها بصفة جزئية أو كلية ، مؤقتة أو نهائية.[70] خاصة فيما يتعلق بالمعلومات الاستراتيجية ، فبمجرد تعريفها يجب الأخذ بعين الاعتبار احتمالية وقوع دمار تام ، سواء كان سببه حادثي أو إجرامي ، لذا في نظام مثالي المعطيات الاستراتيجية تكون مرتبة حسب أهميتها، و مأرشفة بطريقة تجعلها دائما متاحة[71]، و عند تعريف البنية التحتية لا يكفي معرفة 99% من الأجهزة و البرامج الخاصة بالمؤسسة لأن 1% الذي بقي يمكن أن يكون أصل ثغرة أمنية كبيرة.[72]

[68] **Jean Paul Louisot**, «gestion des risques (100 question pour comprendre et agir) », éditions AFNOR, 2010,p 09
[69] **Eric Léopold** , op.cit , p107.
[70] **Jean paul Louisot** ,2010 , op.cit , p35.
[71] **Eric Léopold** , op.cit , p p107 108
[72] **Jean Marc Royer** ,2004, op.cit , p33.

تشخيص المخاطر يكمن في تطبيق متكرر للجرد النظامي لكل موارد المؤسسة : إذ أن أكبر خطر في تعريف المخاطر ليس نسيان ثغرة ، و إنما العيش مع فكرة أنه بما أننا عرفنا في الوقت الراهن "t" في الهيئة "c" مخاطر ، ليس لدينا مجهودات أكبر لبذلها[73] فالفحص يجب أن يكون متكرر كل فترة ، أو عند ادخال أي عنصر جديد .

و من الأصول التي يمكن أن تتعرض للتهديدات و تحتاج إلى جرد دوري ما يلي :[74]

- المواقع و تجهيزات الخدمات العامة.
- الأشخاص.
- الأجهزة : خوادم ، محطات العمل ، الحواسب الشخصية و النهايات المتحركة ، آلات الطباعة و النسخ ، وحدات التخزين ، خطوط التواصل ، المحركات ، جدران الحماية ، جسور الشبكة.....
- البرامج : أنظمة التشغيل ، البرامج التطبيقية و التشخيصية ، برامج جدران الحماية.....
- المعطيات : مخزنة لمعالجتها أو مأرشفة ، محفوظة ، قواعد المعطيات ، جرائد الأخطاء و تقارير الاشراف المرسلة على تحاميل التواصل.
- الأنظمة و الاجراءات ، التوثيق.
- تحاميل تركيب البرامج ، التحاميل المغناطيسية.

اعتمادا على هذه القائمة ، هذا الجرد سيقوم بجمع و حفظ أقل معلومات ممكنة لكل أصل : مالك المعلومة ، موقعه المادي أو المنطقي ، رقم تعريفه.

نتيجة لهذا الاحصاء تتكون نظرة عامة عن أنظمة المعلومات ، ثم يأتي دور المراجعة الداخلية التي تكمن في دراسة كل هذه العناصر من أجل تحديد المخاطر المقدمة في مجال الأمن ، و تعريف المعايير الضرورية للحماية.[75]

كل ما سبق يعتبر جرد للأصول ، أي العنصر الأول من عناصر الخطر (الممتلك) و بعد تعريفه ، و تحديد مدى حساسيته تأتي مراحل أخرى ضرورية:[76]

- تعريف التهديدات (النوع و المصدر) خطورتها ، فرص تكرارها.
- تقدير سهولة استغلال كل تهديد.
- تعريف معايير الأمن الموجودة من أجل تفادي وضع معايير غير مفيدة.
- تعريف الثغرات .

[73] **Jean paul Louisot** , op.cit , p36
[74] **Jean François Carpentier** , op.cit , p42.
[75] **Jean Marc Royer** ,2004, op.cit , p35.
[76] **Jean François Carpentier** , op.cit , p42

- تعريف النتائج و الآثار.
- تقدير أثر كل خطر.

المطلب الثاني : تحليل المخاطر

تحليل المخاطر يمثل قلب عملية تسيير المخاطر، و باعتبار أن المخاطر على أصول المؤسسة سواء (بتهديد أو ثغرة) غير محدودة وأثرها غير متوقع فان معرفة هذه المخاطر وتقييمها وترتيبها ضروري من أجل تحديد أولويات المعالجة.

الفرع الأول : تحليل عناصر الخطر

كما ذكرنا سابقا أنه من أجل فهم الخطر يجب فهم مكوناته ، فكذلك في هذه المرحلة ، من أجل تحليل الخطر يجب تحليل مكوناته و ضبطها :[77]

- التهديدات المحققة أو المتصورة ، الواقعة على الأصول المحصاة سواء تهديدات تعرضت لها بالماضي ، تهديدات أصابت المنافسين أو تهديدات نظرية محضة.
- الثغرات : تنظيمية أو ظرفية موجودة على مستوى المنظمة و تكون كذلك أبواب دخول كبيرة في عدة طوابق في المنظمة.
- أثر استغلال تهديد لثغرة سواء على صورتها ، أثر مالي ، أثر على الزبائن ، أثر على قدرة المنظمة في التوجيه الجيد لأهدافها.

اذا تحليل المخاطر هي عملية تحليل مختلف العوامل ، هذا التحليل يسمح بإقامة معيار قاعدي للخطر ، مرتبط بنظام معين ، هذا المعيار ضروري من أجل القدرة على فهم و تقييم أحسن لمعايير الحماية الموضوعة ، و أيضا التأثيرات المقبولة و غير المقبولة على النظام.[78]

الفرع الثاني : تحليل و تقييم الخطر

يكون عن طريق دراسة عنصري الخطر الأساسيين :

- التكرار (الفرصة ، الاحتمال ، احتمالية الحدوث) عن طريق توزيع الاحتمالات على التهديدات و الثغرات.
- الخطورة (الأثر المالي) : عن طريق تقدير التكاليف الناتجة عن الآثار.

[77] **Christian Harbulot** , 2012 , op.cit , p297.
[78] **Didier Godart** , op.cit , p190.

1- **التكرار** : و يسمى بفرصة التكرار أحيانا أو احتمالية الحدوث أو احتمالية الفرصة. و لا يمكن تحليل المخاطر دون تحليل احتمالية التهديد ، فانطلاقا من قائمة الأصول و التهديدات و المخاطر التي قد تتعرضها و المعرّفة في المرحلة السابقة ، يأتي دور تحديد احتمالية فرصة الخطر ، إذ يجب تحضير قائمة التهديدات مع تعريف فرصة تكرار كل تهديد ، و هذا يختلف حسب طبيعة كل منظمة و أنظمة معلوماتها.

فبالنسبة لكل تهديد ، يجب تقدير احتمالية نتائجه على الأصول و تقدير تكرار فرصة التهديد بالترابط مع سهولة استغلالها ، تعقيدها ، الثغرات الممكن استغلالها.[79]

و في هذا التقييم نجد مدرستين :[80] إما بالاعتماد على تحقيق فحص شامل للنظام و مختلف عناصره و إما انطلاقا من قواعد المعارف الموجودة و المعرّفة مسبقا.

فالمخاطر المتكررة و التي تحدث بانتظام و لكن بنتائج محدودة مثل : الاجازات المرضية في مؤسسة تشغل عدة آلاف من الأشخاص ....فان المقاربة التاريخية بتعريف قوانين الاحتمال للتكرار و الخطورة تسمح بتقييم الخطر.[81]

و في هذا التقييم ، فان تاريخ الحوادث المفهرس للنظام و تجارب الأفراد يمكن أن يحمل دلائل مهمة ، و الاعتماد كذلك على احصائيات الحوادث الأمنية الحادثة مسبقا.

أما بالنسبة للمخاطر الاستثنائية فالأمر يختلف ، و لا يمكن تحديد فرص التكرار إلا بالاعتماد الحقيقي على قياس درجة التنبؤ بحصول هذه الحوادث.

إذن التهديد و الثغرة هما سبب الخطر و تصنفان على مستوى الاحتمال، أما الأثر فيصنف على مستوى الخطورة.

2- **الخطورة** : و تسمى أيضا الأثر المالي للكوارث ، و قد يكون هذا الأثر مقبولا و أحيانا غير مقبول إذا قام بتخريب قوي لعنصر مهم من عناصر العملية العملياتية .

و من أجل تقييم أثر الحوادث المعرفة يجب تخيل " سيناريوهات كوارث " ، و هذا في حال المخاطر الكبيرة التي تتعرض لها المؤسسة مثل : حريق ، زلزال ، فيضان ، انفجار فيجب التفكير عن طريق السيناريو من أجل تحديد شروط البقاء تحت ما يسمى اليوم في المؤسسات المالية " قيمة الخطر " ، فتقييم الخطورة تهدف في أسوأ الحالات إلى تحديد أهمية نزيف الخزينة ، و التي يمكن أن تؤثر على المنظمة ، و هذا التحليل يجب إعادة النظر فيه سنويا ، و إعطاء الاعتبار للخسائر الثانوية و ليس فقط الفورية[82]

[79] **Jean François Carpentier** , op.cit , p43
[80] **Nicolas Mayer** , 2006 , op.cit , p4
[81] **Jean Paul Louisot** , op.cit , p38
[82] ibid , p38.

إذا تقدير مستوى الخطر عن طريق (الاحتمال ، الخطورة) يسمح بحساب الخطر ، و انتاج التقارير التي تحمل قائمة المخاطر و أولوياتها بعلاقة مع سيناريوهات الحوادث الممكنة ، و بمجرد تقدير "تكرار فرصة التهديد " و " تقدير النتائج " يتم الانتقال إلى مرحلة ترتيب حجم الخطر و استنتاج قيمته بتحضير مصفوفة التقييم.[83]

الفرع الثالث : ترتيب و تقدير المخاطر

بمجرد تعريف المخاطر و تحديد إذا كان حدوثها متكرر أو محتمل ، و إذا كان نتائجها كارثية أو غير مهمة ، تأتي مرحلة ترتيب هذه المخاطر ،حيث نجد طريقتين لتقدير المخاطر[84]:

أ- **الطرق النوعية** : التي تبدل دراسة الكميات بتقييم نوعياتها ، و تستعمل عندما لا يملك المدقق الوقت للتقييم الكمي للمخاطر ، أو عند نقص المعلومات مثل : خطر نظري لم ينتج أبدا.

ب- **الطرق الكمية** : المرتبطة بالتقييم عدديا للمخاطر لتقييم الخسارة المالية المتوقعة ، جعل مقارنة بين المخاطر و متابعة تطويرها خلال الوقت من أجل قياس المخاطر التي تتعرض لنظام المعلومات.

و بما أن المخاطر المعلوماتية غير ملموسة و معظمها لا يمكن التعرف عليه و تقدير نتائجه كميا ، فان التركيز سيكون على الطرق النوعية التي تعتمد على عاملي : الخطورة و الاحتمالية.

1- **حسب الخطورة** : هناك عدة تصنيفات ، إذ يمكن ترتيبه من ضعيف ، متوسط ، هام أو غير مهم ، هامشي ، خطِر ، كارثي . و هناك ترتيب آخر :[85]

- **الخطر الكارثي** : يتمثل في التدهور القوي لأمن النظام.
- **الخطر الحرج** : يتمثل في تدهور تكامل النظام.
- **الخطر الخطير** : يتمثل في إصابات بليغة أو توقف المهمة دون تخريب أو عدم إتاحة مهمة.
- **الخطر البليغ** : يتمثل في تدهور نجاعة المهمة.
- **الخطر الطفيف** : يتمثل في نتائج دون تأثير على المهمة أو أمن النظام.

[83] **Jean François Carpentier** , op.cit , p43

[84] **Christian Harbulot** , 2012 , op.cit , p297.

[85] **Alain Desroches ,et autres** , la gestion des risques « principes , et pratique » , 3 éme édition , Lavoisier , Paris , 2015 , p26.

2- **حسب الاحتمالية** : يوجد كذلك عدة تصنيفات : ضعيف ، متوسط ، هام أو غير ممكن / غير محتمل ، نادر ، عرضي ، محتمل ، متكرر أو مستحيل إلى غير محتمل ، جد قليل الاحتمال ، قليل الاحتمال ، محتمل ، جد محتمل إلى أكيد. و لكن قياس الخطر و ترتيبه لا يعتمد على عامل واحد دون الآخر ، و إنما كل خطر معرّف يقابله معامل الخطورة و الاحتمالية أو التكرار.

يمكن وضع نتائج التحليل في جدول ذو مدخلين يسمح بترتيب المخاطر :

الجدول (3.1) : ترتيب المخاطر

الاحتمالية

الخطورة	ضعيف	متوسط	هام
ضعيف			
متوسط			
هام			

Source : Eric Léopold ,op.cit p 109

و يمكن ترتيبها في جدول أكثر تفصيلا:

الجدول(3.2) :Tableau de criticité brute du risque

Occurrence التكرار	Gravité الخطورة				
	1 غير مهمة	**2 هامة**	**3 خطرة**	**4 كارثية**
6 متكرر	6 مهملة	12 غير مرغوبة	18 غير مقبولة	24 غير مقبولة
5 محتمل	5 مهملة	10 غير مرغوبة	15 غير مقبولة	20 غير مقبولة
4 عرضية	4 مهملة	8 غير مرغوبة	12 غير مرغوبة	16 غير مقبولة
3 نادر	3 مهملة	6 مهملة	9 غير مرغوبة	12 غير مرغوبة
2 غير محتملة	2 مهملة	4 مهملة	6 مهملة	8 غير مرغوبة
1 غير ممكنة	1 مهملة	2 مهملة	3 مهملة	4 مهملة

Source : Arnaud Pelletier et Patrick Cuenot ,op.cit, p51

من خلال الجدول و اعتمادا على عاملي التكرار و الخطورة نستنتج 3 أنواع من المخاطر :

1- **مخاطر مهملة** : و تتلخص في المخاطر غير المهمة بغض النظر عن تكرارها ، و المخاطر الهامشية بشرط أن يكون تكرارها نادر ، غير محتمل ، غير ممكن ، و المخاطر الخطرة و لكن تكرارها غير محتمل أو غير ممكن ، و المخاطر الكارثية و التي يكون تكرارها غير ممكن ، و بالتالي هي مخاطر نتائجها و أثرها مقبول.

2- **مخاطر غير مرغوبة** : و تتلخص في المخاطر الهامشية التي يكون تكرارها متكرر، محتمل، عرضي و المخاطر الخطرة التي يكون تكرارها عرضي أو نادر ، و المخاطر الكارثية التي يكون تكرارها نادر إلى غير محتمل ، و بالتالي هي مخاطر نتائجها مقبولة و لكن تحت الرقابة.

3- **مخاطر غير مقبولة** : و هي إما المخاطر الخطرة التي يكون تكرارها محتمل إلى متكرر أو المخاطر الكارثية التي يكون تكرارها عرضي ، محتمل إلى متكرر ، بمعنى عالية التكرار و بالغة الخطورة ، و هي مخاطر غير مقبولة في أي حال من الأحوال.

و يمكن تلخيص هذه المخاطر في جدول سلم الحرج:

الجدول (3.3) : سلم الحرج

رتبة الحرج	مستوى الخطر	القرارات أو النشاطات
C1	مقبول	عدم اتخاذ أي نشاط
C2	مقبول تحت الرقابة	يجب التنظيم و المتابعة في مجال تسيير المخاطر
C3	غير مقبول	يجب رفض الوضعية و اتخاذ معايير لتخفيض المخاطر و إلا يجب رفض كل أو جزء من العمل

Source : Alain Desroches , Alain Leory ,2015 , op.cit , p30

الفرع الرابع : طرق تحليل المخاطر

تحليل المخاطر يمكن أن يسهل عن طريق اللجوء إلى أدوات ، و المتمثلة في الطرق المقترحة لتحليل المخاطر المعلوماتية ، و التي تقدم ميزة وفرصة صريحة لتزويد المسيرين برؤية حول المخاطر المحاطة بمشاريعهم في مدة زمنية دنيا ، و لكن المشكل أن هناك أكثر من 200 طريقة لتسيير تحليل المخاطر ، و عليه كيف يكون الاختيار وسط هذا الكم الهائل من مراجع تحليل المخاطر؟

أول خطوة تكون بالتقديم و معرفة ما يناسب خصائص نظام المعلومات ، و لتقليص نطاق الاختيار داخل الطرق القانونية هناك ما هي أكثر شعبية ، و تمثل مرجع في مجالها ، و تعبّر بفعالية عن دورها في قيادة عملية تسيير المخاطر ، و من بين هذه الطرق :

- **طريقة MARION**

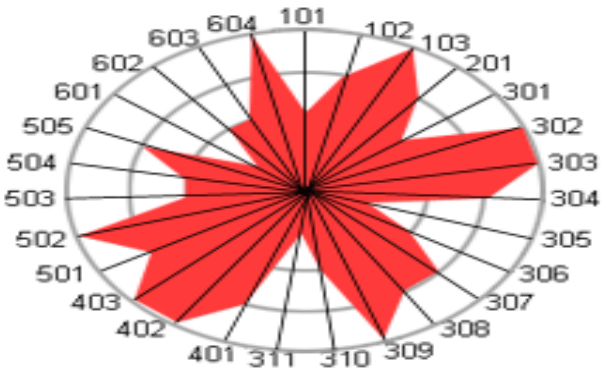
هي منهجية تجارية تطورت في 1984 بالتعاون بين نادي الأمن المعلوماتي الفرنسي (CLUSIF)و ممثل منظمات التأمين الفرنسية (APSAD)[86] و هي مُقدّرة لسهولة فهمها و تحديد كمية الثغرات ، متلائمة جدا مع البيانات المعلوماتية المركزية ، و أقل تلائما مع البيانات المفتوحة[87] و تعمل هذه الطريقة ضمن أربع مراحل :

1- **مرحلة البداية** : و تسعى لتحديد محيط الدراسة و أخذ معرفة حول التنظيم المهني للمؤسسة[88] ، إضافة إلى عملية التحسيس التي تعتبر ضرورية لأن الأمن لا يُضمن إلا إذا كان هناك تشارك داخل المؤسسة من الادارة العامة إلى المستعمل النهائي.[89]

2- **مرحلة دراسة الثغرات** : الطريقة ترتكز على تخفيض الثغرات الراجعة إلى تهديدات و مخاطر لها تأثير على إتاحة ، تكامل و سرية المعلومات ، و من أجل تحليل الثغرات ، من الممكن الآن الاعتماد على قواعد الثغرات من (CERT) (Computer Emergency Reponse Teams)[90].

و ترتكز الطريقة في هذه المرحلة على استبيان من عدة مئات من الأسئلة معتمدة على 27 عامل مُرقّم منها : الأمن التنظيمي ، الأمن المادي ، الاستمرارية ، التنظيم المعلوماتي ، الأمن المنطقي ، أمن التطبيقات.....كل عامل محدد بنقطة من 0 إلى 4 موزنة بعوامل مثبتة احصائيا من قبل نادي الأمن المعلوماتي الفرنسي ، هذه القيم ممثلة بيانيا تحت شكل نجمية مركبة لمجموع ثغرات المؤسسة.[91]

الشكل (3.5) :نموذج لنجمية MARION



Source : Hugo Etiévant , Normes de sécurité : les méthodes d'analyse des risques , article publié le 18 aout 2006, vu sur le site https://cyberzoide.developpez.com/securite/methodes-analyse-risques/ Le 13/06/2019 à 10h.55

[86] **Didier Godart** , op.cit , p191.
[87] **Patrick Boulet** , op.cit , p69
[88] Ibid ,p 66.
[89] **Alain Desroches** , op.cit , p197.
[90] Ibid ,p 197
[91] **Patrick Boulet** , op.cit , p p66- 67

3- **مرحلة تحليل المخاطر** : هذه المرحلة تكمن في تعريف مختلف سيناريوهات المخاطر ، حيث أن الطريقة تدل على عامل خطورة كل سيناريو ، أثره و احتمالية تحققه ، إذ أن الأثر ، الاحتمال و الخطورة مقيمة على سلم من 0 إلى 4 بتقنية خاصة بطريقة **MARION** بفعل قاعدة معارف و ثغرات مدروسة خلال المرحلة 2.[92]

4- **مرحلة مخطط العمل** : في هذه المرحلة يتم وضع خطة العمل انطلاقا من ترتيب السيناريوهات بناءا على درجة الخطورة و اختيار وسائل الأمن حسب نظام الأولوية من أجل إعادة المخاطر إلى مستوى مقبول.

- **طريقة MEHARI**

هي طريقة تسمح بتقييم المخاطر و ادارة أمن المؤسسة في محيط معقد و مفتوح ، تطورت في سنوات 1990 من طرف نادي الأمن المعلوماتي الفرنسي. و أصبحت هذه الطريقة اليوم واحدة من طرق تحليل المخاطر الأكثر استعمالا ، و هي مستمدة من طريقتين أخريتين لتحليل المخاطر (Marion et Melissa)، و تقدم هذه الطريقة كعلبة أدوات تسمح بادراك الخطر بمختلف الطرق على مستوى المنظمة.[93]

هذه الطريقة تقسم 3 مخططات مختلفة حادثة حسب تسلسل زمني :[94]

- **المخطط الاستراتيجي للأمن** : من خلاله يتم نشر أهداف الأمن و تعريف موارد المؤسسة و ترتيبها مع الأخذ بعين الاعتبار سياسة أمن المؤسسة .
- **المخطط العملياتي للأمن** : يتم من خلاله بفحص الموجود و تحديد مستوى الثغرات ، و تقييم خطورة سيناريوهات المخاطر ، و تحضير النشاطات الواجب مباشرتها من أجل القضاء على المخاطر غير المقبولة و تخفيض مستوى خطورتها تحت القيمة المحددة .
- **المخطط العملياتي للمؤسسة** : يتم من خلاله تركيب نشاطات الأمن المحققة في مختلف الهيئات العملياتية.

وتعرف طريقة **MEHARI** 6 معايير أمن مختلفة، الثلاثة الأولى مقامة على أثر الخطر، والثلاثة الأخيرة على احتماليتها:[95]

- معايير الحماية (مضاد فيروسات ، جدار ناري....)
- معايير التمويه (حفظ/تصليح ، مخطط النجدة....)
- معايير الاسترجاع (ضمان الممتلكات غير المادية...)
- معايير وقائية (التأكيد بحجز مزدوج ، التدقيق.....)

[92] **Patrick Boulet** , op.cit ,p 68
[93] **Nicolas Mayer** , 2006 , p09
[94] **Patrick Boulet** , op.cit , pp 69-71.
[95] Ibid ,p70.

- معايير مانعة (التحقق من الهوية..)
- معايير تنظيمية (تكوين المستخدمين).

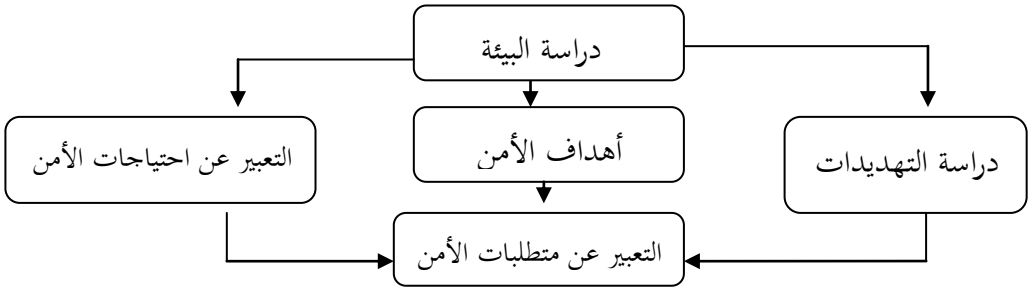
هذه الطريقة بفضل فكرتها " النازلة " من الادارة العامة إلى الهيئات العملياتية تكون ملائمة جدا للمنظمات متعددة البيئات.

- **طريقة EBIOS**

تم خلق هذه الطريقة سنة 1995 من طرف المديرية المركزية لأمن نظم المعلومات (DCSSI) و تسمح بالتعبير بوضوح عن احتياجات أمن النظام و استنتاج الأهداف و المتطلبات الضرورية ، و تستعمل أكثر في الأنظمة الجديدة في مرحلة التعيين ، و كطريقة **MEHARI** تعمل هذه الطريقة بمساعدة برنامج خاص يحوي قاعدة معارف و يسمح بفهم الفرضيات و تركيب النتائج بسرعة.[96] ترتكز طريقة **EBIOS** على 5 مراحل متباينة :[97]

- **المرحلة الأولى** : تتمثل في دراسة النطاق من خلال : دراسة المؤسسة و مواردها ، دراسة النظام المستهدف ، دراسة مكونات النظام.
- **المرحلة الثانية** : يتم فيها تحديد احتياجات الأمن لكل عنصر ضروري معرّف في المرحلة الأولى ، هذه الاحتياجات محددة على سلم من 0 إلى 4 بسؤال فئة ممثلة للمؤسسة.
- **المرحلة الثالثة** : هذه المرحلة موجهة لدراسة التهديدات التي ستكون محفوظة من قبل المؤسسة داخل قائمة مزوّدة من الطريقة ، لكل من هذه التهديدات مستوى حساسية على سلم من 0 إلى 4.
- **المرحلة الرابعة** : يتم هنا مقارنة احتياجات الأمن للعناصر الأساسية المعرفة في المرحلة الثانية مع التهديدات المحفوظة في المرحلة الثالثة ، أيضا من الممكن تحديد النتائج المرتبطة بظهور هذه التهديدات.
- **المرحلة الخامسة** : تسمح بتحويل أهداف الأمن إلى متطلبات وظيفية بمعنى إلى نشاطات للتحقيق

الشكل (3.6) : طريقة EBIOS العامة



Source : :Nicolas Mayer , 2006. P7.

[96] **Patrick Boulet** , op.cit ,p72.
[97] Ibid ,pp 72-73

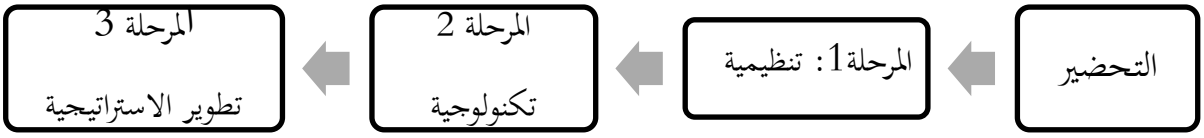
- **طريقة OCTAVE[98]**

هذه الطريقة تم نشرها من طرف SEI (Software Engineering Institue) ، أساسها يرتكز على احتمالية تحقيق تحليل مخاطر لداخل المنظمة ، حصريا مع الموارد الداخلية ، مع أنها موجهة نحو الحسابات الكبرى إلا أنها يمكنها بسهولة أن تميل على مستوى بنية اقتصادية صغيرة.

OCTAVE هي طريقة لتقييم الثغرات و التهديدات على الأصول العملياتية و تضم 3 مراحل :

- **المرحلة الأولى(التنظيمية)** :تسمح بتعريف الموارد المعلوماتية المهمة، التهديدات المشتركة و متطلبات الأمن المرتبطة بها.
- **المرحلة الثانية (التقنية)** : تسمح بتعريف ثغرات البنية التحتية.
- **المرحلة الثالثة** : تعمل على تطوير استراتيجية الأمن و تخطيطها.

الشكل (3.7) : المراحل الأساسية ل OCTAVE



Source : Nicolas Mayer ,op.cit, 2006. P7.

و هناك طرق أخرى إضافة إلى الطرق آنفة الذكر مثل :CRAMM . MESSEDI . MELISA. AMDEC...

المطلب الثالث : معالجة المخاطر و الفحص و التدقيق في برامج تسيير المخاطر

بعد القيام بعملية التحليل و تحديد قائمة المخاطر مع أولوياتها حسب معايير التقييم و سيناريوهات الحوادث يأتي دور المعالجة و التحكم في هذه المخاطر.

الفرع الأول : معالجة المخاطر (التحكم في المخاطر)

تتم العملية عن طريق التحكم في تكاليف الخطر نسبة للخسائر المتوقعة بمعنى جعل الخطر E المعرّف على أنه غير مقبول مقبولا و هذا بالاعتماد على مجموعة من المعايير.

و بالتشابه مع العمل الطبي ، فإن معالجة المخاطر تهدف إلى تحقيق هدفين إمّا الحد من الأعراض أو معالجة المرض من العمق[99] ، فمسير المخاطر يمتلك صندوقي أدوات من أجل التخفيض من الثغرات:[100]

[98] **Nicolas Mayer** , 2006. Pp 8-9.
[99] **Jean François Carpentier** ,op.cit, p165.
[100] Ibid ,p165

- **صندوق تخفيض المخاطر** : يمكن التدخل على الخطر نفسه عن طريق تخفيض الاحتمالات أو النتائج.
- **صندوق تمويل المخاطر** : يمكن وضع الوسائل المالية التي تعوّض الخسائر.

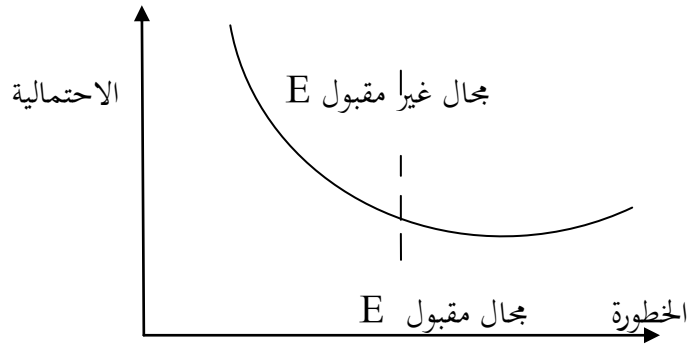
- **معايير التحكم في المخاطر** :

معايير التحكم في المخاطر هي:"العمليات، الاجراءات، الحلول التكنولوجية المستعملة لتخفيض المخاطر "[101] إذ أنه في مادة تسيير المخاطر لا يمكن إلغاء أو القضاء على الخطر و إنما فقط تخفيضه وتخفيض أثره إلى مستوى مقبول.

و يوجد مجموعة من المعايير للتحكم في المخاطر :

- **معايير التخفيض**:بالقضاء على الثغرات وجعل استغلالها صعبا،بالتصدي للتهديد و جعل الهجمة المحتملة أقل جاذبية،باستنزاف قيمة الأصول المتأثرة [102]،ويكون التخفيض إما بنشاطات على التكرار أو نشاطات حول الأثر: الوقاية بنشاطات على التكرار (الفرصة) : فالنشاطات الوقائية تعرّف و توضح قبل ظهور الخطر نفسه بهدف التصرّف على الفرصة و بالتالي تخفيض احتمالية فرصة الخطر ، فالتعامل مع المخاطر يستوجب معرفتها ، و عليه كل نشاط تكوين أو تحسيس يدخل في هذا النوع من الفئات[103]فالوقاية تكمن في تعديل النظام أو استخدامه من أجل تخفيض " **احتمالية** " حدوث الحدث المريب E و جعل الخطر مقبول[104].

الشكل (3.8) : الوقاية بنشاطات حول التكرار

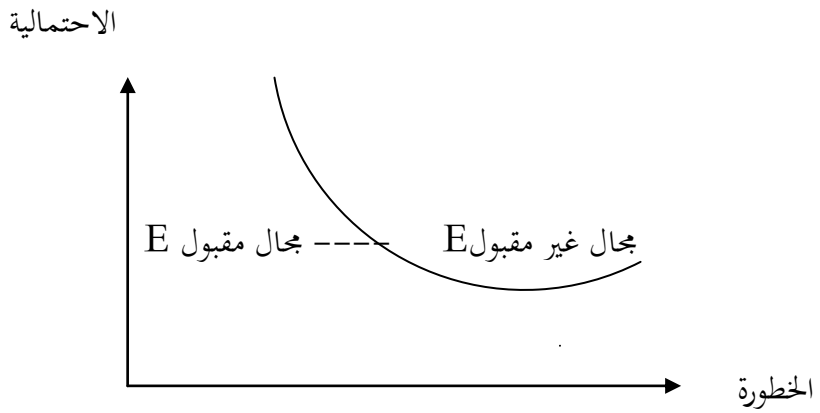


Source : Alain Desroches , op.cit , p37

[101] **Didier Godart** , 2005 , op.cit , p182
[102] **Christian Harbulot** , 20012 , op.cit , p298.
[103] **Michel-Henry Bouchet , Alice Guillon** le Fraper du Hellen, intelligence économique et gestion des risques , ed pearson education , France 2007 , p90
[104] **Alain Desroches** , op.cit , p37.

الحماية بنشاطات حول الأثر : نشاطات الحماية تحدّ من خطورة الخطر ، و تتصرف على الخطر بالحد من الخسائر ، و لكن تخرج من مبدأ أن حدوث الخطر يمكن تجنّبه ، فالعديد من المخاطر لا يمكن تجنّبها. هناك معايير فورية مخططة مسبقا تبين أن الخطر يمكن تخفيضه كما أن العديد من تجهيزات الكشف تسمح باتخاذ نشاطات فورية من أجل الوقاية بأقصى سرعة من الحدوث المفاجئ للكارثة و منع انتشارها السريع.[105] فالحماية تكمن في تعديل النظام أو استغلاله من أجل تخفيض **خطورة** الحدث المريب E و جعل الخطر مقبول .

الشكل (3.9). الوقاية بنشاطات حول الأثر



Source : Alain Desroches , op.cit , p37

– **معايير التجنب** : فبدلا من مداواة الجرح نقطع العضو ، مثلا : بيع الفروع المتضررة ، إلغاء أو استئصال نظم المعلومات التي تحمل ثغرات[106]، أخذ قرار بعدم تولّي نشاطات من أجل الخروج أو التفلّت من وضعية الخطر، إلغاء النشاط أو الوضعية المعنية بالخطر إذا كان مستوى الخطر غير مقبول،أو إذا كان تكلفة وضع حلول جدّ مرتفعة.[107]

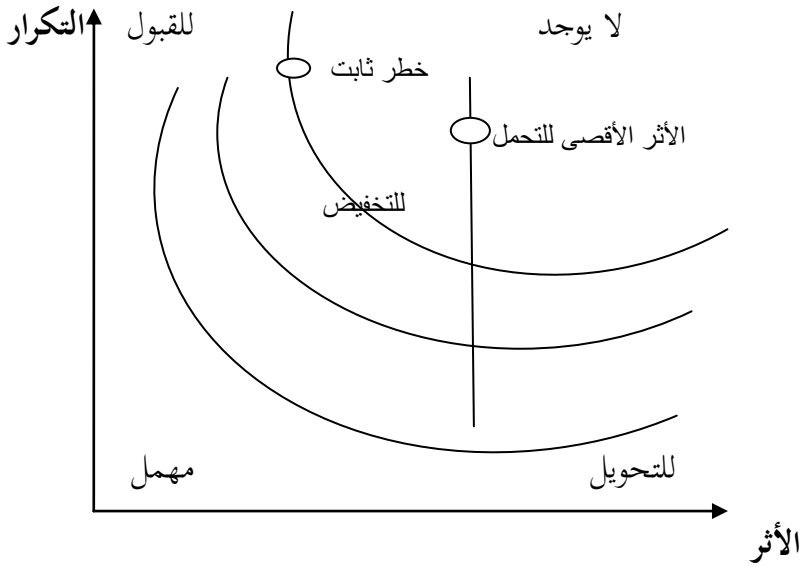
– **معايير التحويل** : تحويل الخطر هو تقاسمه مع طرف آخر كعقود التأمين مثلا التي تسمح في حال التعرّض للخطر الحصول على تعويض مالي أو شريك خارجي مثلا يقبل تحمّل تكاليف الخطر.

– **معايير القبول**:إذا كان هناك نشاط يجلب المخاطر،فنشاط التحكم لا يجب اتخاذه إلا بعد دراسة ملائمة، هذه الدراسة يجب أن تبيّن أن تكلفة اتّخاذ هذه النشاطات ليست أعلى من تكلفة النتائج المباشرة لحدوث الخطر.[108]

إذ أن قبول الخطر في العديد من الحالات هو الحل الأصوب ، و هذا في حال كان تأثيره غير مهم مقابل تكلفة معايير الحماية ، أو أن تكلفة المعالجة أكبر من تكلفة أثره إذا تم تحققه.

[105] **Michel-Henry Bouchet** , 2007 ,op.cit, p91.
[106] **Christian Harbulot** , 20012 , op.cit , p298.
[107] **Jean François Carpentier** ,op.cit, p45.
[108] **!m** , op.cit , p35.

الشكل (3.10): مختلف مناطق الخطر



Source : Nicolas Mayer , op.cit , p4

بعد اختيار الطريقة و المعيار المناسب لكل خطر معرّف يتم تقرير المعالجة المناسبة لكل خطر محلّل ، و بعدها يتم الانتقال إلى تحضير مخطط المعالجة ، إذ أن هذا الأخير يفرض احترام الخطوات التالية :

- **إحصاء أدوات تسيير المخاطر المتصوّرة** من أجل تخفيض الثغرات المكتشفة ، هنا يجب تجنّب المراقبة عن طريق العادات ،و إنما يجب حضور مختصين في تسيير المخاطر[109] أو خبراء نظم الأمن ، إذ أن تعريف متطلبات الأمن بفعل أهميتها و تعقيدها تُنفّذ بدقة متناهية، و من الأفضل البدء بمتطلّبات عامة التي تعرف الغاية لمواجهة المخاطر المعرّفة(على المستوى الاستراتيجي)من أجل تصفيتها لاحقا إلى متطلبات أكثر تحديد (نحو المستوى العملياتي)[110].

- **اختيار رقابات الأمن و معرفة الاختيارات التقنية للحلول الأمنية** ، و بمجرد اختيار الرقابات يبقى اذن تركيبها في نظام المعلومات و اختبارها و تقييمها.[111]

- **موافقة الادارة العامة**:الاعداد و الموافقة على برنامج معالجة المخاطر من قبل الادارة هي مرحلة التفاعل المباشر بين المختص و الادارة، أين يجب تقديم برنامج متناسق لمعالجة مجموع الثغرات الحيوية ، و تبرير ماليا اختياراتها في ظل احترام الأهداف الموضوعة، هذه الموافقة هي التي تعطي للبرنامج شرعيته في كل الوحدات العملياتية.[112]

[109] **Jean Paul Louisot** , 2010 , op.cit , p163.
[110] **Nicolas Mayer** , 2006. , op.cit p 06.
[111] Ibid ,p06
[112] **Jean Paul Louisot** , 2010 , op.cit , p p 163.164

- **تبريرات حالات قبول الخطر** : قرار قبول كل خطر من المخاطر يجب أن يكون مبرّر نسبة للمعايير المعرّفة من قبل المنظمة مع الأخذ بعين الاعتبار المخاطر الكامنة حتّى بعد القيام بالمعالجة.[113]

- **التفعيل** : بمعنى متابعة تنفيذ البرنامج الموافق عليه على المستوى العملياتي أي العمل الميداني ، و في هذا المجال على المختص في تسيير المخاطر اقناع المسؤولين العملياتيين بتفعيل القرارات المتخذة.[114]

الفرع الثاني : الفحص و التدقيق في برامج تسيير المخاطر

تسمى هذه المرحلة ب " فحص البرنامج " ، إذ على المختصين بعد تطبيق مخطط المعالجة مراقبة النتائج المحققة و التحقق من فعالية البرنامج عن طريق زيارات المراقبة من أجل التأكد أن المعايير المتخذة تم تفعيلها بشكل جيد و أن أثرها كان نفسه المتوقّع.[115]

و بعد تحقيق الفحص ، و تبين أن نظام المعلومات ليس آمن بعد ، يجب القيام بفحص آخر عن طريق اختبارات التدخل التي يقوم بها مختص الأمن أو المسؤول عن المخطط ، أو من خلال مكتب فحص خارجي متخصص في الأمن المعلوماتي ، أو بمساعدة برامج مخصصة لذلك تقوم باختبار عدد من نقاط الضعف و تنتج تقرير مفصل بالثغرات المكتشفة ، و الفحص الخارجي هو الأفضل لأنه محايد و يكون أكثر موضوعية.[116]

ففي مادة الأمن لا يكفي تطبيق الحلول و افتراض أنّها مفعّلة بشكل جيد و أن النظام آمن ، و إنما يجب التحقق بكل الطرق الممكنة ، و إجراء عدة اختبارات تدخل لكشف الثغرات ، لأن الموضوع دقيق و أي ثغرة يمكن أن تكون مصدر تهديد كبير.

أول مرحلة في مادة تسيير المخاطر هي التشخيص ، و بعد التشخيص و تقييم المخاطر و ترتيبها تأتي مرحلة المعالجة ، و بعد تطبيق كل الحلول لابد من التحقق من فعاليتها عن طريق مرحلة " الفحص " ، نتائج هذه المرحلة هي التي تبين لنا ثغرات جديدة تقودنا إلى إعادة الدورة.

---

[113] **Jean François Carpentier** ,op.cit, p46.
[114] **Jean Paul Louisot** , 2010 , op.cit , p p 163.164
[115] Ibid ,p164
[116] **Jean Marc Royer** ,2004, op.cit , p40.

الفرع الثالث : مخطط استمرارية النشاط و تسيير الأزمات

نظرا لأهمية نظم المعلومات ، أصبح محتما على كل مؤسسة التفكير في حمايته و توفير الإتاحة الكاملة و المستمرة له، و هنا ظهرت عدة أنواع من الخطط و المصطلحات منها : مخطط استمرارية النشاط ، مخطط استئناف النشاط ، مخطط النجدة ، مخطط الطوارئ ، تسيير الأزمات ...، كل هذه الخطط تصب في معنى واحد وهو كيفية الحفاظ على عمل نظام المعلومات و استمراريته خلال حدوث أي طارئ أو أزمة.

1- **تعريف الأزمة** : نستطيع القول أننا في حالة أزمة عند حدوث حدث استثنائي يعطل بصفة كبيرة العمل العادي و المعتاد للعمليات المهمة للزبائن الداخليين و الخارجيين ، هذا الحدث إن لم يحل ينتج عنه تأثيرات مباشرة أو غير مباشرة كبيرة.[117]

كما تتمثل وضعية الأزمة في الأثر السلبي المهم و المستمر على النتائج المالية للمؤسسة ، على العلامات و على صورتها ، إضافة إلى علاقاتها مع الشركاء الأساسيين.[118]

إذا الأزمة هي عبارة عن كشف الاختلالات ما يدفع المؤسسة إلى إعادة التفكير ، فالأزمة تضع الإدارة في وضعية حساسة تفرض عليها أخذ معايير فورية و جذرية ، و تقاس شدة الأزمة بمستوى ضياع نشاط المؤسسة.[119]

2- تعريف مخطط استئناف/استمرارية النشاط:

أصبحت هذه المخططات قضية أساسية لنظم المعلومات ، فمجرد الحفظ البسيط لم يعد كافيا خصوصا في حال الكوارث الكبرى ، و بما أن نظم المعلومات أصبح عنصر حساس و حرج للمؤسسة فعليه دائما أن يكون متاحا ، و كما يشير مسؤولي مخططات استئناف النشاط : " لكي تكون مستعدا لجميع الاحتمالات عليك أن تتخيل الأسوأ ".[120]

و هناك فرق بين مخطط استئناف النشاط و مخطط استمرارية النشاط، فهذا الأخير مرتبط بمفهوم الاتاحة العالية ، و هدفه ضمان اتاحة المعلومات مهما كان المشكل ، في حين أن مخطط الاستئناف لا يسمح باتاحة كلية على مستوى المعلومات ، و إنما يسمح فقط بضمان أن النشاطات يمكن استرجاعها خلال وقت محدد مسبقا ، فالفرق بينهما ضئيل ، و هما مرتبطان ببعضهما ، إذ يتدخل مخطط الاستئناف عندما يواجه مخطط الاستمرارية سيناريو خطير أو كارثة.[121]

---

[117] **Foray Bernard** , op.cit , p251.
[118] **Jean Paul Louisot** , op.cit , p127.
[119] **Nicolas Moinet** , op.cit , pp 100-101
[120] **Philippe Gillet** , « Virtualisation des systèmes d'information avec VM ware –Architectures , Projet ,Sécurité et retours d'expérience -» ,Editions ENI , France , 2009 , p199.
[121] Ibid , p 200.

3- عملية استمرارية /استئناف النشاط في ظل الأزمة

في مادة ضمان استمرارية النشاط في ظل الأزمة هناك مرحلتين أساسيتين: مرحلة التحضير (قبل الازمة) و مرحلة التنفيذ (خلال الأزمة).

1.3- **مرحلة (مخطط) التحضير** : استعدادا للأزمة هناك عدة ترتيبات من الضروري تحضيرها مسبقا، و هي:

- **التوثيق** : يجب أن يكون كامل و جاهز ، ففي يوم الكارثة فرق التدخل ليس لها وقت لتضييعه في التفكير و التفسير ، و إنما عليهم الاعتماد على إجراءات مكتوبة و مفصلة[122] ، لذا على مسؤول استمرارية النشاط تحضير وثيقة بيداغوجية تعمل على تقديم استراتيجية استمرارية الخدمة .

- **تحديد النطاق** : تحديد التطبيقات و التجهيزات و البرامج و الملفات المهمة حسب معايير التكييف للمؤسسة حيث سترتكز جهود استعادة النشاط عليها ، و تحديد نطاق مخطط الاستمرارية.

- **توفير موقع بديل** : من أجل حماية نظم المعلومات لابد من توفير موقع بديل يسمى قاعة النجدة ، يتم اللجوء إليه حالة حدوث الكارثة ، و المؤسسة أمام عدة خيارات منها : إقامة هذا الموقع داخل المؤسسة و هذا في حالة المنشآت الكبيرة ، اتفاقيات التعاون المتبادل بين مؤسستين حيث تحول المنظمة المضيفة نظامها إلى نمط التشغيل في حال الطوارئ لمساعدة المؤسسة الأخرى على معالجة بياناتها المهمة ، المواقع الباردة و هي عبارة عن بنايات خارج المؤسسة فارغة و تكون جاهزة لاستيعاب الأجهزة اللازمة لمعالجة البيانات بشكل مؤقت ، و المواقع الساخنة و تختلف عن الباردة بأنها مجهزة بكافة الأجهزة و الحواسيب اللازمة لاستعادة النشاط خلال فترة قصيرة من وقوع الأزمة[123]

- **تعيين خلية أزمة** : مواجهة الأزمة تتطلب كفاءات بشرية تُحدد مهامها مسبقا ،كل حسب تخصصه ، و أهم شخص في هذا الفريق هو مسؤول مخطط الاستمرارية أو مخطط النجدة و هو المسؤول عن عملية التخطيط لتسيير الأزمة و يكون إما تحت إشراف المدير العام أو مدير نظم المعلومات أو مسؤول أمن نظم المعلومات ، مدير مخطط الاستمرارية هو المسؤول الأول عن اتخاذ القرارات و تنفيذها و تسيير العمليات خلال وقوع الكارثة ، ولكن ليس بمفرده بل بمساعدة فريق عمل أو ما يسمى أحيانا بخلية تسيير الأزمة.

---

[122] **Patrick Boulet** , op.cit , p197

[123] **تركي راجي الحمود و آخرون** ، "التخطيط لمواجهة الطوارئ الخاصة بأنظمة المعلومات المحاسبية في المصارف التجارية الأردنية "، مجلة جامعة الملك عبد العزيز : الاقتصاد و الادارة ، العدد 2 ،الأردن ، 2017 ، ص ص 186-187.

- **اختيار مخطط عمل مناسب للمؤسسة** : إذ أنه لا يوجد أزمة مشابهة لأخرى بسبب اختلاف الأسباب و أنواع المؤسسات ، لذا من غير الممكن تحضير مخطط نموذجي ، و لا يمكن الاستفادة من بعض مبادئ مخطط آخر.[124]

- **القيام باختبارات منتظمة** من أجل التحقق من التنفيذ الجيد للمخطط و تصحيح الأعطال الممكنة ، كما أن اختبار و تكوين و تحقيق عمليات يسمح بتعريف الفجوات من أجل تحضير الأفراد المشاركين في تفعيل مخططات النجدة و تحسين فعالية المخططات.

- **تحليل العمليات** : غالبا في كل مخطط استمرارية من المهم جدا ذكر أو استخدام العناصر التالية :[125]

- **RTO (Recovery Time Objective)**: يمثل الوقت الأقصى المقبول لعدم الاتاحة ، بمعنى أقصى مدة تتحملها المؤسسة قبل استرجاع نشاطها ، و تكون بين عدة ثواني إلى عدة أيام.
- **RPO (Recovery Point Objective)** :يمثل نقطة إعادة البناء ، بمعنى أقصى ضياع مقبول للمعطيات و تختلف المدة بين 0 إلى عدة أيام ، و بالتشابه مع المعلم السابق فالمؤسسة لا تقبل أي ضياع معطيات لتطبيق استراتيجي في حين يمكنها تحمل ضياع يوم كامل لمعطيات قليلة و سهلة الاسترجاع.
- **أقصى تدهور أداء مقبول** : بمعنى وقت الإجابة المقبول من قبل المستخدمين في وضع متدهور .

2.3- مرحلة (مخطط) التنفيذ :

واحدة من الصعوبات التي تواجه تسيير الأزمة تتمثل أساسا في فهم الظاهرة و تعريف الوقت الذي يجب اطلاق عملية التسيير فيه و تبدأ بإجراءات محدودة في الوقت و الهدف ، و هنا يجب إعطاء ملاحظة لمن له فرصة النجاح، المخطط يجب أن يفعّل بسرعة منذ الاشارات الأولى للكارثة إن أمكن ، بمعنى قبل ظهور الاضطراب و هي وظيفة العملياتيين ، و في الحالات الأكثر خطورة يمكن البدء بمرحلة الانقاذ التي تهدف في حالة الطوارئ إلى حماية الأشخاص ، السمعة و الممتلكات. المهم هو التنظيم بطريقة مختلفة من أجل السماح بمواصلة الإنتاج بأقل وقت توقف ممكن.[126]

[124] **Nicolas Moinet** , op.cit , p101.
[125] **Patrick Boulet** , op.cit , p198 , et Philippe Gillet , op.cit , p204.
[126] **Jean Paul Louisot** , op.cit , p125.

و من الصعوبات التي يواجهها المسؤولون أيضا في حالة الأزمة هي التحكم في الأعصاب،فالتحكم الجيد في الأزمة هو قبل كل شيء نتيجة قرارات المدير الذي يجب أن يكون له القدرة على فرز المعلومات حسب درجة أهميتها ، و الإبتعاد تماما عن جانب المشاعر (الغضب ، الغيرة ، الغرور.....)لأنها الخطر الأول الذي يواجه المقرر.[127]

و عليه يتم التفكير و الاستنتاج إذا كان من الممكن ، أو من المفيد و المهم العودة إلى الوضعية الأولى ، و اختيار الاستراتيجية المناسبة إما بالعودة إلى الوضعية الأولى أو العمل على تطوير المؤسسة.[128]

المبحث الثالث : نظام إدارة أمن المعلومات و الايزو 27001

نظام ادارة أمن المعلومات هو نظام لا يمكن تطبيقه عشوائيا ، و إنما يحتاج إلى مراجع من أجل اقتباس أفضل التطبيقات و الممارسات ، و معرفة الطريق الصحيح في التطبيق الجيد ، و أفضل مرجع يمكن اعتماده في مجال أمن المعلومات هو معيار ايزو 27001 ، فالمؤسسة حتى لو لم تتحصل على الشهادة أو المصادقة من طرف المعيار إلا أنها يمكن أن تتبنى العديد من التطبيقات الموجودة فيه ، فما هو ايزو 27001 ؟ و ما أهميته ؟ و كيف يمكن الحصول على المصادقة ؟ و كيف يعمل نظام ادارة أمن المعلومات في ظل هذا المعيار؟

المطلب الأول : معيار الايزو 27001

المنظمة العالمية للقياس " ايزو " هي منظمة عالمية ظهرت سنة 1947 متكونة من ممثلي منظمات قياس وطنية في حوالي 150 بلد ، و إضافة إلى معايير "ايزو" المعروفة عالميا هناك معايير أخرى وطنية و عالمية و يكون ممثليها عموما أعضاء الايزو مثل :CEN[129] (اللجنة الأوروبية للقياس) ، BSI (المنظمة البريطانية للقياس) ، ANSI (المعهد الوطني الأمريكي للقياس) ، AFNOR (الجمعية الفرنسية للقياس) ، و لكن تبقى المعايير المرجعية لأمن نظم المعلومات هي بالتأكيد الخاصة بالايزو 27000 .

الفرع الأول : تاريخ معيار ايزو 27001:

- **1995** : في مارس 1995 تم اطلاق معيار $BS7799^{-1}$ من طرف BSI منظمة القياس البريطانية ، و هو عبارة عن وثيقة لأحسن التطبيقات التي تغطي الجوانب التنظيمية ، الاجتماعية ، القانونية ، و المعايير الممكن اتخاذها في مجال أمن المعلومة ، مواضيع لا يتم معالجتها في المعايير التي تهتم بالجوانب التقنية مثل ايزو 15408.[130]

---

[127] **Nicolas Moinet** , p102

[128] Ibid , p101.

[129] **Jérôme Del DUCA ,Alexandre Planche** ,op.cit , p 110.

[130] **Daniel Linlaud** , « sécurité de l'information « Elaboration et gestion de la politique de l'entreprise suivant l'iso 17799 » , AFNOR , France , 2003 , pp 7.8.

- **1998**: منظمة القياس البريطانية BSI أضافت جزء ثاني لهذا المعيار و سمته $BS7799^{-2}$ " $^{-2}$ " لا يعني هنا الطبعة 2 و لكن الجزء 2 ، هذه الاضافة تبين المتطلبات التي تحتاجها المنظمة لوضع نظام ادارة أمن المعلومات.[131]
- **2000** : في ديسمبر 2000 تم تبني المعيار $BS7799^{-1}$ رسميا من طرف الايزو و IEC تحت مرجع ISO/IEC17799 :2000[132] ، مع اثراءها ببعض المعايير الأمنية الاضافية حيث أن ISO17799 هو مرجع لا يعالج أكثر من مسألة نظام إدارة أمن المعلومات.[133]
- **2002** : بالتوازي مع أعمال الايزو ، BSI تابعت عملها على $BS7799^{-2}$ و نشرت طبعة قانية و هي $BS7799^{-2}$:2002[134].
- **2005** : في جوان 2005 أخرجت طبعة جديدة تحت مرجع ISO/IEC17799 :2005[135] ، و في أكتوبر 2005 الايزو يتبنى أخيرا $BS7799^{-2}$ تحت مرجع ISO27001 :2005 ، الايزو 27001 يحدد إذن المتطلبات التي يجب أن تجيب المنظمة من أجل وضع نظام إدارة أمن المعلومات.[136]
- **2007** : الايزو يعيد تسمية ISO17799 إلى ISO 27002[137].
- **2013** : امتداد لاتساع التشاورات بين أعضاء منظمة ISO/IE .الطبعة الاخيرة ل ISO27001 تمت في أكتوبر 2013.[138]

إذن من خلال تاريخ هذه المعايير نستنتج أنه يوجد اليوم معيارين :

- ISO27001 : التي تحدد متطلبات من أجل نظام ادارة أمن المعلومات.
- ISO 27002 : التي تستقبل التطبيقات الجيدة في مادة أمن المعلومات ، لكن لا تعالج نظام ادارة أمن المعلومات.

131 **Alexandre Fernandez- Toro** , sécurité opérationnelle , op.cit , p15.
132 **Daniel Linlaud** , op.cit , p7.
133 **Alexandre Fernandez- Toro** , op.cit, p15.
134 Ibid , p 15.
135 **Alain calder** ," ISO 27001/ISO27002 , A pocket guide , second edition , IT Gouvernance Publishing" , 2013 , p17.
136 **Alexandre Fernandez- Toro** , op.cit, p15.
137 Ibid , p15
138 **Alain calder** , op.cit, p25.

الفرع الثاني : التوافق بين ISO27001 و ISO 27002

الملحق Aل2013: ISO/IEC 27001 فيه 114 ضابط هي في 2013: ISO/IEC 27002 تتبع نفس نظام الترقيم و تستعمل نفس كلمات الضوابط و أهداف الرقابة .

ISO 27002 أيضا يزود ادارة التجهيزات الأساسية بكيف أن الفرد المسيطر يجب أن يكون قريبا. أي شخص ينفذ أو يحقق نظام ادارة أمن المعلومات **ISO27001** يحتاج أن يحصل و يدرس نسخة كلا من **ISO27001 و ISO 27002** ، في حين **ISO27001** في الواقع يأمر باستخدام **ISO 27002** كمصدر للتوجيهات بشأن الضوابط و اختيار السيطرة و تطبيقات التحكم ، فانه لا يحد من اختيار المنظمة للضوابط ، و تنص المواصفات على : " أهداف الرقابة و الضوابط الواردة في المرفق A ليست شاملة ، و أهداف الرقابة و الضوابط الاضافية يمكن الاحتياج إليها "

كلا المعيارين يعترفان أن أمن المعلومات لا يمكن أن يتحقق من خلال الوسائل التكنولوجية فقط ، كما أنه يجب أن لا يتم التنفيذ بالطريقة الخاطئة ، و التي قد تؤدي بالمؤسسة للخطر أو تخلق صعوبات لعملياتها التجارية.[139]

الفرع الثالث : أصناف الايزو

نستطيع تقسيم أصناف الايزو 27000 إلى 3 أنواع : [140]

- **معايير التصديق** : تصف المعايير التي يجب الالتزام بها من أجل الحصول على الشهادة مثل : ايزو 27001 (معيار تعريف وضع نظام ادارة أمن المعلومات) و ايزو 27006 (تعرف المتطلبات الواجب تطبيقها للمنظمات المعتمدة من أجل تطبيق الشهادة بأنفسهم)
- **معايير التوصية** : هذه المعايير تقترح الممارسات الجيدة الواجب اتباعها من أجل تعريف نظام الادارة و تحديد معايير الحماية مثل : ايزو 27002 ، ايزو 27003 ، ايزو 27004 و ايزو 27005.
- **المعايير القطاعية و التقنية** : الايزو يحضر أيضا "أنظمة ادارة أمن المعلومات قطاعية" مثل ايزو 27011 (الاتصالات) ، و ايزو 27799 (الصحة).

[139] **Alain calder** , op.cit , pp 17-18

[140] **Laurent Bellefin** , « L'ISO 27000 nouveau nirvana de la sécurité ? » , Solucum group, Livre Blanc, paris , p04.

1– ايزو 27001 : نظام إدارة أمن المعلومات

معيار ايزو 27001 هو عبارة عن مرجع في مجال أمن أنظمة المعلومات ، يعمل على تعريف و وضع نظام ادارة أمن المعلومات.

ايزو 27001 هو معيار مصادقة نظام ادارة أمن المعلومات ، هدفه السماح بتصور تخطيط و تفعيل نظام التحسين المستمر لتنظيم أمن المعلومات على مستوى المؤسسة[141] و هناك طبعتين :

- **ايزو 27001:2005** : ينتمي إلى عائلة المعايير المتعلقة بأنظمة إدارة الأمن المعلوماتي و التي هي موجهة إلى كل المنظمات و المؤسسات باختلاف حجمها و قطاع عملها ، و هو معيار مرن في الإجابة على احتياجات المؤسسات الصغيرة و المتوسطة و الكبيرة ، كما أنه قابل للتطبيق على كل القطاعات الاقتصادية ، المنظمات العمومية ، المعاهد الجامعية[142].

- **ايزو 27001:2013** : العنوان الرسمي لهذا المعيار هو : تكنولوجيا المعلومات – التقنيات الأمنية – نظام ادارة أمن المعلومات–المتطلبات،منذ أكتوبر 2013 جاء محل الطبعة القديمة ISO/IEC 27001 :2005.

هذا المعيار عبارة عن 30 صفحة طويلة فقط ، و يرد جوهر هذا المعيار في الصفحات التسع التي تحدد مواصفات تصميم و تنفيذ إدارة أمن المعلومات ، و أيضا في الصفحات B من الملحق A و التي تحوي 114 عناصر فردية تحت المعيار ، و التي يجب أخذها بعين الاعتبار عند التطبيق.[143]

2– معيار ايزو 27002 : هناك طبعتين :

– ايزو 27002:2005 : معيار ايزو 27002 هو عبارة عن وثائق للتطبيقات الجيدة لإدارة أمن المعلومات ، هو معيار توصيات محتواه مطابق تماما لايزو 17799 و يغطي 11 فئة.

– ايزو 27002:2013 : العنوان الرسمي لهذا المعيار هو تكنولوجيا المعلومات – التقنيات الأمنية – مدونة قواعد الممارسة لإدارة أمن المعلومات ، نشر في اكتوبر 2013 ، حل محل الطبعة القديمة ISO/CEI 27002 :2005 ، هو مدونة قواعد الممارسة و ليس مواصفة ، يستعمل كلمات مثل "يجب" ، "قد" ، يمكن اعتباره نقطة انطلاق لتطوير مبادئ توجيهية محددة و منظمة ، و هو أطول مرتين من ايزو 27001 ، حوالي 90 صفحة ، 8 منها مواد تمهيدية ، 78 صفحة تتعامل بالتفصيل مع الضوابط الأمنية.[144]

---

[141] **Jérôme Del DUCA ,Alexandre Planche**, op.cit, p.112
[142] **Edward Humphreys** , revue ISO/CEI 27001 pour les PME , 2009 , p6 , p33.
[143] **Alain calder** , op.cit, p25
[144] Ibid, p27

3- معيار ايزو 27003:2010 : يقدم نهج عملي من أجل النجاح في عملية وضع نظام ادارة أمن المعلومات مطابقة لايزو 27001 ، يصف عملية ادارة أمن نظم المعلومات و مواصفات التصميم منذ البداية إلى غاية انتاج مخططات تنفيذ المشروع ، مغطيا التحضير و التخطيط للأنشطة التي تسبق التنفيذ الفعلي .[145]

4- معيار ايزو 27004:2009 : هذا المعيار العالمي يقدم نصائح حول تطوير و استعمال المعايير من أجل تقييم فعالية نظام ادارة أمن المعلومات الموضوع كما هو مقرر في معيار ايزو 27001 .[146]

5- معيار ايزو 27005:2011 : عملية تسيير المخاطر المتعلقة بأمن المعلومة ، تقترح منهجية تقييم رو معالجة المخاطر[147] .

6- معيار ايزو 27006:2011 : دليل يشرح المتطلبات للمؤسسات المتبعة للفحص و تصديق أنظمة ادارة أمن المعلومات الذين أنجحوا مصادقة ايزو 27001.[148]

7- معيار ايزو 27007:2011 : دليل لفحص أنظمة ادارة أمن المعلومات.[149]

8- معيار ايزو 27008:2011: هذا المعيار يقترح دليل حول ضوابط أمن مراجعة المعلومة .[150]

هذه هي معايير الايزو الخاصة بأمن المعلومات عموما ، و هناك معايير أمنية خاصة بقطاعات معينة مثل:[151]

- **ايزو 27010 : 2012**: هذا المعيار متعدد الأجزاء ، يقترح دليل حول ادارة أمن المعلومة لقطاع الاتصالات.

- **ايزو 27011: 2008** : دليل لتسيير أمن المعلومات في قطاع الاتصال عن بعد (معروفة أيضا ك ITUX.1051).

- **ايزو 27013:2012** : دليل لإدماج التنفيذ بين ايزو 20000.1 و ايزو 27001 (نظام ادارة أمن المعلومات) لقطاع الصناعة.

- **ايزو 27014** : هذا المعيار سيغطي حوكمة أمن المعلومة (غير منشور).

- **ايزو 27015** : هذا المعيار سيكون دليل نظام ادارة أمن المعلومات للخدمات المالية في المنظمات (مقترح).

---

[145] **Abbes Rharrab** , « Audit sécurité des systémes d'information » , licence professionnelle , université mohammed V Agdal , Maroc , 2010 , p20.

[146] ISO 27001 management de la sécurité de l'information , rapport technique , librairie technique , scientifique et industriel , NORMADOC , PARIS , 2016.

[147] .**Michel Berteau , Eric Doyen** et autres , Livre Blanc : « Benchmark des outils SMSI , club 27001 » , 1ere édition , novembre 2013 , p10

[148] **Jean François Carpentier** ,2012 op.cit, p33.

[149] **Michel Berteau , Eric Doyen** et autres , Livre Blanc , op.cit , p10

[150] **Jean François Carpentier** ,2012 op.cit, p33.

[151] Ibid , p 34

- **ايزو 27031:2011** : هذا المعيار سيرتكز على استمرارية النشاط في أنظمة المعلومات.
- **ايزو 27032:2012** : هذا المعيار يقترح دليل حول أمن الانترنت.

المطلب الثاني : نظام ادارة أمن المعلومات

نظام ادارة أمن المعلومات متعلق أساسا بمعيار ايزو 27001 ، و من خلال هذا المطلب سيتم تعريف نظام ادارة أمن المعلومات علاقتها بايزو 27001 ، و كيفية تطبيق نظام ادراة أمن المعلومات في ظل ايزو 27001 ، إضافة إلى مراحل الحصول على هذه الأخيرة و أهميتها على المؤسسة .

الفرع الأول : تعريف نظام إدارة أمن المعلومات

أنظمة إدارة أمن المعلومات هي قبل كل شيء أنظمة إدارة ، بمعنى أنها تطبق على الأمن المعلوماتي الوصفات المجرّبة من قبل على ميادين أخرى خاصة الجودة ، في هذا المعنى هو يمثل تماما نفس خصائص أنظمة الادارة الأخرى.

في معيار ايزو 9001 و في الركن المعنون ب " نظام الادارة " يعرّف نظام الادارة على أنه نظام يسمح ب:

- وضع سياسة.
- وضع أهداف .
- تحقيق هذه الاهداف.

و عليه فان **نظام الادارة** هو مجموعة معايير تنظيمية و تقنية تهدف لتحقيق هدف ، و بمجرد تحقيقه تسعى لتجاوزه.[152]

نظام الادارة أيضا يرتكز على مرجع مكتوب ، و الذي يخضع للفحص بوسيلة تدقيق التي تعمل على مقارنة المرجع مع الواقع من أجل استخراج الاختلافات المسماة بالفجوات أو عدم التطابق ، و بدون مرجع المدقق سيكون له عدة صعوبات في اتمام مهمته.[153]

أما بالنسبة **لأمن المعلومات** فنحن لا نتكلم فقط عن الأمن المعلوماتي ، بل يهمنا الكلام عن المعلومة في كل أشكالها بعيدا عن كل تحاميلها : برامج، أجهزة، و حتى العنصر البشري، أوراق، مهارات .....مهما كان التحميل الذي يميز المعلومة ، المعلوماتية تأخذ حيز مهم و لكن حصر نظام ادارة أمن المعلومات في الجهة المعلوماتية فهذا خطأ.[154]

[152] **Alexander –Fernandez Toro** , op.cit , p6.
[153] **Laurent Bloch** , 2011 ,op.cit , p22.
[154] **Alexander –Fernandez Toro** ,op.cit , p13.

و عليه يعرف ايزو 27000 أمن المعلومات على أنه : " الحفاظ على سرية ، تكامل ، و توافر المعلومات ، بالإضافة إلى خصائص أخرى مثل الأصالة ، المساءلة ، عدم التنصل و الموثوقية.[155]

من خلال تعريف نظام الادارة و أمن المعلومات نتوصل إلى تعريف نظام ادارة أمن المعلومات بصفة عامة ،

و هناك عدة تعريفات في هذا المجال نذكرها كالتالي :

لعل أشهر تعريف لنظام ادارة أمن المعلومات هو تعريف منظمة القياس العالمية "ايزو" و التي تعرفه على أنه " جزء من نظام الادارة الشاملة معتمدة على نهج مخاطر الأعمال لتأسيس و تنفيذ و تشغيل و مراقبة و صيانة و تحسين أمن المعلومات ."[156]

– و يعرف على أنه مجموع العناصر المتفاعلة التي تسمح للمنظمة بتحضير سياسة و أهداف في مجال أمن المعلومة بتطبيق السياسة ، بتحقيق هذه الأهداف و مراقبة تحقيق هذه الأهداف.[157]

– نظام ادارة أمن المعلومات هو معيار واضح يشمل الهيكل التنظيمي ، السياسات ، أنشطة التخطيط ، المسؤوليات ، الممارسات ، الاجراءات ، العمليات و الموارد.[158]

– و هو نهج اداري منظم خاص بأمن المعلومات ، يهدف إلى ضمان التفاعل الفعال للمكونات الرئيسية الثلاثة لتنفيذ سياسة أمن المعلومات : العمليات ، التكنولوجيا ، سلوك المستخدم.[159]

– و يعرف نظام ادارة أمن المعلومات على أنه مجموع الموارد المستعملة من أجل التنظيم و التسيير اليومي لأمن المعلومة ، أكثر دقة هو يضم مجموع الوثائق التي تعرف قواعد و عمليات الأمن ، المنظومة المشاركة (مسؤول أمن المعلومات ، المراسلين الامنيين ، المستخدمين ، هيئات القرار....) إضافة إلى البنيات التحتية ، التقنية للأمن و بالتالي هو جهاز أو آلية عامة لحوكمة أمن المعلومة.[160]

---

[155] **Alain calder** , op.cit, p23

[156] **Sigurjon Thor Arnason , Keith D.Willett** , "how to achieve 27001 certification " An example of applied compliance management "" ,Averbach publications , 2008 , p 98.

[157] **Alphonse Etienne ETOGA** , « Définir un modèle générique de l'ISMS » ,Travail de diplôme , Haute école de gestion de Genève , Genève , 2006, p13.

[158] **Alain calder** , op.cit, p24

[159] ibid , p24.

[160] **Laurent Bellefin** , l'iso 27000 , nouveau nirvana de la sécurité ? op.cit., p5.

الفرع الثاني : علاقة الايزو 27001 بنظام ادارة أمن المعلومات

المعيار الذي يعالج نظام ادارة أمن المعلومات هو ايزو 27001 ، هذا الأخير يرتكز على مفاهيم السرية ، السلامة و التوافر ، و الهدف الأساسي لنظام ادارة أمن المعلومات هو العمل على حماية هذه الخصائص الثلاثة بالنسبة للمعلومات الحساسة للمؤسسة ، إضافة إلى عناصر أخرى مثل : التحقق من الهوية ، متابعة الطلب و امكانية التعقب ، المرجعية ، عدم التخلي و العديد من الميكانيزمات الأخرى. [161]

المعيار ايزو 27001 يحدد الطريقة الواجب اتباعها من أجل اعداد و وضع نظام ادارة أمن المعلومات و هو كالتالي :

- تعريف نطاق نظام ادارة أمن المعلومات : إذ أن ايزو 27001 ليست ذات حجم واحد يناسب جميع الحلول، كما أنه لم يكن على الاطلاق كيان ثابت باعتباره يتداخل مع نمو وتطور الأعمال التجارية ، و المعيار يعترف صراحة بأنه سيتم تحجيم نظام ادارة أمن المعلومات وفقا لاحتياجات المنظمة .[162]
- تكوين سياسة الادارة.
- تحديد طرق تحليل المخاطر المستعملة : ايزو 27001 يفرض تحليل مخاطر و لكن لا يقترح أي طريقة من أجل تحقيقها ، صاحب نظام ادارة أمن المعلومات حر في اختيار الطريقة المناسبة بشرط أن تكون موثقة ، ايزو يقترح مع ذلك طريقته في التحليل و هي ايزو 27005 ، و هناك طريقة أخرى لتحليل المخاطر مستعملة في اطار ايزو 27001 و هي طريقة EBIOS التي تسمح بتقييم و معالجة المخاطر المتعلقة بأمن أنظمة المعلومات.[163]
- تعريف ، تحليل و تقييم المخاطر ، و تحديد المعالجات المطبقة على مختلف المخاطر ، فمعيار ايزو 27001 يفرض قيادة تحليل المخاطر ثم تعريف مخطط معالجة هذه المخاطر التي يكون تطبيقها مراقب بصفة مستمرة. تحليل المخاطر يمثل نقطة انطلاق ايزو 27001 ، فهو تطبيق معقد و حساس يتطلب ارتكاز قوي على الادارة و أيضا منهجية و مخطط تواصل محضر جيدا.
- اثبات التزام ادارة المنظمة في طريقة نظام ادارة أمن المعلومات.

[161] **Alexander –Fernandez Toro** ,op.cit , p14.
[162] **Alain calder** , op.cit, p24
[163] **Laurent Bloch** , 2011 , op.cit , p23

الفرع الثالث : شروط (طريقة) تبني شهادة الايزو 27001

من أجل الحصول على المصادقة ، من الضروري القيام بتدقيق في نظام ادارة أمن المعلومات من طرف منظمة مصادقة خارجية ، فشهادة نظام ادارة أمن المعلومات ايزو 27001 تتبع نفس العملية في أنظمة الادارة الأخرى مثل ايزو 9001 و ايزو 14001[164] ، إذ يكون العمل بين ثلاثة أعوان [165]:

- المؤسسة التي تسعى للشهادة.
- مكتب التحضير للمصادقة.
- المكتب المصادق.

المنظمة التي تسعى للحصول على الشهادة يجب أولا أن تتعاقد مع منظمة تصديق ، هذا العقد لمدة سنوات سيؤطر مجموع دورة المصادقة ، منظمة التصديق ستفوض مدققين مصادقين أو مفوضين لتحقيق الرقابات ، هناك العديد من التدقيقات ، التدقيق الابتدائي يغطي مجموع النطاق ، تدقيقات مراقبة على مستوى محيط أكثر تقييد ، و تدقيق التجديد. مدة الفحص و التدقيق محددة من قبل ايزو 27006 و تختلف تبعا لعدد و حجم المواقع ، عدد الأشخاص في النطاق.[166] لكن عملية التدقيق لا تقتصر فقط على المدققين المفوضين بل تكون بمشاركة 3 أطراف ، تدقيق الطرف الأول هو مراجعة الممارسات الخاصة التي تقوم بها المؤسسة و التي تتم من قبل تلك المؤسسة ، تتم مراجعة الطرف الثاني من قبل منظمة شريكة عادة عملها العلاقات التجارية لبعض المواصفات ، و يتم تدقيق الطرف الثالث من قبل طرف ثالث مستقل مثل هيئة اصدار الشهادات أو مدقق الحسابات الخارجي.[167]

المنظمة تحصل على الشهادة بعد ضمان قدرتها على العمل في الداخل و الحفاظ على نظام ادارة أمن المعلومات ، و البند 4-8 من ايزو 27001 الزامية من أجل الحصول على الشهادة ، و يتطلب الايزو تنفيذ و تشغيل نظام ادارة أمن المعلومات ليكون على نفس نهج ادارات أنظمة الايزو الأخرى و هي نموذج PDCA.

المصادقة ليست شهادة مكتسبة إلى الأبد ، بل يتم فحص نظام ادارة امن المعلومات و تحديثه و تحسينه بانتظام وفقا لمبدأ PDCA.

[164] **Laurent Bellefin** , l'iso 27000 , nouveau nirvana de la sécurité ? op.cit., p15.
[165] **Jérôme Del Duca** , 2012 , op.cit , p 113.
[166] **Laurent Bellefin** , l'iso 27000 , nouveau nirvana de la sécurité ? op.cit., p15.
[167] **Alain calder** , op.cit, p19

تبني "ايزو 27001" لا يعطي فعاليته التامة إلا إذا تم تفعيل مبادئه الأساسية المقترحة بفعالية ، فمشروع تبني " ايزو 27001" يجب أن يأخذ مكانته في قلب ادارة أمن نظم المعلومات ، أو يكون متبنى من قبل مسؤول أمن نظم المعلومات بمساعدة جماعات الجودة و تسيير المخاطر ، و لكن يجب أن يدعم من قبل الادارة.[168]

الفرع الرابع : أهمية تبني ايزو 27001

من وراء ارتفاع التبادلات الرقمية ، أنظمة المعلومات هي اليوم موصولة داخليا مع كل المخاطر الممكنة ، و مصادقة ايزو 27001 هي ضمان ثقة بين الشركاء و يمكن أن يصبح في عدة حالات ضرورة[169] ، فأكثر من 5000 مؤسسة صادقت على أنظمة ادارة أمن المعلومات بالامتثال لايزو 27001 ، و العديد منها في طريقها لفعل ذلك نظرا لفعاليتها الواسعة للمساعدة في حماية تجهيزات و معلومات المؤسسة ، فالتفعيل التدريجي لنظام ادارة أمن المعلومات يسمح للمؤسسات بتحقيق و دون جهد كبير مستوى حماية قاعدي ، اقتصادي أكثر ، فبإتباع خطوتين أو ثلاث خطوات اضافية ، المنظمة يمكنها الحصول على نظام ادارة أمن المعلومات مطابق تماما لايزو 27001 و مناسب جدا للمؤسسة ، فكل مؤسسة بحاجة إلى ضمان على الأقل الحد الأدنى من الأمن ، فهذا المعيار أصبح اللغة المشتركة على مستوى المؤسسات و بين المؤسسات مختلفة النشاط.[170]كما أن استخدامه يدعم ثقة الادارة في المنهجية المتبعة من قبل مسؤول أمن نظم المعلومات و مصداقيته ، إذ تهدي له دعم جد فعال من أجل الحصول على الوسائل التي يحتاجها من أجل اتمام نشاطاته.

المطلب الثالث : تطبيق الايزو 27001 حسب نموذج PDCA

المنظمة عليها استعمال نموذج PDCA المحدد في ايزو 271011 لتنفيذ نظام ادارة أمن المعلومات.

الفرع الأول : تعريف دورة PDCA

نموذج PDCA هو عبارة عن دورة نشاطات تم تصميمه من أجل الحث على التحسينات المستمرة ، أول تطوير و حديث كان من طرف" Walter Shewarts " الاحصائي الأمريكي مخترع دورة دمينغ في كتابه " Statistical Method for the viewpoint of quality control" ، هذا النموذج أصبح أكثر شعبية من خلال " Edward Deming" الاحصائي و الفيلسوف الأمريكي ، مخترع مبادئ الجودة عندما شجع المراحل الأربع لنموذج

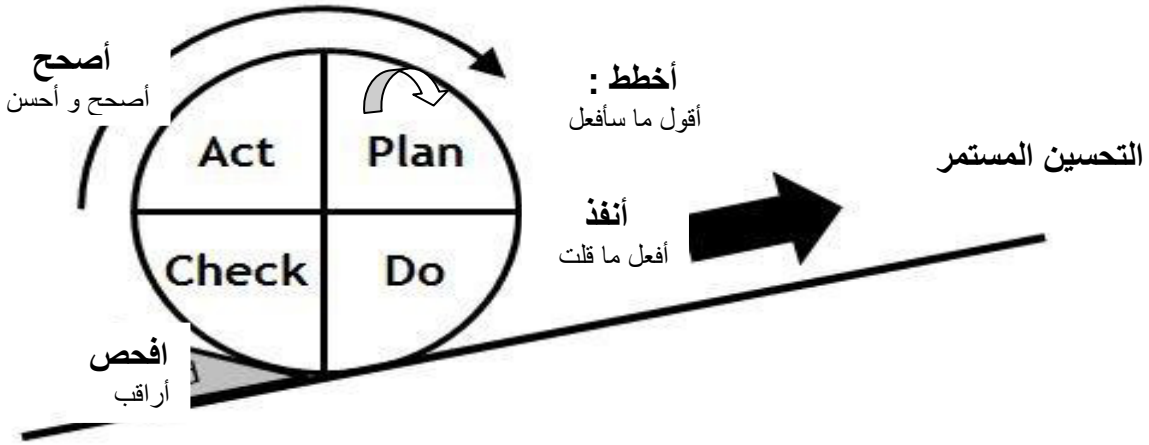
[168] **Laurent Bellefin** , l'iso 27000 , nouveau nirvana de la sécurité ? op.cit., p9.
[169] **Patrick Boulet** , 2007 , op.cit , p64.
[170] **Edward Humphreys** , ISO/IEC 27001 , op.cit , p6

PDCA للتحسين المستمر ، و عليه فان دورة PDCA الناتجة عن ايزو 9000 تسمى أيضا دورة التحسين ، أو دورة دمينغ نسبة لادوارد دمينغ [171].

نموذج أو دورة PDCA هو نموذج يطبق على كل المعايير المتعلقة بأنظمة الادارة ، مبدأها التحكم في العملية و تحسينها باستعمال دورة مستمرة من أربع مراحل تهدف لتخفيض الحاجة إلى التصحيح ، و ايزو 27001 الموجه للاهتمام بنظام ادارة أمن المعلومات كغيره من المعايير المتعلقة بأنظمة الادارة ، يرتكز على مقاربة عملية و أكثر دقة على نموذج PDCA.

سمي بهذا الاسم اختصارا لمبادئه الأربعة:خطط (plan)، نفذ (do) ،افحص (check) ،صحح (act)..

الشكل (3.11) : دورة ديمنغ (التحسين المستمر)



Source : André CHARDONNET – Dominique THIBAUDON , le guide du PDCA de Deming « progrès continu et management », Editions d'Organisation , 2003 , p62

يتسم هذا النموذج بطابعه الدوري ، فدورة PDCA تسمح بالوصول إلى الأهداف المسطرة من قبل الادارة ، و لكن ماذا يحصل في حال تحقيق الأهداف ؟ هنا يجب اتخاذ دورة أخرى لهذا يمكننا رؤية سهم بين مرحلة Actو مرحلة Plan فنظام الادارة هو عملية تدور بدون توقف.[172]

[171] **Sigurjon Thor Arnason , Keith D.Willett** , "how to achieve 27001 certification " An example of applied compliance management " ",Averbach publications , 2008 , p 98.et Jean- François carpentier , la sécurité informatique , op.cit.

[172] **Alexandre Fernandez toro** , op.cit , 2016 , p12.

هذا النموذج يطبق على نظام الادارة في مجموعه كما يطبق على كل مرحلة من مراحله ، فمثلا مرحلة خطط لوحدها يمكن تنفيذها عن طريق نموذج PDCA آخر.

الفرع الثاني : مراحل دورة PDCA

المراحل الأربعة لدورة PDCA هي مراحل مستمرة ، فبمجرد الوصول إلى المرحلة الأخيرة يتم اتخاذ دورة أخرى جديدة و تكون المراحل كالتالي :

1- **مرحلة خطط** : تتمثل هذه المرحلة في وضع أساسيات نظام ادارة أمن المعلومات ، فيتم تعريف الهدف الأساسي ، و القيام بجرد لكل الوسائل الضرورية لتحقيقه ، و تحديد تكلفة تحقيقه ، و وضع الخطة للوصول إليه. و تضم هذه المرحلة عدة خطوات أساسية :[173]

- تعريف نطاق و سياسة نظام ادارة أمن المعلومات.
- تعريف و تقييم المخاطر.
- تحديد أهداف الرقابة و ضوابط علاج المخاطر.
- صياغة مخطط معالجة المخاطر.
- تحضير بيان قابلية التطبيق Statement of Applicability[174]

2- **مرحلة نفذ** : هذه المرحلة هي المرحلة العملياتية للطريقة ، و تضم :

- **مخطط المعالجة** : هذه المرحلة ترتكز أساسا على مخطط معالجة المخاطر ، بمعنى مخطط الأعمال المفصل الناتج عن تحليل المخاطر الذي يعرف المسؤول عن كل نشاط ، الميزانية ، المخططات ، الوقت اللازم ، الأولويات.....[175]

- **اختيار المؤشرات** : هذه المرحلة تكمن في وضع مؤشرات الأداء للتحقق من فعالية معايير الأمن إضافة إلى مؤشرات الامتثال لمراقبة امتثال نظام ادراة أمن المعلومات . ايجاد أحسن المؤشرات ليس بالأمر الهين ، المعيار لا يدعو إلى مؤشرات معينة و لكن ايزو 27004 يقترح اجراءات مساعدة.[176]

- **تحسيس و تكوين المستخدمين.**

---

[173] **Sigurjon Thor Arnason , Keith D.Willett** , op.cit , p99.

[174] : بيان قابلية التطبيق (SoA): هو ملف على شكل جدول يسمح بتحديد معايير الأمن الموضوعة أو المرفوضة حسب الأهداف المرجوة و هو ضروري من أجل المصادقة.

[175] **Laurent Bellefin** , l'iso 27000 , nouveau nirvana de la sécurité ? op.cit., p6.

[176] **Thierry Boileau** , « mise en œuvre de la SSI de SUSS Micro Optics par l'approche processus iso/IEC 27001 » , mémoire présentée en vue d'obtenir le diplôme d'ingénieurs , CNAM, Conservatoire National des Arts et métiers , centre régionale associe de Lyon ,Hal « archives ouvertes », 2010 , p42

- **اجراءات تسيير نظام ادارة أمن المعلومات** : كتحرير الوثائق الضرورية ، تسيير موارد النظام ، تسيير المخاطر ، صيانة نظام ادارة امن المعلومات عن طريق ضمان العمل الجيد لكل مراحله ، تنفيذ المهام ....

3- **مرحلة افحص** : تكمن هذه المرحلة في مراجعة عمل نظام ادارة أمن المعلومات بتحديد العناصر غير المتماثلة و نقاط الضعف فيه و القيام بالتحسينات الملائمة [177] ، و أيضا التحقق من أن العمليات المتخذة موافقة للاحتياجات المرجوة حسب الوقت و التكلفة المحدد في المرحلة الأولى.[178] و تكون عملية الفحص من خلال الاجراءات التالية :[179]

- **التدقيق الداخلي** : يمكن أن ينظم من طرف عمال المنظمة أو يكون تحت اشراف شركة استشارات ، و الهدف منه مراقبة امتثال و فعالية نظام ادارة أمن المعلومات بالبحث عن الثغرات بين توثيق النظام و نشاطات المنظمة ، المعيار يفرض أن تكون الطريقة المستخدمة في التدقيق موثقة في اجراءات ، و التقارير محفوظة من أجل أن تكون مستخدمة من قبل مراجعات الادارة.

- **المراقبات الداخلية** : هدفها ضمان يوميا أن المساهمين يطبقون بطريقة صحيحة الاجراءات ، على عكس التدقيقات الداخلية التي تكون مخططة بمدة مسبقة.

- **مراجعات الادارة** : المراجعة هي اجتماع سنوي يسمح لمسيري المنظمة بتحليل الأحداث التي جرت في تلك السنة ، النقاط المدروسة غالبا هي : نتائج التدقيق ، عودة أصحاب المصلحة ، حالة النشاطات الوقائية و التصحيحية ، التهديدات المفهومة بطريقة سيئة من خلال تقدير المخاطر.

مرحلة افحص هي عبارة عن مراجعة ادارية لنظام ادارة امن المعلومات تسمح بإعادة تموقع النظام حسب أهداف و قضايا و التزامات المؤسسة ، و في حالة الضرورة يتم طلب تحديث تحليل المخاطر و مخطط معالجة المخاطر.[180]

4- **مرحلة صحح** : في هذه المرحلة يتم الأخذ بعين الاعتبار الفجوات و المشاكل المكتشفة خلال مرحلة افحص ، و اقتراح النشاطات الضرورية لتصحيحها و استباق المشاكل المستقبلية ، هذه المرحلة تسمح أيضا بإنهاء دورة ديمنغ تحضيرا للدورة المقبلة .

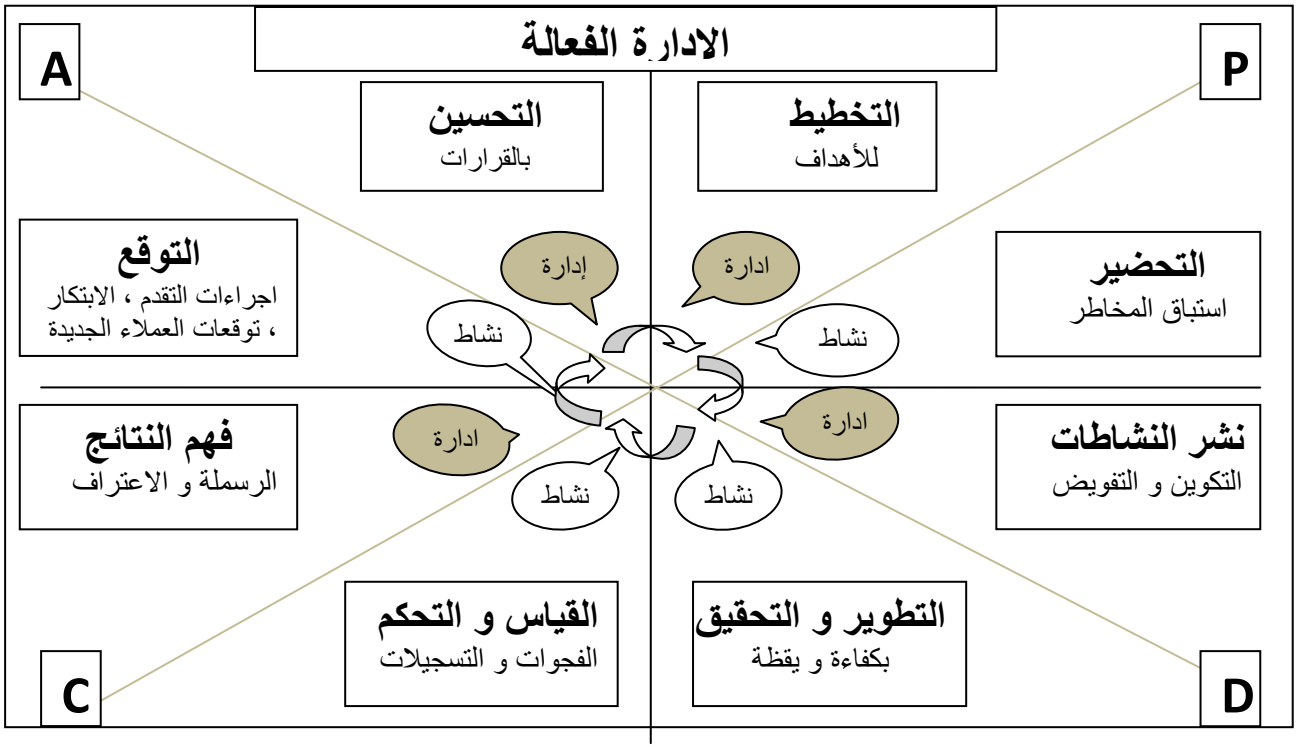
المعيار يؤكد على ضرورة تحضير مخطط النشاطات التصحيحية موجه لتصحيح الضعف أو الاختلال الوظيفي الظاهر في نظام ادارة أمن المعلومات و الذي يعود إما لعيوب في نظام إدارة أمن المعلومات نفسه أو لعدم فعالية

[177] **Laurent Bellefin ,** op.cit , p7
[178] **Jean François Carpentier** , op.cit , p9.
[179] **Thierry Boileau**, op.cit , p44
[180] **Laurent Bellefin** , op.cit , p7

معايير الأمن ، و في إطار نموذج التحسين المستمر PDCA يجب أيضا اقتراح مخطط النشاطات الوقائية ، الهدف منه منع الاختلالات المستقبلية (وضع رقابات إضافية مستقبلية).[181]

هذا عبارة عن نموذج ديمنغ المعروف ذو الأربعة مراحل ، و هناك نموذج آخر أكثر تفصيلا يسمى نموذج الادارة الفعالة يتكون من 8 مراحل حيث يبين لنا أن نشاطات كل مرحلة من المراحل الأربعة تنتمي إلى جانب من الجانبين : هما جانب التنظيم و الادارة أو جانب آخر هو الجانب التنفيذي.

الشكل (3.12) : الادارة حسب نموذج PDCA بثمانية مراحل



Source : **André CHARDONNET – Dominique THIBAUDON** , **le guide du PDCA de Deming « progrès continu et management »**, **Editions d'Organisation** , **2003** , **p66**

نموذج "الادارة الفعالة " المقترح يتم الحصول عليه عن طريق سلسلة متناوبة من الأنشطة الادارية و الانشطة التنفيذية ، و من هنا يمكن استخراج العديد من الممارسات الجيدة :[182]

- اتخاذ الاجراءات التصحيحية قبل تقديم الابتكارات.
- تخطيط و تنظيم التطوير قبل إعداد نشر الاجراء نفسه.
- نشر التدريب والاتصال و المرافقة قبل إطلاق المشروع نفسه.

[181] Ibid , p7
[182] **André chardonnet** , op.cit , p66.

خلاصة الفصل

أمن المعلومات هو مفهوم جديد على مستوى عالم المؤسسات لأنه مفهوم شامل و عام هدفه حماية المعلومة بكل أشكالها ، سواء في شكلها المعلوماتي أو الورقي أو الشفهي...، و لكن عملية تطبيقه ليست بالأمر البسيط ، بل تحتاج إلى تخطيط و تجنيد للموارد المادية و البشرية ، و دراسة لمحيط المؤسسة و تحديد النطاق الذي تسعى لحمايته، و دراسة كل التهديدات المحيطة و الممكنة و التخطيط لطرق التعامل معها و معالجتها ، و لتجنب التطبيق العشوائي لأمن المعلومات ظهرت اليوم معايير خاصة بذلك و أشهرها معيار ايزو 27001 الخاص بنظام ادراة أمن المعلومات الذي يبين الاطار العام لتطبيق الأمن داخل المؤسسة ، و عليه فان أي مؤسسة تسعى لتحسين مستوى أمن المعلومات لديها عليها أولا دراسة المحيط و البيئة الداخلية و الخارجية لها و من ثم انشاء سياسة أمنية ملائمة لطبيعتها تنص على كل القواعد الأساسية التي تضمن حماية أنظمة معلوماتها و كل الارث المعلوماتي لديها ، و من الضروري تفعيل هذه القواعد و مراقبة عملية التطبيق و معاقبة كل شخص قام بأي مخالفة ، و هذا لا يتم إلا بدورات التكوين و التحسيس للعمال و المسؤولين ، كما على المؤسسة انتهاج عملية تسيير مخاطر مناسبة تدرس فيها كل احتمالات التهديد التي قد تتعرض لها و تحضير السيناريوهات الممكنة لمواجهتها و هذا لتجنب أكبر قدر من المخاطر و الخروج بأقل الخسائر ، فالواقع اليوم يفرض على المؤسسة التفكير الاستراتيجي ، و دراسة الاحتمالات الممكنة ، و الحلول المناسبة لكل احتمال ، إذ أن الاستراتيجية المتبعة في تحقيق أمن المعلومات ليست موحدة و صالحة لكل المؤسسات ، فربما استراتيجية ناجحة لمؤسسة ما قد تؤدي للهاوية بمؤسسة أخرى ، لذا على كل مؤسسة احترام خصوصيتها و طبيعتها عند رسم استراتيجيتها ، و تحضير مخططات الاستئناف و استمرارية النشاط عند حدوث أي كارثة ، و الاستعداد لمواجهة أي سيناريو قد يواجهها مسبقا.

الفصل الرابع : واقع أمن المعلومات على مستوى المؤسسات الجزائرية

المبحث الأول : واقع أمن المعلومات في الجزائر

المطلب الأول : تعريف عينة الدراسة

المطلب الثاني : واقع أمن المعلومات على مستوى العينة المدروسة.

المبحث الثاني : منهجية الدراسة

المطلب الأول : مجتمع و عينة الدراسة

المطلب الثاني : أساليب جمع البيانات

المطلب الثالث : أساليب تحليل البيانات

المبحث الثالث : تحليل نتائج الدراسة

المطلب الأول : وصف عينة الدراسة و طبيعة وظيفة أمن المعلومات فيها

المطلب الثاني : قياس ثبات و صدق أداة الدراسة

المطلب الثالث : تحليل نتائج الدراسة

المطلب الرابع : اختبار الفرضيات

تمهيد

بدأ الاهتمام بمصطلح أمن المعلومات منذ تطور التقنية و بداية الاعتماد عليها في عملية التخزين لأهم المعلومات ، و زاد الاهتمام منذ ظهور الانترنت الذي أصبح وسيلة نقل لهذه المعلومات بين مختلف الجهات ، الأمر الذي أقلق المؤسسات التي باتت تسعى جاهدة لحماية أنظمتها المعلوماتية ، و لكن تختلف درجة توفير الحماية من نظام لآخر و من مؤسسة لأخرى و من دولة لأخرى و ذلك حسب أهمية المعلومات التي تريد حمايتها و مدى الضرر الذي يسببه افشاءها ، و لمعرفة مدى تطبيق المؤسسات الجزائرية لأمن المعلومات و مدى وعيها بخطورة التهديدات التي قد تتعرض لها قمنا بدراسة شملت عينة من المؤسسات الصناعية و الخدماتية الجزائرية تمثلت في 35 مؤسسة ، و سنقوم من خلال هذا الفصل بتعريف العينة المدروسة و توضيح مدى وعيها و تطبيقها لموضوع الدراسة مع التطرق إلى نموذج من هذه العينة بطريقة مبسطة و هو المؤسسة الوطنية للأشغال البترولية الكبرى نظرا للمسنا بعض مؤشرات الأمن فيها ، إضافة إلى تعريف طرق جمع المعلومات و منهجية البحث و تحليل النتائج المتوصل إليها من خلال الدراسة الميدانية بالاعتماد على مجموعة من الأساليب الاحصائية ، و دراسة أثر متغيرات الدراسة المتمثلة في التهديدات و الحماية على أمن المعلومات.

المبحث الأول : واقع أمن المعلومات في الجزائر

الجزائر بمختلف مؤسساتها من بين الدول التي لا تزال بعيدة نوعا ما عن هذا التطور الأمني الجديد و الذي نجد أثره الجيد فقط في المؤسسات العسكرية ، أما على مستوى المؤسسات الاقتصادية و السلطات المحلية فلا يمكن أن نتحدث عن تعاليم الأمن المعلوماتي ، و هذا بشهادة مجموعة من الدراسات و التحقيقات (تحقيق AASSI ، دراسة Kaspersky lab ، دراسة ألجيريا ديجيتال تراندس) تم التعرض إليها في أول البحث ، و التي أسفرت عن نتائج مقلقة في مجال الاهتمام بأمن المعلومات ، أما من الناحية القانونية فنجد أن المشرع الجزائري بدأ يولي أهمية للقوانين المتعلقة بحماية أنظمة المعلومات و ذلك من خلال بعض القوانين و التعديلات منها تعديل قانون العقوبات بالقانون رقم 04-15 و الذي أفرد فيه قسم 7 مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " و الذي تضمن 8 مواد (من المادة 394 مكرر إلى المادة 394 مكرر7) ، كما أصدر المشرع الجزائري قانونا مستقلا و هو القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، إضافة إلى الاتفاقيات الدولية التي أبرمتها الجزائر لمكافحة الجريمة المعلوماتية ، و لكن رغم هذه المجهودات إلا أن المشرع الجزائري لم يخصص بعد قانونا خاصا بالجريمة الالكترونية ، و الجزائر ككل لم تصل إلى المستوى المطلوب لمكافحة الجريمة الالكترونية و السيطرة عليها ، كما أن اهتمام المؤسسات الجزائرية بتطبيق أمن المعلومات محدود جدا و لا نلمسه سوى على مستوى المؤسسات الخدمية التي تعتمد في عملها على الوسائل التكنولوجية.

المطلب الأول : تعريف العينة المدروسة

الفرع الأول : تعريف عينة المؤسسات الصناعية و الخدمية

تمت هذه الدراسة على مجموعة من المؤسسات الجزائرية ، و المتمثلة في المؤسسات الكبيرة و المتوسطة و الصغيرة، و تم استثناء المؤسسات المصغرة ، هذا حسب عدد العمال ، أما حسب المعيار الاقتصادي فقد شملت الدراسة المؤسسات الصناعية ، و المؤسسات ذات القطاع الثالث من بنوك و مؤسسات مالية و خدماتية.

أما بالنسبة لعملية توزيع الاستبيان ففي بداية الدراسة حاولنا تخصيص الدراسة فقط على المؤسسات التي فيها مصلحة أو مسؤول عن أمن المعلومات أو حتى على الأقل مصلحة نظم معلومات ، و لكن اصطدمنا بشبه انعدام هذه الوظيفة على مستوى المؤسسات الجزائرية ، و حتى التي يوجد فيها ترفض القيام بأي مقابلة أو ملئ الاستبيان بحجة السرية و الحفاظ على أمن المعلومات ، فقمنا بتوسيع الدراسة لتشمل حتى المؤسسات التي لا يوجد فيها مصلحة خاصة بذلك و لكن تطبق الأمن ضمنيا ، و يتم اكتشاف ذلك من خلال المقابلة مع المسؤول عن الاعلام الآلي الذي غالبا ما توكل هذه المهمة إليه ، و نظرا لخصوصية الموضوع و قلة المدركين له و لتفاصيله

و ضرورة التخصص من أجل الإجابة على الاستبيان بطريقة موضوعية ، تم توزيع هذا الأخير على مستوى مصلحة الاعلام الآلي فقط أو مصلحة نظم المعلومات إن وجدت. و هذه مؤسسات العينة :

الجدول (4.1): المؤسسات الجزائرية محل الدراسة

المؤسسات الصناعية	المؤسسات الخدماتية
تلمسان	
1. المؤسسة الوطنية للسيارات الصناعية SNVI 2. الشركة الوطنية لاستغلال المواد البترولية SONATRAC 3. شركة النفط الجزائرية NAFTAL 4. الشركة الوطنية للكهرباء و الغاز SONELGAZ 5. الشركة العمومية لدراسات و انجازات الري SOGERHWIT 6. مؤسسة انتاج الحليب و مشتقاته " المنصورة" Giplait 7. المؤسسة الوطنية للاتصالات ENTC 8. LTPE 9. تعاونية الحبوب و البقول الجافة CCLS 10. شركة تسوية و تهيئة و تعبيد الطرق STARR 11. الشركة الصناعية الجزائرية للاتصالات SITEL 12. الشركة الجزائرية لصناعة الهواتف INATEL 13. مجمع خربوش للتصنيع الفلاحي و عتاد الموارد المائية. 14. SEROR	15. اتصالات الجزائر للهاتف المحمول Mobilis 16. الجزائرية للاتصالات Algérie télécom 17. الجزائرية للتأمينات 2a 18. الشركة الجزائرية للتأمينات saa 19. الوكالة الجزائرية للتأمينات الشاملة caat 20. الشركة الجزائرية للتأمين و إعادة التأمين caar 21. بنك الجزائر الخارجي BEA 22. البنك الوطني الجزائري BNA 23. بنك الفلاحة و التنمية الريفية BADR 24. الصندوق الوطني للتوفير و الاحتياط CNEP 25. ديوان الترقية و التسيير العقاري OPGI
سيدي بلعباس	

26. المؤسسة الوطنية للصناعات الالكترونية ENIE 27. مؤسسة انتاج الحليب و مشتقاته "عريب" Giplait 28. مجمع شالي للخدمات Groupe Chiali	29. الجزائرية للاتصالات Algérie télécom
الجزائر العاصمة	
30. المؤسسة الوطنية للأشغال البترولية الكبرى GTP 31. المؤسسة الوطنية للسيارات الصناعية SNVI 32. شركة النفط الجزائرية NAFTAL 33. شركة أنابيب الجزائرية ANABIB 34. المؤسسة الوطنية للفنون المطبعية	
وهران	
35. المؤسسة الوطنية للأشغال البترولية الكبرى	

الفرع الثاني : تعريف المؤسسة النموذج (المؤسسة الوطنية للأشغال البترولية الكبرى)

تم اختيار حالة من الحالات العديدة التي وقعت عليها الدراسة من أجل تقريب معنى و مفهوم الأمن و كيفية تطبيقه داخل المؤسسة ، أما بالنسبة لاختيار المؤسسة هذه بالذات فهذا يعود لعدة أسباب : أولها أنها تقريبا المؤسسة الصناعية الوحيدة التي اهتمت بتطبيقات أمن المعلومات ، و هذا مثال جيد يحتذى به ، لأن أغلب المؤسسات الصناعية تحتج بعدم اهتمامها بالموضوع لعدم وجود معلومات استراتيجية يمكن أن تسرق منها أو عدم وجود منافسة تدعو لمثل هذه الافعال و هذا يرجع لعدم ادراكهم لمعنى الأمن و أنه مفهوم شامل يتضمن حماية كل ما يوجد بالمؤسسة و أنه يرفع من قيمة المؤسسة و يصل بها إلى مصاف العالمية ، السبب الثاني و هو معرفتنا بوجود وظيفة مخصصة لمسؤول أمن نظم المعلومات و هذا ما لم نجده حتى في المؤسسات الخدمية التي تعتبر أنظمتها حساسة مثل البنوك و شركات الاتصال ، و علمنا أثناء المقابلة مع مسؤول أمن المعلومات أن المؤسسة تحصلت على شهادة ايزو 27001 الخاصة بأمن المعلومات ، و ثالثا و أهم سبب هو التعاون الكبير الذي تلقيناه من قبل

المؤسسة و المسؤول المذكور على وجه الخصوص و تقديرهم لأهمية البحث العلمي و حاجتنا للمعلومات التي نصل بها إلى النتائج المرجوة ، هذا ما غاب عند أغلب المؤسسات الأخرى .

المطلب الثاني : واقع أمن المعلومات على مستوى العينة المدروسة

الدراسة تمت على مستوى المؤسسات الصناعية و الخدمية ، و واقع الأمن يختلف اختلافا كبيرا في القطاعين :

الفرع الأول : أمن المعلومات على مستوى مؤسسات القطاع الثالث

لقد كان جزء من العينة المدروسة متمثل في مؤسسات القطاع الثالث من بنوك ، شركات تأمين ، شركات اتصالات، ففي هذا النوع من المؤسسات تجد ثقافة أمنية عالية نسبة إلى المؤسسات الصناعية و وعي بضرورة توفير أمن المعلومات ، نظرا لحساسية المعلومات التي تمتلكها هذه المؤسسات ، فسرية هذه المعلومات و ضرورة الحفاظ عليها هي التي تفرض توفير الأمن ،كما أن نجاح و استمرار هذه المؤسسات مرتبط بسرية و توافر المعلومات.

الفرع الثاني: أمن المعلومات على مستوى المؤسسات الصناعية

من خلال الدراسة على عينة من المؤسسات الجزائرية استنتجنا أن واقع أمن نظم المعلومات في هذه المؤسسات متدني حتى في أكبر المؤسسات ، فالمؤسسة الصناعية الجزائرية لازالت بعيدة عن هذا المفهوم الجديد ، و تجد الأمن يتجسد فقط في أمن الموقع المتمثل في الكاميرات و مراقبة الدخول أو من خلال برامج لحماية الحاسب ، و المتمثلة غالبا في برامج مكافحة الفيروس ، و تسند مهمة أمن نظم المعلومات غالبا إلى المسؤول عن الاعلام الآلي ، أما بالنسبة لوجود وظيفة أو مسؤول عن امن المعلومات لم نلمسها إلا في مؤسستين صناعيتين و هما المؤسسة الوطنية للأشغال البترولية الكبرى ، و مؤسسة نفطال ، أما بالنسبة لباقي المؤسسات فلا نجد حتى مصلحة خاصة بأنظمة المعلومات.

الفرع الثالث : نموذج المؤسسة الوطنية للأشغال البترولية الكبرى

1- مكانة أمن المعلومات على المستوى التنظيمي

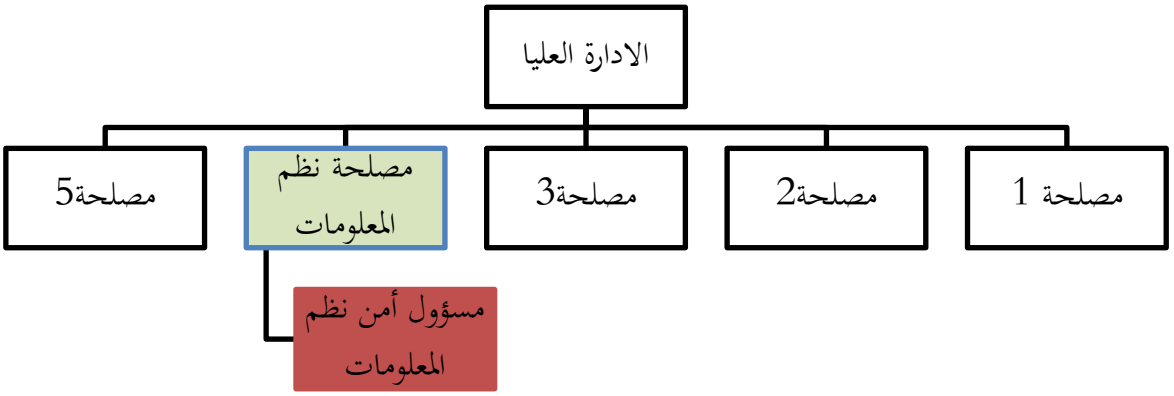
أ- وظيفة أمن المعلومات على مستوى المنظمة:

المؤسسة الوطنية للأشغال البترولية الكبرى من بين المؤسسات الجزائرية القلة التي نجدها تخصص وظيفة لأمن نظم المعلومات ، إذ هناك مصلحة خاصة في المنظمة تسمى مصلحة نظم المعلومات ، و تتكون من رئيس المصلحة و مختصين في مجال أنظمة المعلومات و الاعلام الآلي ، و هناك مسؤول أمن نظم المعلومات.

في هذه المصلحة يوجد غرفة خاصة بتجهيزات نظم المعلومات ، تضم أجهزة متصلة بكل أجهزة نظم المعلومات في المؤسسة ، و هي غرفة محدودة الدخول ، إذ يمنع دخول أحد دون المسؤولين عنها من عمال المصلحة.

في مؤسسة الأشغال البترولية الكبرى مسؤول أمن نظم المعلومات متواجد على مستوى مصلحة نظم المعلومات ، و هو مسؤول عن أمن حواسب و تجهيزات نظم المعلومات و المعلومات الحساسة و الموارد الحرجة في المصلحة و كل المؤسسة.

الشكل (4.1) : مكانة مسؤول أمن المعلومات في تنظيم المؤسسة



المصدر : من إعداد الباحثة بناءا على معلومات من المؤسسة

ب- سياسة أمن المعلومات في المؤسسة :

المؤسسة الوطنية للأشغال البترولية الكبرى تعتمد سياسة أمن معلومات واضحة المعالم و محددة القواعد و المبادئ و يتم نشرها الكترونيا على مستوى موقع المؤسسة ليتم الاطلاع عليها من قبل كافة الموظفين.

ت- وعي الادارة و الموظفين :

رغم اهتمام المؤسسة بأمن نظم المعلومات و تسخير كل الوسائل المادية و البشرية و التقنية لذلك ، إلا أن وعي الادارة العليا بخطر التهديدات على نظم المعلومات منخفض ، كما أن الثقافة الأمنية للموظفين ليست بالمستوى المطلوب ، إذ نجد أن أمن المعلومات يطبق فقط من الناحية المادية التي تتمثل في أمن المحيط ، و من الناحية التقنية من برامج مطبقة على الحواسب و الخوادم ....، أما الوعي الحقيقي و اليقظة الاستراتيجية بخطر التهديدات و أهمية الأمن نجده فقط على مستوى مصلحة نظم المعلومات ، فهي المصلحة الوحيدة التي تهتم بأمن المعلومات و كل ما يتعلق به على الوجه المطلوب ، و تحاول جاهدة في تعزيز الثقافة الأمنية على مستوى المؤسسة.

ث- المؤسسة و ايزو 27001:

المؤسسة الوطنية للأشغال البترولية الكبرى هي المؤسسة الوحيدة من بين المؤسسات الصناعية التي شملتها الدراسة التي اهتمت بضرورة تطابق أمن المعلومات لديها بمعايير و مقاييس دولية معترف بها عالميا ، و وقع اختيارها على أشهر معيار خاص بأمن نظم المعلومات و هو معيار ايزو 27001 ، حيث باشرت كل الاجراءات اللازمة من أجل الحصول على شهادة ايزو 27001 و كيفت أنظمة معلوماتها و سياستها الأمنية و طرق الحماية حسب متطلبات المواصفة ، و حصلت على شهادة ايزو 27001 سنة 2010 لمدة 3 سنوات ، و لكن للأسف المؤسسة لم تستمر في عملية التجديد ، لأن هذه الشهادة ليست أبدية كباقي الشهادات ، و إنما تكون لفترة معينة و تتطلب في كل مرة التجديد و التحقيق من أجل أن تكون المؤسسة دائما في المستوى المطلوب.

2- تهديدات أمن المؤسسة

المؤسسة كغيرها من المؤسسات الكبرى تتعرض إلى تهديدات عدة منها المادية مثل السرقة و الكوارث... و منها التقنية كالقرصنة ، و من التهديدات التي تعرضت لها المؤسسة ما يلي :

أ- التهديدات المادية :

- الدخول غير المصرح : و يقصد به دخول أي شخص معروف أو غير معروف ، غير مرخص له بالدخول إلى موقع المنظمة ، فمجرد دخوله يعتبر خطر على المؤسسة.
- سرقة التجهيزات : حيث تعرضت المؤسسة لعمليات سرقة تمت عن طريق اقتحام موقع المؤسسة بطريقة غير شرعية و سرقة تجهيزات خاصة بالمؤسسة.
- كوارث طبيعية : تعرضت المؤسسة لمرة واحدة فقط و ذلك على مستوى فرع من فروعها لكارثة طبيعية كلفتها بعض الخسائر.

ب– التهديدات التقنية : من بين التهديدات التقنية التي تعرضت لها المؤسسة ما يلي :

- دخول غير مرخص : و نقصد هنا الدخول لجهاز أو نظام معلومات من طرف شخص غير مصرح له بذلك ، سواء كان من داخل (العمال) أو من خارج المؤسسة (الهاكر).
- قرصنة : و كانت هذه القرصنة خارجية من طرف هاوي ، و خلفت آثار بسيطة.
- سبام :
- الدودة المعلوماتية : فالمؤسسة كغيرها من المؤسسات لم تسلم من خطر هذا البرنامج الخبيث و الذي تم شرح طريقة انتشاره سابقا.

و تم التعامل مع هذه التهديدات باتخاذ عدة إجراءات نذكر منها : إجراءات تصحيحية ، تعديل الاعدادات ، تحقيقات داخلية ، تعزيز أمن محيط المؤسسة ، تغيير كلمات المرور ، تحسين و تعديل التجهيزات.

3– وسائل الحماية المطبقة من طرف المؤسسة

الحماية المطبقة من طرف المؤسسة هي حماية مادية و برمجية

أ– حماية مادية : و تتمثل الحماية المادية في حماية الموقع و حماية التجهيزات

- **أمن موقع المنظمة** : و تمثل في مجموعة من الاجراءات نذكر :

- مراقبة الدخول : و يكون ذلك من خلال مكتب الاستقبال الموجود في مدخل المنظمة يضم عدد كبير من أعوان الأمن ، و يمنع أي دخول للمؤسسة دون المرور عليه ، فالدخول للمؤسسة يتطلب تبرير و من ثم الاتصال بالجهة المستقبلة ، و بعد التصريح بالدخول يتم كتابة المعلومات الشخصية و تاريخ و توقيت الدخول على سجل الزيارات ، مع حجز البطاقة الشخصية.
- الشارات : إجبار الزوار على حمل شارات تميز بين الزوار و العمال و المتدربين.
- مرافقة عون الأمن للزائر إلى المكان المحدد من أجل منع أي دخول إلى موقع غير مصرح له.
- استخدام البطاقات الممغنطة من أجل الدخول.
- المراقبة عن طريق الكاميرات الموجودة في كل مكان داخل و خارج المؤسسة .
- منع دخول أي سيارة للمؤسسة غير سيارات العمال.

- **أمن تجهيزات المنظمة** : لأمن تجهيزات نظم المعلومات اتخذت المؤسسة التدابير الأمنية التالية:

- توفير التهوية المناسبة خصوصا للغرف التي تحوي أجهزة و خوادم ، و التي تتطلب مستوى تهوية محدد.

- التجهيزات الحساسة موجودة في أماكن محددة و مؤمنة بطريقة مكثفة.
- المؤسسة لديها مركز احتياطي مجهز بأنظمة معلومات في حال حصول كارثة يتم اللجوء إليه.

ب– حماية برمجية : و تتمثل في البرامج و التطبيقات التي تحمي أجهزة نظم المعلومات و نذكر :

- مضادات الفيروسات : و هي القاعدة الأولى لأي حماية برمجية ، حيث أن المؤسسة لا تعتمد على البرامج المقرصنة و إنما تشتري برامج مضادات فيروس أصلية.
- مضادات السبام
- الجدران النارية : فالمؤسسة تعتمد على الجدران النارية المتمثلة في أجهزة مخصصة لذلك و ليس تلك التي تكون في شكل برامج.
- التشفير : و نقصد بذلك تشفير كل المعلومات الحساسة المرسلة سواء عند التواصل مع فروعها أو مع أعوان خارجية
- الشبكة الافتراضية
- الدعم الاحتياطي
- البيئة الافتراضية
- الحفظ الدوري للمعلومات داخل و خارج المؤسسة
- التحديث الدوري
- تغيير كلمات المرور من فترة لأخرى أو عند حصول أي اختراق.

ت– الحماية اليومية : تكون من خلال التحسيس و التكوين من فترة لأخرى .

المبحث الثاني : منهجية الدراسة

يميل الاتجاه السائد لدى العلماء و الباحثين إلى الجمع بين المناهج النظرية و التطبيقية ، فأي دراسة نظرية لابد لها من دراسة تطبيقية ميدانية على المجتمع ترفع من مصداقيتها.

المطلب الأول : مجتمع و عينة الدراسة

الفرع الأول : مجتمع الدراسة

يتمثل مجتمع هذه الدراسة في كل مؤسسات القطاع الصناعي و الخدمي في الجزائر ، و التي تملك قاعدة بيانات مهمة تسعى إلى حمايتها ، و تطبق أمن المعلومات إما صراحة و بسياسة أمنية واضحة أو تطبقه ضمنيا من خلال نشاطاتها اليومية دون التصريح به.

الفرع الثاني : عينة الدراسة

شملت الدراسة الميدانية لهذا البحث مجموعة من المؤسسات الجزائرية العاملة سواء في القطاع الصناعي أو الخدمي ، و التي بلغ عددها (35) مؤسسة موزعة على ولايات مختلفة : تلمسان (25) ، سيدي بلعباس (4) ، الجزائر العاصمة (5) ، وهران (1) ، و استخدمت الباحثة أسلوب العينة العشوائية الطبقية لسحب العينة من المجتمع ، و الفئة التي تم استهدافها كوحدات معاينة هي فئة مديري أمن نظم المعلومات و التي لم نجدها إلا في مؤسسة واحدة ، لذا تعاملنا في المؤسسات الأخرى مع فئة مديري أنظمة المعلومات ، فان غابت هذه الأخيرة كانت يتم التعامل مع مسؤولي الاعلام الآلي أو المعلوماتية باعتبارهم الفئة التي تتعامل مع أنظمة المعلومات .

المطلب الثاني : أساليب جمع البيانات

تم الاعتماد في هذا البحث على أداتين : المقابلة الشخصية و الاستبيان.

الفرع الأول : المقابلة الشخصية

نظرا لعدم امكانية الحصول على كل المعلومات المطلوبة من خلال الاستمارة ، اعتمدت الباحثة أسلوب المقابلة الشخصية التي يتم من خلالها أولا التعرف على طبيعة نظام معلومات المؤسسة لمعرفة مدى توافقه و تماشيه مع موضوع الدراسة ، و ثانيا لشرح عناصر الاستبيان و المقصود منها لكي تكون الاجابات موضوعية ، وثالثا من أجل الحصول على معلومات إضافية و شرح معمق لطبيعة الأنظمة المعلوماتية في المؤسسة و مكوناتها ، و الطرق المستخدمة لحمايتها ، و تتم المقابلات عن طريق أسئلة تم تحضيرها مسبقا من أجل اختصار الوقت و الحصول على أكبر كم من المعلومات التي تحتاج إليها الدراسة ، حيث يتم تسجيل البيانات صوتيا ثم تفريغها بعد ذلك طبعا بعد

الحصول على إذن الشخص المقابل ، أو يتم تدوينها يدويا مباشرة ، إلا أن هناك بعض المؤسسات التي لم نستطع فيها الاعتماد على المقابلة الشخصية إما لعدم امكانية التنقل أو لرفض المؤسسة لذلك فاكتفينا بالاستبيان.

الفرع الثاني : الاستبيان

يعتبر الاستبيان أهم و أسرع أداة لجمع البيانات ، لاحتوائه على قدر كبير من الأسئلة تفرض إجابات محددة ، ما يقدم لنا كم هائل من المعلومات في وقت وجيز و في هذه الدراسة مثّل الاستبيان الأداة الرئيسية للبحث ، و بغية تحليل الاشكالية و نفي أو اثبات الفرضيات ، و بناء على ما ورد في الجانب النظري تم تصميم استبيان موجه لمسؤولي أنظمة المعلومات أو المعلوماتية باعتبارهم الوحيدين القادرين على الاجابة على الاستبيان بشكل موضوعي نظرا لطبيعة الموضوع ، فتم توزيع 50 استمارة تم استرجاع منها 38 مع استبعاد 3 منها لعدم الاجابة على عدد كبير من الأسئلة ما يجعلها غير صالحة للتحليل الاحصائي ، و عليه تم تحليل 35 استمارة و تمت عملية التوزيع وفق عدة طرق و هي :

- مدخل طريقة الخروج : و هي تسليم الباحثة الاستبيان يدويا إلى المسؤول عن أمن أنظمة المعلومات، و شرح كل بنود الاستبيان ، و الاجابة تكون مباشرة ، و هذا ما تم في أغلب الحالات ، إلا أن هناك بعض المؤسسات التي نجد المسؤول فيها جد منشغل فتتم ترك الاستبانة و الرجوع لأخذها في وقت آخر .
- الاستبيان الالكتروني : تم تصميم استبيان الكتروني وجه للمؤسسات التي صعُب الانتقال اليها ، أو التي تم الانتقال إليها و لكن صعُب الوصول إلى المسؤولين فيها ، و لجمع أكبر كم من المعلومات و الوصول إلى عدد أكبر من المؤسسات تم اعتماد هذه الطريقة على مستوى حالات قليلة.

و قد كان تصميم الاستبيان موافقا لما جاء في الجانب النظري ، و هذا لاسقاط هذا الأخير على واقع المؤسسات الجزائرية ، و تم تخصيص الجزء الأول من الاستبيان للبيانات الشخصية و الوظيفية و بعض المعلومات العامة حول الموضوع ، أما الجزء الثاني فتم تخصيصه لمحاور الدراسة الثلاثة :

- المحور الأول : طبيعة أمن المعلومات داخل المؤسسة ، و يشمل العبارات من 1 إلى 9.
- المحور الثاني : طبيعة التهديدات ، و شمل العبارات من 10 إلى 29 ، و ينقسم هذا المحور إلى أبعاد ، البعد الأول المتمثل في العبارات من 10، 12، 13 مخصص للتهديدات الداخلية التي تتعرض لها المؤسسة ، أما البعد الثاني المتمثل في العبارات 11 ، 14 ، 15، 16 مخصص للتهديدات الخارجية التي تتعرض لها المؤسسة ، و البعد الثالث المتمثل في العبارات من 17 إلى 19 مخصص للتهديدات المادية ، و البعد الرابع المتمثل في العبارات 20 ،

21 مخصص للتهديدات البرمجية و البعد الخامس المتمثل في التهديدات التنظيمية من العبارة 22 إلى 25 و البعد السادس المتمثل في العبارات من 26 إلى 29 مخصص لدوافع التهديدات التي تتعرض لها المؤسسة .

- المحور الثالث : طبيعة الحماية المطبقة ، يشمل العبارات من 30 إلى 50 ، و ينقسم هذ المحور إلى أبعاد ، البعد الأول يشمل العبارات من 30 إلى 33 مخصص لطبيعة الحماية المادية التي تطبقها المؤسسة لحماية موقعها ، أما البعد الثاني الذي يشمل العبارات 34 إلى 40 مخصص لطبيعة الحماية البرمجية التي تطبقها المؤسسة، و البعد الثالث الذي يشمل العبارات 41 إلى 44 مخصص لتصنيف المعلومات الحساسة و طبيعة التعامل معها ، أما البعد الرابع الذي يشمل العبارات من 45 إلى 50 مخصص لعملية تسيير المخاطر المحتملة.

و تم تصميم الاستبيان وفق سلم ليكرت الخماسي لتحويل المتغيرات الكيفية إلى متغيرات كمية كي يسهل تحليلها وذلك كما يلي :

موافق تماما ← 5

موافق ← 4

محايد ← 3

غير موافق ← 2

غير موافق تماما ← 1

المطلب الثالث : أساليب تحليل البيانات

بغية التحليل الاحصائي للبيانات المجمعة تم الاعتماد على مجموعة من الأدوات الاحصائية التي يوفرها برنامج الحزمة الاحصائية للعلوم الاجتماعية SPSS 19 ، و من أهم الأساليب التي اعتمدت عليها الباحثة:

- **معامل ألفا كرونباخ لقياس الثبات Cronbach's Alpha:**

تم استخدام هذا المعامل لاختبار و قياس ثبات أداة الدراسة ، و قياس مدى الاتساق الداخلي بين عبارات و محاور الدراسة ، و تتراوح قيمته بين (0و1) ، و انخفاض قيمته عن 0.6 دليل على انخفاض الثبات الداخلي ، أما اذا تجاوزت 0.6 فهذا دليل على ثبات الأداة و امكانية اعتمادها في الدراسة.

- **معامل ارتباط بيرسون Pearson Correlation:**

تم استخدام معامل ارتباط بيرسون لقياس صدق مضمون الاستمارة ، حيث يتم حساب معامل الارتباط بين درجة كل عبارة و المحور الذي تنتمي إليه ، حيث تتراوح قيمته بين (1 و -1) و تكون كالتالي:

1-	0.5-	0	0.5	1

ارتباط طردي تام إ.طردي متوسط لا يوجد ارتباط إ.عكسي متوسط إ.عكسي تام

- **الجداول التكرارية :**

تم استخدام الجداول التكرارية لمعرفة توزيع الاجابات (عدد تكرار الاجابات و النسب المئوية) حسب مقياس ليكرت الخماسي المستعمل في الاستمارة.

- **مقاييس النزعة المركزية و التشتت**

تم استخدام المتوسطات الحسابية و الانحرافات المعيارية من بين مقاييس النزعة المركزية و التشتت لتحديد درجات الموافقة على الإجابات و معرفة مدى تشتتها.

- **المتوسط الحسابي** : تم استخدامه لحساب متوسط الإجابات في الأسئلة المغلقة فقط ، و ذلك بعد تحويل البيانات الكيفية إلى كمية وفق سلم ليكرت الخماسي، (1+2+3+4+5/5=3) ، فاذا كان الوسط أكبر من 3 تكون الإجابات مائلة إلى موافقة عالية ، عالية جدا ، أما إذا كان الوسط أقل من 3 تكون الإجابات مائلة إلى موافقة قليلة أو عدم موافقة.

- بما أن المتغير الذي يعبر عن الخيارات (موافق بشدة : موافق.....) مقياس ترتيبي ، و الأرقام التي تدخل في البرنامج تعبر عن الأوزان و هي (موافق بشدة = 5 ، موافق =4 .....) فان حساب المتوسط الحسابي يتم بحساب طول الفترة و هي حاصل قسمة 4 على 5 ، حيث تمثل 4 عدد المسافات (من 1 إلى 2 مسافة أولى ، من 2إلى 3 مسافة ثانية ، من 3 إلى 4 مسافة ثالثة ، من 4 إلى 5 مسافة رابعة) ، و 5 تمثل عدد الخيارات ، و عند قسمة 5/4 ينتج طول الفترة و يساوي 0.80 و يصبح التوزيع حسب الجدول التالي[1] :

[1] **وليد عبد الرحمن خالد الفرا** ، "تحليل بيانات الاستبيان باستخدام البرنامج الاحصائي spss ، الندوة العالمية للشباب الاسلامي ، إدارة البرامج و الشؤون الخارجية ، 1430ه ، ص 26

المتوسط	المستوى
من 1 إلى 1.79	لا توجد موافقة
من 1.80 إلى2.59	درجة موافقة قليلة
2.60 إلى 3.39	درجة موافقة متوسطة
من 3.40 إلى 4.19	درجة موافقة عالية
من 4.20 إلى 5	درجة موافقة عالية جدا

- **الانحراف المعياري** : هو أكثر مقاييس التشتت استخداما في الدراسات التطبيقية ، و كلما كان الانحراف المعياري صغيرا كلما كانت النتائج أقل تشتتا و بالتالي النتائج أكثر مصداقية.

- **مصفوفة الارتباط لبيرسون** لاختبار العلاقة بين المتغيرين
- **تحليل الانحدار الخطي البسيط** لمعرفة مدى تأثير كل متغير من المتغيرات المستقلة أو أبعاد المتغيرات المستقلة على المتغير التابع (مستوى أمن المعلومات)
- **تحليل الانحدار الخطي المتعدد** لمعرفة أي المتغيرات المستقلة أكثر تأثيرا على المتغير التابع.
- **تحليل التباين الأحادي One Way Anova** لتفسير الفروق الموجودة في مستوى أمن المعلومات في المؤسسات الجزائرية على أساس طبيعة التهديدات و طبيعة الحماية المطبقة .

المبحث الثالث : تحليل نتائج الدراسة

المطلب الأول : وصف عينة الدراسة و طبيعة وظيفة أمن المعلومات فيها

الفرع الأول : وصف عينة الدراسة

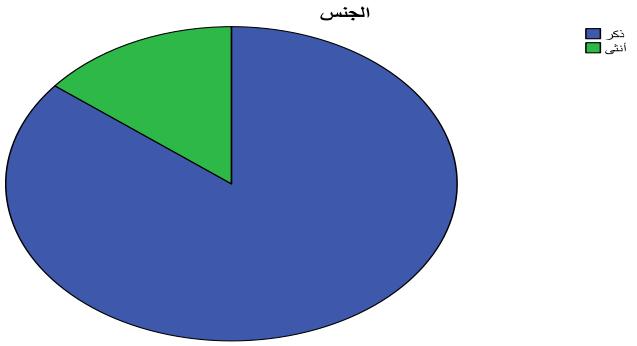
من خلال الجزء الأول من الاستمارة سنتعرف على أهم خصائص العينة على أساس الجنس ، التحصيل العلمي ، عدد سنوات الخبرة.

أ– الجنس

الجدول (4.2) : توزيع أفراد العينة حسب الجنس

الجنس	التكرار	النسبة
ذكر	30	%85.7
أنثى	5	%14.3
المجموع	35	%100

الشكل (4.2): التوزيع النسبي لأفراد العينة حسب الجنس



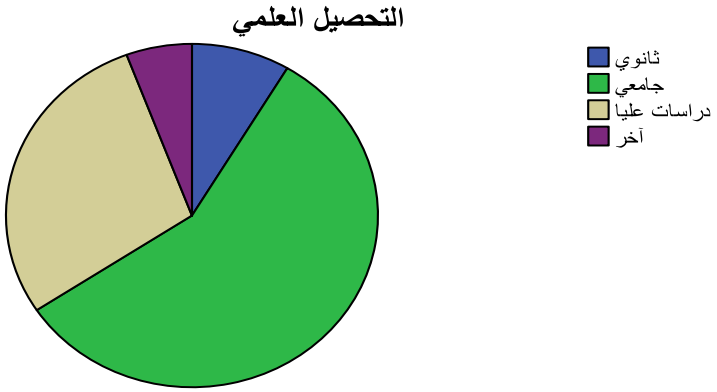
من خلال الجدول و الشكل (4.2) نلاحظ اكتساح فئة الذكور لأفراد العينة بنسبة 85 % ما يعني أن وظيفة أمن المعلومات أو نظم المعلومات أو الاعلام الآلي بصفة عامة في المؤسسات الجزائرية هي موكلة لفئة الذكور و هذا قد يعود لطبيعة العمل التي قد تتطلب أحيانا مجهودا للتعامل مع المعدات و الآلات.

ب- التحصيل العلمي

الجدول (4.3) : توزيع أفراد العينة حسب التحصيل العلمي

التحصيل العلمي	التكرار	النسبة
ثانوي	3	%8.6
جامعي	20	%57.1
دراسات عليا	10	%28.6
آخر	2	%5.7
المجموع	**35**	**%100**

الشكل (4.3) : توزيع أفراد العينة حسب التحصيل العلمي



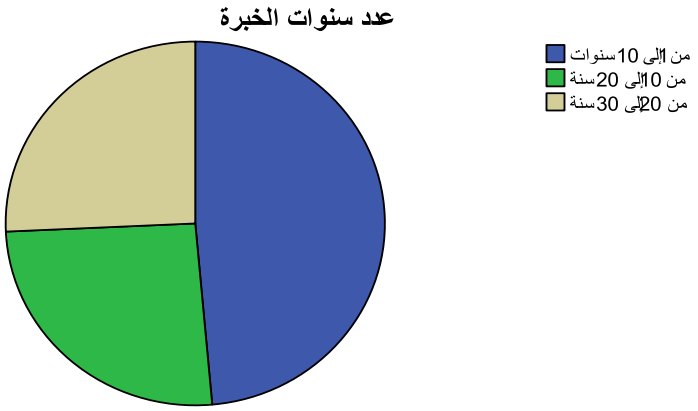
من خلال الجدول و الشكل (4.3) نستنتج أن أغلب أفراد العينة لهم مستوى تعليمي مناسب إذ أن 57.1 % من أفراد العينة ذوي مستوى جامعي و 28.6 % منهم لهم دراسات عليا سواء ماجستير أو دكتوراه و 8.6% لهم مستوى تعليم ثانوي و غالبا ما تكون هذه الفئة من أعمار متقدمة و لها خبرة واسعة في هذا المجال و 5.7 % لهم مستوى آخر و نقصد بها غالبا شهادات التكوين أو شهادات من مدارس و معاهد خاصة ، و علية فان معظم أفراد العينة لهم مستوى تعليمي عالي يتناسب مع وظيفة الاعلام الالي و أمن نظم المعلومات.

ث- عدد سنوات الخبرة

الجدول(4.4) : توزيع أفراد العينة حسب عدد سنوات الخبرة

عدد سنوات الخبرة	التكرار	النسبة
من 1 إلى 10 سنوات	17	% 48.6
من 10 إلى 20 سنة	9	% 25.7
من 20 إلى 30 سنة	9	% 25.7
المجموع	**35**	**% 100**

الشكل(4.4) : توزيع أفراد العينة حسب عدد سنوات الخبرة



من خلال الجدول و الشكل (4.4) نلاحظ أن 48.6 % من أفراد العينة لهم خبرة تتراوح بين 1 و 10 سنوات ، و 25.7 % لهم خبرة تتراوح بين 10 إلى 20 سنة و 25.7 % ذوو خبرة تتراوح بين 20 إلى 30 سنة و هذا ما يعكس التنوع في هذا المجال ، فالنسبة الأكبر هي لأصحاب أقل خبرة و هذا يدل على إعطاء الفرص للشباب و خريجي الجامعات و المعاهد الجدد لدخول هذا المجال بدراساتهم و أفكارهم الحديثة و تطبيقها على مستوى المؤسسات دون الاستغناء عن أصحاب الخبرة الذين يقدمون الدعم لمن سيخلفهم ، فوظيفة المسؤول عن نظم المعلومات و أمنها وظيفة تتطلب فطنة و حنكة و رصيد معرفي عالي و احتكاك كبير بالبيئة الخارجية خصوصا التكنولوجية.

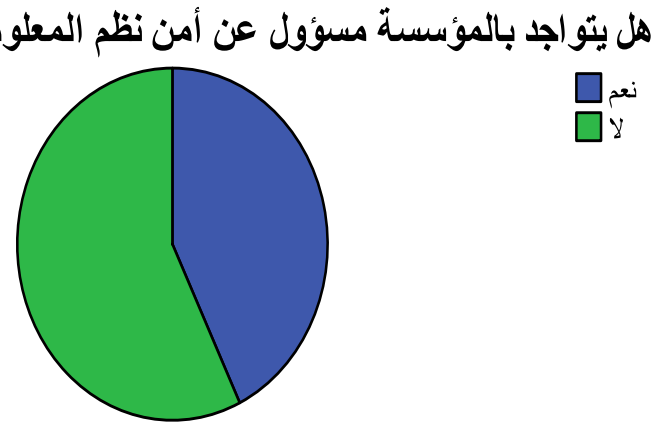
الفرع الثاني : وظيفة مسؤول أمن المعلومات على مستوى العينة المدروسة

أ- هل يتواجد بالمؤسسة مسؤول أمن المعلومات؟

الجدول (4.5): وظيفة مسؤول أمن المعلومات بالمؤسسات محل الدراسة

	التكرار	النسبة
نعم	15	%42.9
لا	20	%57.1
المجموع	**35**	**%100**

الشكل (4.5) : وظيفة مسؤول أمن المعلومات بالمؤسسات محل الدراسة



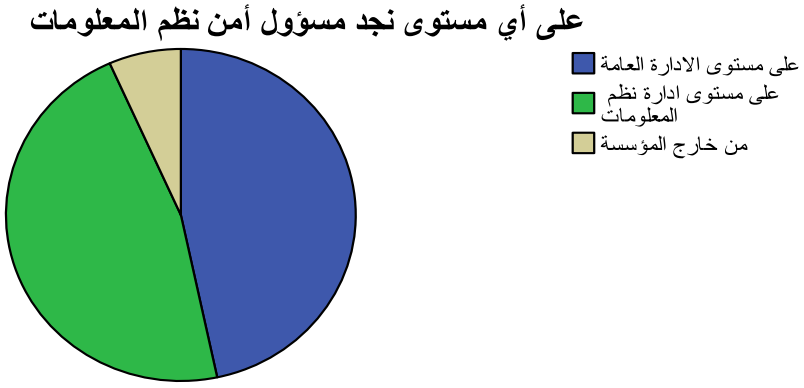
من خلال الجدول و الشكل (4.5) نلاحظ أن أغلب المؤسسات الجزائرية محل الدراسة لا يتواجد بها وظيفة خاصة باسم مسؤول أمن المعلومات (57.1 %) و هذا يعود لتدني مستوى الأمن بها و غياب الثقافة الأمنية و عدم ادراك أهمية خلق مثل هذه الوظيفة على مستوى المؤسسة في حين 42 % أجابت ب نعم لوجود وظيفة أمن المعلومات بمؤسساتهم و أغلب هذه المؤسسات نجدها إما بنوك أو مؤسسات مالية أو شركات اتصال و التي تفرض عليها طبيعة عملها خلق مثل هذه الوظيفة.

ب- إذا نعم .على أي مستوى نجد مسؤول أمن المعلومات؟

الجدول (4.6): مستوى تواجد مسؤول أمن المعلومات

	التكرار	النسبة
على مستوى الادارة العليا	7	%46.6
على مستوى ادارة نظم المعلومات	7	%46.6
من خارج المؤسسة	1	%6.8
المجموع	**15**	**%100**

الشكل (4.6) مستوى تواجد مسؤول أمن المعلومات



من خلال الجدول و الشكل (4.6) نلاحظ أن المؤسسات التي صرحت بتواجد وظيفة مسؤول أمن المعلومات على مستواها فان 46.6 % من هؤلاء المسؤولين متواجدون على مستوى الادارة العليا في حين 46.6 % على مستوى ادارة نظم المعلومات و 6.8 % منهم فقط من يستعين بمسؤول أمن معلومات من خارج المؤسسة .

المطلب الثاني : قياس ثبات و صدق أداة الدراسة

الفرع الأول : قياس ثبات أداة الدراسة

لقياس ثبات الاستبيان و مدى اتساق أسئلته تم استخدام مقياس " ألفا كرونباخ Alpha Cronpach "

الجدول (4.7) : قيمة معامل الثبات " ألفا كرونباخ Alpha Cronpach "

	عدد العبارات	قيمة ألفا كرونباخ
المحور الأول	**9**	**0.959**
المحور الثاني	**20**	**0.616**
المحور الثالث	**21**	**0.970**
الاجمالي	**50**	**0.949**

المصدر : بناء على نتائج الدراسة (spss .19)

من خلال الجدول (4.7) نلاحظ أن قيمة معامل الثبات عالية تفوق الحد الأدنى المطلوب ما يؤكد صلاحية أداة الدراسة للاستخدام و التي تتمتع بدرجة ثبات و موثوقية عالية جدا بنسبة 94.9%

الفرع الثاني : قياس صدق أداة الدراسة

للحكم على صدق أداة الدراسة يتم الاعتماد على معامل الارتباط بيرسون Pearson و الذي يعبر عن صدق المضمون ، حيث يتم حساب معامل الارتباط بين كل عبارة و المحور الذي تنتمي اليه.

1- **المحور الأول : مستوى أمن المعلومات داخل المؤسسة**

الجدول (4.8) معامل الارتباط بيرسون لعبارات المحور الأول مع و الدرجة الكلية للمحور

مستوى أمن المعلومات داخل المؤسسة			
رقم العبارة	**معامل الارتباط**	**رقم العبارة**	**معامل الارتباط**
العبارة 1	0.825**	العبارة 6	0.891**
العبارة 2	0.886**	العبارة 7	0.916**
العبارة 3	0.815**	العبارة 8	0.821**
العبارة 4	0.909**	العبارة 9	0.896**
العبارة 5	0.856**		

المصدر : من إعداد الطالبة اعتمادا على نتائج spss19

2- **المحور الثاني : طبيعة تهديدات أمن المعلومات**

الجدول (4.9) : معامل الارتباط بيرسون لعبارات المحور الثاني و الدرجة الكلية له

المحور الثاني : طبيعة تهديدات أمن المعلومات							
مصادر التهديد		طبيعة التهديد		أسباب التهديد		دوافع التهديد	
رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
العبارة 10	0.581**	العبارة 17	0.337*	العبارة 22	0.353*	العبارة 26	0.264
العبارة 11	0.322	العبارة 18	0.410*	العبارة 23	0.314	العبارة 27	0.413*
العبارة 12	0.500**	العبارة 19	0.447**	العبارة 24	0.529**	العبارة 28	0.051-
العبارة 13	0.350*	العبارة 20	0.411*	العبارة 25	0.275	العبارة 29	0.007
العبارة 14	0.560**	العبارة 21	0.445**				
العبارة 15	0.394*						
العبارة 16	0.150						

3- **المحور الثالث : طبيعة الحماية المطبقة داخل المؤسسة**

الجدول (4.10): معامل الارتباط بيرسون لعبارات المحور الثالث و الدرجة الكلية للمحور

المحور الثالث : طبيعة الحماية المطبقة داخل المؤسسة							
الحماية المادية		الحماية البرمجية		تصنيف المعلومات الحساسة		تسيير المخاطر المحتملة	
رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
العبارة 30	0.746**	العبارة 34	0.458**	العبارة 41	0.597**	العبارة 45	0.952**
العبارة 31	0.729**	العبارة 35	0.675**	العبارة 42	0.859**	العبارة 46	0.898**
العبارة 32	0.762**	العبارة 36	0.835**	العبارة 43	0.740**	العبارة 47	0.951**
العبارة 33	0.678**	العبارة 37	0.849**	العبارة 44	0.775**	العبارة 48	0.893**
		العبارة 38	0.867**			العبارة 49	0.705**
		العبارة 39	0.879**			العبارة 50	0.912**
		العبارة 40	0.800**				

المطلب الثالث : تحليل نتائج الدراسة

الفرع الأول : مستوى أمن المعلومات في المؤسسة الجزائرية (المتغير التابع)

الجدول(4.11) : مستوى تطبيق أمن المعلومات في المؤسسة الجزائرية

رقم العبارة	العبارة	الوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
1	الإدارة العليا واعية و محسسة بما يكفي بطبيعة التهديدات التي تتعرض لها نظم المعلومات	3.45	1.521	عالية	2
2	الادارة العليا واعية بأهمية و ضرورة توفير الأمن لأنظمة المعلومات	3.62	1.456	عالية	1
3	اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية	3.37	1.476	متوسطة	4
4	المؤسسة تخصص ميزانية خاصة لإدارة عملية أمن نظم المعلومات	3.11	1.604	متوسطة	7
5	المصاريف التي تصرف على تطبيق أمن المعلومات ضرورية و تساهم في حماية المؤسسة و تطورها	3.40	1.376	عالية	3
6	المؤسسة تعتمد سياسة أمنية مكتوبة و يعرفها الجميع	3.31	1.711	متوسطة	5
7	قواعد و مبادئ السياسة الأمنية محددة و واضحة	3.11	1.728	متوسطة	6
8	الموظفون ذوي ثقافة أمنية و واعون بمسؤولياتهم	2.82	1.562	متوسطة	8
9	المؤسسة تقوم بدورات تكوينية و تحسيسية حول موضوع أمن المعلومات	2.80	1.510	متوسطة	9
	المجموع	**3.22**	**1.347**	**متوسطة**	

يمثل هذا المحور مستوى أمن المعلومات في المؤسسة الجزائرية و درجة تطبيقها له ، حيث يتضح من خلال الجدول أن درجة تطبيق المؤسسة الجزائرية لأمن المعلومات متوسطة بوسط حسابي قدرة 3.22 و انحراف معياري 1.347 ، أما درجات الموافقة على عبارات المحور فكانت متباينة ، و سيتم ترتيبها تنازليا :

- **الموافقة العالية** :

- العبارة " **الادارة العليا واعية بأهمية و ضرورة توفير الأمن لأنظمة المعلومات** " : جاءت هذه العبارة في الترتيب الأول بمتوسط حسابي 3.62 و انحراف معياري 1.45 ما يدل على أن الادارة العليا في المؤسسة الجزائرية واعية و مدركة لأهمية حماية أنظمتها المعلوماتية و أهمية هذه الأخيرة في ضمان استمراريتها.

- العبارة " **الإدارة العليا واعية و محسسة بما يكفي بطبيعة التهديدات التي تتعرض لها نظم المعلومات**" جاءت في الترتيب الثاني بمتوسط حسابي 3.45 و انحراف معياري 1.52 ما يعني أن الادارة العليا في المؤسسات الجزائرية لها خلفية جيدة وادراك قوي لطبيعة التهديدات التي تفرضها البيئة المحيطة سواء الداخلية أو الخارجية.

- العبارة " **المصاريف التي تصرف على تطبيق أمن المعلومات ضرورية و تساهم في حماية المؤسسة و تطورها** " جاءت في المرتبة الثالثة بمتوسط حسابي 3.40 وانحراف معياري 1.376 ما يؤكد درجة وعي المؤسسة الجزائرية بأهمية أمن المعلومات و أن المصاريف التي تصرف عليه ليست مصاريف زائدة و انما استثمار مربح.

- **الموافقة المتوسطة** :

- العبارة " **اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية** " جاءت في المرتبة الرابعة بمتوسط حسابي 3.37 و انحراف معياري 1.476 و عليه يمكن القول أن نسبة معقولة من المؤسسات الجزائرية تعتمد على اجراءات حماية مواكبة للتطورات التكنولوجية و واعية بالتغير المستمر في البيئة.

- العبارة " **المؤسسة تعتمد سياسة أمنية مكتوبة و يعرفها الجميع** " جاءت في المرتبة الخامسة بمتوسط حسابي 3.31 و انحراف معياري 1.711 تتبعها العبارة " **قواعد و مبادئ السياسة الأمنية محددة و واضحة** " في المرتبة السادسة بمتوسط حسابي 3.11 و انحراف معياري 1.728 ما يعكس نسبة تشتت عالية وهذا دليل على الاختلاف الواضح بين آراء المستجوبين حول موضوع السياسة الأمنية، إذ يوجد بعض المؤسسات لا تعرف حتى ما معنى السياسة الأمنية و عليه يمكن القول أن نسبة معقولة من المؤسسات الجزائرية تعتمد على سياسة أمنية مكتوبة و يعرفها الجميع.

- العبارة " **المؤسسة تخصص ميزانية خاصة لإدارة عملية أمن نظم المعلومات** " جاءت في المرتبة السابعة بمتوسط حسابي 3.11 و انحراف معياري 1.604 ما يدل على أن نسبة متوسطة من المؤسسات الجزائرية من تخصص ميزانية لإدارة عملية أمن المعلومات على مستواها.

- العبارة " **الموظفون ذوي ثقافة أمنية و واعون بمسؤولياتهم** " جاءت في المرتبة الثامنة بمتوسط حسابي 2.82 و انحراف معياري 1.562 تليها العبارة " **المؤسسة تقوم بدورات تكوينية و تحسيسية حول موضوع أمن المعلومات** " بمتوسط حسابي 2.80 و انحراف معياري 1.510 في المرتبة التاسعة ما يدل على أن سبب تدني مستوى الأمن في المؤسسة الجزائرية راجع لنقص الوعي و الثقافة الأمنية عند العمال ، و عدم توفير المؤسسة الجزائرية الحملات التحسيسية والدورات التدريبية و التكوينية على أساسيات أمن المعلومات و نظم المعلومات.

الفرع الثاني : طبيعة التهديدات التي تتعرض لها المؤسسة الجزائرية (المتغير المستقل 1)

1- مصادر التهديدات

الجدول (4.12): مصادر التهديدات (الداخلية و الخارجية)

رقم العبارة	العبارة	الوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
10	التهديدات التي تتعرض لها المؤسسة هي من مصادر داخلية	3.228	1.059	متوسطة	2
12	التهديدات التي تتعرض لها المؤسسة هي من طرف العمال	2.885	0.993	متوسطة	4
13	التهديدات التي تتعرض لها المؤسسة هي من طرف المتدربين	2.885	1.050	متوسطة	5
المجموع : التهديدات الداخلية		**3.00**	**0.840**	**متوسطة**	**1**
11	التهديدات التي تتعرض لها المؤسسة هي من مصادر خارجية	2.914	1.010	متوسطة	3
14	التهديدات التي تتعرض لها المؤسسة هي من طرف الزوار	2.628	1.002	متوسطة	6
15	التهديدات التي تتعرض لها المؤسسة هي من طرف المنافسين	2.571	1.065	منخفضة	7
16	التهديدات التي تتعرض لها المؤسسة هي من طرف غرباء (هاكر ، كراكر....)	3.60	1.062	عالية	1
المجموع : التهديدات الخارجية		**2.928**	**0.739**	**متوسطة**	**2**

يمثل الجدول (4.12) مصادر التهديدات الداخلية و الخارجية التي تتعرض لها المؤسسة الجزائرية ، حيث أن التهديدات الداخلية سجلت أكبر متوسط حسابي 3.00 بانحراف معياري 0.840 تتبعها التهديدات الخارجية بمتوسط حسابي 2.92 و انحراف معياري 0.739 ، إلا أن التهديد الذي سجل أكبر متوسط حسابي كان تهديد خارجي ، و كانت العبارات مرتبة كالتالي :

- **درجة الموافقة العالية** :

- العبارة " **التهديدات التي تتعرض لها المؤسسة هي من طرف غرباء (هاكر ، كراكر....)** " جاءت في المرتبة الأولى بمتوسط حسابي 3.60 و انحراف معياري 1.062 و هذا يعني أن أكبر تهديد تتعرض له أنظمة معلومات المؤسسة الجزائرية يكون من طرف غرباء ، و هذا قد يكون صحيحا و قد يكون مجرد تضليل للرأي العام يُقال كلما

عجزت المؤسسة عن كشف الجاني أو تكاسلت عن ذلك أو تعمدت اخفاء شخصية المهدد الذي قد يكون داخليا و هذا ما تثبته بطريقة غير مباشرة اجابات العبارة 10-11.

- **درجة الموافقة المتوسطة** :

- العبارة " **التهديدات التي تتعرض لها المؤسسة هي من مصادر داخلية** " و العبارة " **التهديدات التي تتعرض لها المؤسسة هي من مصادر خارجية** " جاءتا في المرتبة الثانية و الثالثة على التوالي بمتوسط حسابي 3.228 و 2.914 بانحراف معياري 1.059 و 1.010 على التوالي و ربما كان السبب في تقدمهما عن العبارات الأخرى هو عدم تحديد المهدد و انما عبارات عامة ما يشجع المستجوبين على الاجابة و بالتالي الحصول على الاجابة المرادة بطريقة غير مباشرة ، و منه نستنتج أن التهديدات التي تتعرض لها المؤسسة الجزائرية تكون بصفة عامة من الداخل ، تليها التهديدات من الخارج.

– العبارة " **التهديدات التي تتعرض لها المؤسسة هي من طرف العمال** " جاءت في المرتبة الرابعة بمتوسط حسابي 2.885 و انحراف معياري 0.993 تليها في المرتبة الخامسة العبارة " **التهديدات التي تتعرض لها المؤسسة هي من طرف المتدربين** " بمتوسط حسابي 2.885 و انحراف معياري 1.050 ما يؤكد أن أغلب التهديدات التي تتعرض لها المؤسسة الجزائرية هي تهديدات داخلية و لكن بدرجة متوسطة و ليست مرتفعة و هذا يعود لسبب واحد و وحيد و هو خوف المستجوبين من التصريح عن ذلك فكانوا يتملصون من الاجابة بقول لا أعرف أو محايد وهذا ما حال دون ارتفاع درجة الموافقة.

– العبارة " **التهديدات التي تتعرض لها المؤسسة هي من طرف الزوار** " جاءت في المرتبة السادسة بمتوسط حسابي 2.628 و انحراف معياري 1.002 وكانت درجة الموافقة متوسطة قريبة من الانخفاض ما يعني أن الزوار لا يشكلون خطرا على أنظمة معلومات المؤسسة عند نسبة معتبرة من المؤسسات الجزائرية .

– درجة الموافقة المنخفضة

– العبارة " **التهديدات التي تتعرض لها المؤسسة هي من طرف المنافسين** " جاءت في المرتبة الأخيرة بمتوسط حسابي 2.571 و انحراف معياري 1.065 و هذا دليل واضح على عدم وجود منافسة بين المؤسسات الجزائرية و عليه فان المنافسين يشكلون خطرا على أنظمة معلومات المؤسسة الجزائرية بدرجة منخفضة.

2- طبيعة التهديدات (المادية ، البرمجية ، التنظيمية)

الجدول (4.13) : طبيعة التهديدات (مادية ، برمجية ، تنظيمية)

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
17	التهديدات التي تتعرض لها المؤسسة عبارة عن سرقة	2.628	1.238	متوسطة	7
18	التهديدات التي تتعرض لها المؤسسة عبارة عن دخول غير مصرح	2.457	1.066	منخفضة	8
19	التهديدات التي تتعرض لها المؤسسة عبارة عن هندسة اجتماعية(التفتيش في المهملات ، الخداع...)	1.714	0.825	لا يوجد موافقة	9
المجموع (التهديدات المادية)		**2.266**	**0.843**	**منخفضة**	**3**
رقم العبارة	**العبارة**	**المتوسط الحسابي**	**الانحراف المعياري**	**درجة الموافقة**	**الترتيب**
20	التهديدات التي تتعرض لها المؤسسة عبارة عن برامج خبيثة : فيروس ، دودة ، حصان طراودة.....	3.342	1.211	متوسطة	3
21	التهديدات التي تتعرض لها المؤسسة عبارة عن قرصنة معلوماتية : التصنت ، رفض الخدمة ، التزوير	2.628	1.165	متوسطة	6
المجموع(التهديدات البرمجية)		**2.985**	**1.067**	**متوسطة**	**2**
رقم العبارة	**العبارة**	**المتوسط الحسابي**	**الانحراف المعياري**	**درجة الموافقة**	**الترتيب**
22	التهديدات التي تتعرض لها المؤسسة ناتجة عن سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات	3.60	1.168	عالية	1
23	التهديدات التي تتعرض لها المؤسسة ناتجة عن ثغرات أمنية في الأنظمة و البرامج	3.057	1.083	متوسطة	5
24	التهديدات التي تتعرض لها المؤسسة ناتجة عن بساطة أنظمة الحماية	3.20	1.023	متوسطة	4
25	التهديدات التي تتعرض لها المؤسسة ناتجة عن غياب اليقظة داخل المؤسسة	3.60	1.034	عالية	2
المجموع (التهديدات التنظيمية)		**3.364**	**0.845**	**عالية**	**1**

يمثل الجدول(4.13) طبيعة التهديدات التي تتعرض لها المؤسسة الجزائرية حيث احتلت التهديدات التنظيمية المرتبة الأولى بمتوسط حسابي 3.364 و انحراف معياري 0.845 بدرجة موافقة عالية تليها التهديدات البرمجية في المرتبة الثانية بمتوسط حسابي 2.985 و انحراف معياري 1.067 بدرجة موافقة متوسطة ، و في المرتبة الثالثة التهديدات المادية بمتوسط حسابي 2.266 و انحراف معياري 0.843 بدرجة موافقة منخفضة ، و سنقوم بعرض نتائج العبارات كل حده :

- **درجة الموافقة العالية** :

- العبارة " **التهديدات التي تتعرض لها المؤسسة ناتجة عن سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات** " و العبارة " **التهديدات التي تتعرض لها المؤسسة ناتجة عن غياب اليقظة داخل المؤسسة** " بنفس المتوسط الحسابي 3.60 و انحراف معياري 1.168 و 1.034 على التوالي و عليه فان أكبر تهديد يهدد أنظمة معلومات المؤسسات الجزائرية و يخفض مستوى من المعلومات على مستواها هو سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات و غياب اليقظة داخل المؤسسة و هذا كله راجع إلى نتيجة المحور الأول و هي غياب الثقافة الأمنية و نقص التوعية و التحسيس و التدريب.

- **درجة الموافقة المتوسطة**

- العبارة " **التهديدات التي تتعرض لها المؤسسة عبارة عن برامج خبيثة : فيروس ، دودة ، حصان طراودة..**" جاءت في المرتبة الثالثة بمتوسط حسابي 3.342 و انحراف معياري 1.211 بمعنى أن هناك نسبة معتبرة من المؤسسات الجزائرية تعاني من تهديدات البرمجيات الخبيثة و أشهرها الفيروسات و الدودة الالكترونية الخطيرة.

- العبارة " **التهديدات التي تتعرض لها المؤسسة ناتجة عن بساطة أنظمة الحماية** " جاءت في المرتبة الرابعة بمتوسط حسابي 3.20 و انحراف معياري 1.023 تليها في المرتبة الخامسة العبارة " **التهديدات التي تتعرض لها المؤسسة ناتجة عن ثغرات أمنية في الأنظمة و البرامج** " بمتوسط حسابي 3.057 و انحراف معياري 1.083 أي أن الثغرات و النقائص الموجودة على أنظمة معلومات المؤسسة تكون السبب في تهديد أمن معلومات نسبة معتبرة من المؤسسات الجزائرية .

- العبارة " **التهديدات التي تتعرض لها المؤسسة عبارة عن قرصنة معلوماتية : التصنت ، رفض الخدمة ، التزوير..**" جاءت في المرتبة السادسة بمتوسط حسابي 2.628 و انحراف معياري 1.165 و عليه فان القرصنة المعلوماتية تشكل تهديدا على نسبة قليلة من المؤسسات الجزائرية و هذا أمر طبيعي فهذا النوع من التهديد غير منتشر بكثرة مقارنة مع تهديد البرامج الخبيثة.

– العبارة " **التهديدات التي تتعرض لها المؤسسة عبارة عن سرقة** " جاءت في المرتبة السابعة بمتوسط حسابي 2.628 و انحراف معياري 1.238 بمعنى أن السرقة تشكل تهديد على مستوى قليل من المؤسسات الجزائرية

– **درجة الموافقة المنخفضة** :

شملت العبارة " **التهديدات التي تتعرض لها المؤسسة عبارة عن دخول غير مصرح** " بمتوسط حسابي 2.457 و انحراف معياري 1.066 بمعنى أن نسبة قليلة جدا من المؤسسات الجزائرية من تعاني من تهديد الدخول غير المصرح للمؤسسة عموما و قاعات تواجد أنظمة المعلومات خصوصا وهذا يفسر بتواجد الحراسة في كل مؤسسة من المؤسسات الجزائرية.

درجة الموافقة المنعدمة :

شملت العبارة " **التهديدات التي تتعرض لها المؤسسة عبارة عن هندسة اجتماعية (التفتيش في المهملات ، الخداع...)** بمتوسط حسابي 1.714 و انحراف معياري 0.825 بمعنى أن المؤسسة الجزائرية غير معرضة أبدا لهذا النوع من التهديد و لا يؤثر أبدا على مستوى الأمن لديها و هذا يفسر إما أنه حقيقة الهندسة الاجتماعية طريقة غير مستعملة في التجسس على المؤسسات الجزائرية أو أن هناك نقص يقظة من طرف العمال و المسيرين لخطر هذا التهديد الذي لا يكلف مالا و لا وقتا و لا جهدا.

3– دوافع التهديدات

الجدول (4.14) : دوافع التهديدات على أمن نظم المعلومات

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
26	التهديدات التي تتعرض لها المؤسسة هي بدافع الانتقام	2.171	1.150	منخفضة	4
27	التهديدات التي تتعرض لها المؤسسة هي بدافع الحصول على المال	2.228	1.285	منخفضة	3
28	التهديدات التي تتعرض لها المؤسسة هي بدافع المنافسة	2.314	1.105	منخفضة	2
29	التهديدات التي تتعرض لها المؤسسة غير متعمدة	3.20	1.051	متوسطة	1
المجموع		**2.478**	**0.648**	**متوسطة**	

يمثل الجدول (4.14) الدوافع الخفية وراء حدوث التهديدات المختلفة و كانت نسبة الموافقة على وجود دوافع متوسطة بمتوسط حسابي 2.478 و انحراف معياري 0.648 و كانت الاجابة على كل عبارة كالتالي :

- **درجة الموافقة المتوسطة**

شملت العبارة " **التهديدات التي تتعرض لها المؤسسة غير متعمدة** " بمتوسط حسابي 3.20 و انحراف معياري 0.648 و هذه الأرقام تبين نسبة تشتت قليلة في الاجابات و بهذا يكون الدافع الذي احتل المرتبة الأولى في مجموع الدوافع هو عدم التعمد بمعنى التهديدات الحاصلة هي أخطاء خصوصا الناتجة من قبل أفراد من داخل المؤسسة و لكن التأكد من أنها غير متعمدة يبقى أمرا صعبا.

- **درجة الموافقة المنخفضة**

شملت العبارة " **التهديدات التي تتعرض لها المؤسسة هي بدافع المنافسة** " و العبارة " **التهديدات التي تتعرض لها المؤسسة هي بدافع الحصول على المال** " و العبارة " **التهديدات التي تتعرض لها المؤسسة هي بدافع الانتقام** " بمتوسطات حسابية 2.314 ، 2.228 ، 2.171 و انحرافات معيارية 1.105 ، 1.285 ، 1.150 على التوالي ما يعني أن نسبة قليلة جدا من المؤسسات الجزائرية تعرضت للتهديد بسبب المنافسة أو المال أو الانتقام ، إذ نجد أن المؤسسات التي توافق على التهديد من أجل المال هي إما بنوك أو تأمينات ، و المؤسسات التي تتعرض للتهديد بسبب المنافسة أغلبها مؤسسات الاتصالات أما الانتقام فليس دافعا معتبرا للهجوم على مستوى المؤسسات الجزائرية.

الفرع الثالث : طبيعة الحماية المطبقة في المؤسسة الجزائرية (المتغير المستقل 2)

1- الحماية المادية لنظم معلومات المؤسسة

الجدول (4.15) : الحماية المادية لنظم معلومات المؤسسة الجزائرية

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
30	المؤسسة تعتمد على كاميرات المراقبة لحماية الموقع و التجهيزات	3.714	1.226	عالية	1
31	المؤسسة تعتمد على مراقبة الدخول عن طريق حمل الشارات و مرافقة الزوار لمنع أي تجاوزات	2.914	1.442	متوسطة	3
32	المؤسسة تعتمد على كاشف الحريق و الاطفاء الآلي لحماية موقعها	3.20	1.430	متوسطة	2
33	المؤسسة تعتمد على أجهزة الانذار عند أي تدخل غير مسموح	2.457	1.462	منخفضة	4
	المجموع	**3.071**	**1.237**	**متوسطة**	

يمثل الجدول (4.15) طبيعة الحماية المادية التي تطبقها المؤسسة الجزائرية ، و من خلال الدرجة الكلية تبين أن المؤسسة الجزائرية تطبق الحماية المادية لحماية نظم معلوماتها بدرجة متوسطة بمتوسط حسابي قدره 3.071 و انحراف معياري 1.237 و سيتم ترتيب العبارات حسب درجة الموافقة :

- **درجة الموافقة العالية** :

تمثلت في العبارة " **المؤسسة تعتمد على كاميرات المراقبة لحماية الموقع و التجهيزات** " بمتوسط حسابي 3.714 و انحراف معياري 1.226 و هذا يعني أن أغلب المؤسسات الجزائرية تعتمد على كاميرات المراقبة لحماية موقعها من أي دخول غير مصرح.

- **درجة الموافقة المتوسطة** :

- العبارة " **المؤسسة تعتمد على كاشف الحريق و الاطفاء الآلي لحماية موقعها** " جاءت في المرتبة الثانية بمتوسط حسابي 3.20 و انحراف معياري 1.430 و يعني ذلك أن نسبة متوسطة من المؤسسات الجزائرية من تحوي كاشف الحريق و جهاز الاطفاء لديها.

- تليها العبارة " **المؤسسة تعتمد على مراقبة الدخول عن طريق حمل الشارات و مرافقة الزوار لمنع أي تجاوزات** " بمتوسط حسابي 2.914 و انحراف معياري 1.442 بمعنى أن نسبة متوسطة من المؤسسات الجزائرية من تقوم بمراقبة الدخول إلى المؤسسة و مرافقة الزوار إلى المكان المحدد و هذا يُفسَّر بنقص يقظة عند العمال و الذي مثل في المحور السابق تهديد كبير للمؤسسة الجزائرية.

- **درجة الموافقة المنخفضة** :

تمثلت في العبارة " **المؤسسة تعتمد على أجهزة الانذار عند أي تدخل غير مسموح لحماية موقعها** " بمتوسط حسابي 2.457 و انحراف معياري 1.462 ما يعني أن نسبة قليلة جدا من المؤسسات التي تعتمد على أجهزة الانذار عند حصول أي تعدي على موقعها.

2- الحماية البرمجية لنظم معلومات المؤسسة

الجدول (4.16) : الحماية البرمجية لنظم معلومات المؤسسة الجزائرية

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
34	المؤسسة تعتمد على مضادات الفيروس لحماية أنظمتها المعلوماتية	4.40	0.774	عالية جدا	1
35	المؤسسة تعتمد على الجدران النارية لحماية أنظمتها المعلوماتية	3.857	1.115	عالية	2
36	المؤسسة تعتمد على برامج لتشفير كل البيانات و الاتصالات و التطبيقات المتنقلة و المخزنة لحمايتها من التصنت	2.628	1.516	متوسطة	7
37	المؤسسة تعتمد على أنظمة كشف التدخل لحماية أنظمتها المعلوماتية من أي دخول غير مصرح	2.685	1.529	متوسطة	6
38	المؤسسة تعمل على تحديث برامج الحماية دوريا	3.228	1.476	متوسطة	3
39	المؤسسة تقوم باختبار أنظمة الحماية دوريا لاكتشاف الثغرات	3.057	1.433	متوسطة	4
40	تتم معالجة الثغرات المكتشفة فورا	2.971	1.524	متوسطة	5
	المجموع	**3.261**	**1.118**	**متوسطة**	

يمثل الجدول (4.16) طبيعة الحماية البرمجية التي تطبقها المؤسسات الجزائرية و التي تمثلت في درجة متوسطة بمتوسط حسابي 3.261 و انحراف معياري 1.524 ما يعني أن نسبة متوسطة من المؤسسات الجزائرية من تطبق أنواع الحماية البرمجية المذكورة ، و سيتم ترتيب العبارات حسب درجة الموافقة :

- **درجة الموافقة العالية جدا** :

تمثلت في العبارة " **المؤسسة تعتمد على مضادات الفيروس لحماية أنظمتها المعلوماتية** " بمتوسط حسابي 4.40 و انحراف معياري 0.774 و هذا دليل على أن الغالبية العظمى من المؤسسات الجزائرية تعتمد على مضادات الفيروس لحماية أنظمتها المعلوماتية.

- **درجة الموافقة العالية :**

تمثلت في العبارة " المؤسسة **تعتمد على الجدران النارية لحماية أنظمتها المعلوماتية** " بمتوسط حسابي 3.857 و انحراف معياري 1.115 و هذا يعني أن نسبة عالية من المؤسسات الجزائرية تعتمد على الجدران النارية لحماية أنظمتها المعلوماتية ، و تأتي في المرتبة الثانية بعد مضادات الفيروس.

- **درجة الموافقة المتوسطة :**

- العبارة " **المؤسسة تعمل على تحديث برامج الحماية دوريا** " جاءت في المرتبة الثالثة بمتوسط حسابي 3.228 و انحراف معياري 1.476 ما يعني أن نسبة المؤسسات التي تستعمل برامج الحماية كمضادات الفيروس و الجدران النارية نسبة عالية لكن نسبة متوسطة فقط من من تقوم بعملية التحديث و هذا مؤشر خطير حول مستوى الحماية فمجرد تركيب برنامج حماية دون تحديث دوري أمر غير فعال في حماية أنظمة المعلومات.

- العبارة " **المؤسسة تقوم باختبار أنظمة الحماية دوريا لاكتشاف الثغرات** " و العبارة " **تتم معالجة الثغرات المكتشفة فورا** " جاءتا في المرتبة الرابعة و الخامسة بمتوسط حسابي 3.057 ، 2.971 و انحراف معياري 1.433 ، 1.524 على التوالي ، ما يعني أن نسبة متوسطة من المؤسسات الجزائرية تقوم باختبار أنظمة الحماية دوريا لاكتشاف الثغرات ، لكن نسبة من يعالج هذه الثغرات فور اكتشافها هي نسبة أقل.

- العبارة " **المؤسسة تعتمد على أنظمة كشف التدخل لحماية أنظمتها المعلوماتية من أي دخول غير مصرح** " جاءت في المرتبة السادسة بمتوسط حسابي 2.685 و انحراف معياري 1.529 تليها العبارة " **المؤسسة تعتمد على برامج لتشفير كل البيانات و الاتصالات و التطبيقات المتنقلة و المخزنة لحمايتها من التصنت** " في المرتبة السابعة بمتوسط حسابي 2.628 و انحراف معياري 1.516 ، و عليه فان برامج التشفير و كشف التدخل هي آخر ما قد تعتمد عليه المؤسسة الجزائرية في حماية أنظمتها اذ أن نسبة قليلة منها من تقوم بذلك ، و هذا ما يجعل المؤسسة الجزائرية متأخرة في مجال أمن المعلومات ، فبرامج مكافحة الفيروس غير كافية أبدا في حماية المعلومات و الأنظمة ما لم تدعم ببرامج و أنظمة أخرى تعزز من فاعليتها.

3- تصنيف الموارد الحرجة للمؤسسة

الجدول : (4.17) : تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة الجزائرية

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
41	الموارد الحرجة و الحساسة للمؤسسة معرّفة	2.828	1.562	متوسطة	4
42	المؤسسة تصنف المعلومات السرية و الموارد الحرجة لديها حسب أهميتها و درجة الخطورة التي قد تتعرض لها	3.257	1.400	متوسطة	3
43	المعلومات الحساسة في المؤسسة يتم الاحتفاظ بها الكترونيا	3.685	1.105	عالية	1
44	فريق الأمن يعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث	3.657	1.349	عالية	2
المجموع		**3.357**	**1.116**	**متوسطة**	

يمثل الجدول (4.17) نسبة المؤسسات الجزائرية التي تعمل على تصنيف مواردها الحرجة و معلوماتها الحساسة من أجل الحذر في التعامل معها و كانت درجة الموافقة على ذلك متوسطة بمتوسط حسابي 3.357 و انحراف معياري 1.116 و عليه فان نسبة متوسطة من المؤسسات الجزائرية من تقوم باعطاء أهمية لهذا الموضوع ، و كانت الاجابات على العبارات كالتالي :

- **درجة الموافقة العالية** :

- العبارة " **المعلومات الحساسة في المؤسسة يتم الاحتفاظ بها الكترونيا** " جاءت في المرتبة الأولى بمتوسط حسابي 3.685 و انحراف معياري 1.105 ما يعني أن نسبة عالية من المؤسسات الجزائرية تحتفظ بمعلوماتها الحساسة الكترونيا.

- العبارة " **فريق الأمن يعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث** " جاءت في المرتبة الثانية بمتوسط حسابي 3.657 و انحراف معياري 1.349 ما يعني أن نسبة عالية من المؤسسات الجزائرية تعتمد طرق النسخ الاحتياطية و الرجوع اليها في حالة الكوارث و هذا مؤشر جيد عن يقظة المسؤولين لذلك.

درجة الموافقة المتوسطة

- العبارة " **المؤسسة تصنف المعلومات السرية و الموارد الحرجة لديها حسب أهميتها و درجة الخطورة التي قد تتعرض لها** " جاءت في المرتبة الثالثة بمتوسط حسابي 3.257 و انحراف معياري 1.400 تتبعها العبارة " **الموارد الحرجة و الحساسة للمؤسسة معرّفة** " بمتوسط حسابي 2.828 و انحراف معياري 1.562 ، و هذا يعني أن نسبة متوسطة من المؤسسات الجزائرية من تعرف الموارد الحرجة و المعلومات الحساسة لديها و ترتبها حسب أهميتها و درجة الخطورة التي قد تتعرض لها.

4- عملية تسيير المخاطر

الجدول (4.18) : عملية تسير المخاطر في المؤسسة الجزائرية

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الترتيب
45	فريق الأمن يدرس التهديدات التي قد يتعرض لها أي مورد	3.114	1.586	متوسطة	2
46	فريق الأمن بقيم احتمال تعرض الموارد الحرجة للخطر	2.942	1.570	متوسطة	5
47	فريق الأمن المعلوماتي يدرس درجة خطورة التهديد الذي تتعرض له الموارد الحرجة	3.085	1.541	متوسطة	3
48	فريق الأمن يحدد مستوى الخطر المقبول	2.971	1.543	متوسطة	4
49	فريق الأمن يعتمد طرق دولية لتحليل و تقييم المخاطر	2.228	1.681	منخفضة	6
50	المؤسسة لديها مخططات لاستئناف العمل بعد حدوث أي طارئ	3.20	1.676	متوسطة	1
	المجموع	**2.923**	**1.482**	**متوسطة**	

يبين الجدول (4.18) عملية تسيير المخاطر على مستوى المؤسسة الجزائرية حيث درجة الموافقة على هذا العنصر متوسطة بمتوسط حسابي 2.923 و انحراف معياري 1.482 و هي نسبة قليلة حتى و إن كانت الدرجة متوسطة فهي قريبة من الانخفاض و عليه نقول أن نسبة قليلة من المؤسسات الجزائرية من تقوم بعملية تسيير المخاطر التي تتعرض لها على أسس صحيحة و متينة و سيتم عرض الاجابات عن العبارات المتعلقة بهذا الجانب كالتالي :

- **درجة الموافقة المتوسطة**

- جاءت العبارة " **المؤسسة لديها مخططات لاستئناف العمل بعد حدوث أي طارئ** " في المرتبة الأولى بمتوسط حسابي 3.20 و انحراف معياري 1.676 و عليه فان نسبة متوسطة من المؤسسات الجزائرية من تمتلك مخططات لاستئناف العمل بعد حدوث أي طارئ.

- جاءت العبارة " **فريق الأمن يدرس التهديدات التي قد يتعرض لها أي مورد** " في المرتبة الثانية بمتوسط حسابي 3.114 و انحراف معياري 1.586 تتبعها العبارة " **فريق الأمن المعلوماتي يدرس درجة خطورة التهديد الذي تتعرض له الموارد الحرجة** " بمتوسط حسابي 3.085 و انحراف معياري 1.541 و عليه فان نسبة متوسطة من المؤسسات الجزائرية من تمتلك فريق أمن أو مسؤول أمن يقوم بدراسة التهديدات التي قد تتعرض لها موارد المؤسسة خصوصا الحرجة منها و دراسة درج خطورة هذا التهديد و هنا تكمن أهمية تصنيف الموارد الحرجة ، و أغلب المؤسسات التي تقوم بهذه الدراسات تكون مؤسسات خدمية أو مالية.

– جاءت العبارة " **فريق الأمن يحدد مستوى الخطر المقبول** " و العبارة " **فريق الأمن يقيم احتمال تعرض الموارد الحرجة للخطر** " في المرتبتين الرابعة و الخامسة بمتوسط حسابي 2.971 ، 2.942 و انحراف معياري 1.543 ، 1.570 على التوالي و هي نسب أقل من سابقاتها و عليه فان نسبة متوسطة قريبة من منخفضة من المؤسسات الجزائرية من تقوم ب دراسة احتمالات التعرض للخطر و تحديد مستوى الخطر المقبول الذي لا يجب تجاوزه ، فأغلب المؤسسات الجزائرية تتعامل مع الخطر بعد وقوعه و لا تقوم بدراسة الاحتمالات الممكنة و تحضير السيناريوهات المناسبة لكل احتمال.

– **درجة الموافقة المنخفضة**

تمثلت في العبارة " **فريق الأمن يعتمد طرق دولية لتحليل و تقييم المخاطر** " بمتوسط حسابي 2.228 و انحراف معياري 1.681 ما يعني أن نسبة منخفضة من المؤسسات الجزائرية من تعتمد طرق دولية لتحليل و تقييم المخاطر مثل ايزو 27001.

المطلب الرابع : اختبار الفرضيات

لاختبار فرضيات الدراسة اعتمدنا على معامل الارتباط بين المتغيرات Pearson و تحليل الانحدار البسيط و المتعدد و معامل التباين ANOVA

الفرع الأول : اختبار الفرضية الأولى : تؤثر طبيعة التهديدات على مستوى أمن المعلومات في المؤسسات

H_{01} :لا تؤثر طبيعة التهديدات على مستوى أمن المعلومات في المؤسسات الجزائرية

H_{a1} : تؤثر طبيعة التهديدات على مستوى أمن المعلومات في المؤسسات الجزائرية

1- معامل الارتباط Pearson

الجدول (4.19) : مصفوفة الارتباط بين طبيعة التهديدات و مستوى أمن المعلومات

		طبيعة التهديدات التي تتعرض لها المؤسسة	مستوى أمن المعلومات في المؤسسة
طبيعة التهديدات التي تتعرض لها المؤسسة	Pearson	1	- 0.080
	مستوى المعنوية		0.647
	العدد	35	35
مستوى أمن المعلومات في المؤسسة	Pearson	-0.080	1
	مستوى المعنوية	0.647	
	العدد	35	35

من خلال الجدول (4.19) يتضح أن قيمة معامل **Pearson** بلغت (-0.080) و هي قيمة قريبة من الصفر ما يدل على عدم وجود ارتباط بين طبيعة التهديدات و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم قبول الفرضية العدمية " **لا تؤثر طبيعة التهديد على مستوى أمن المعلومات في المؤسسة الجزائرية** "، و عليه لا يوجد علاقة بين التهديدات التي تتعرض لها المؤسسة و أنظمتها و بين مستوى أمن المعلومات أي أن مستوى الأمن في المؤسسات الجزائرية محل الدراسة لا يتأثر بالتهديدات التي يتعرض لها.

2- معامل التحديد

الجدول (4.20) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالتهديدات

الأبعاد	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
الدرجة الكلية	0.080[a]	0.006	-0.24	1.363

3- تحليل التباين ANOVA

الجدول (4.21) : تحليل التباين ANOVA للمتغير المستقل 1

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	قيمة Sig
الانحدار	0.398	1	0.398	0.214	0.647[a]
الخطأ	61.367	33	1.860		
الاجمالي	61.765	34			

من خلال تحليل الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 0.6 % من خلال طبيعة التهديدات التي تتعرض لها المؤسسة و هي نسبة ضئيلة لا يمكن اعتمادها ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و طبيعة التهديدات ليست علاقة معنوية ذات دلالة احصائية ، و عليه يتم قبول الفرضية العدمية " **لا تؤثر طبيعة التهديد على مستوى أمن المعلومات في المؤسسة الجزائرية** " . و قد كانت نتائج الفرضيات الفرعية كالتالي:

- **الفرضية الفرعية الأولى** : تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية

$\mathbf{H_{01.1}}$: " لا تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية "

$\mathbf{H_{a1.1}}$: " تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية "

الجدول (4.22) : مصفوفة الارتباط بين التهديدات المادية و مستوى الأمن في المؤسسات الجزائرية

البعد	المتغيرات	مستوى أمن المعلومات
التهديدات المادية	معامل الارتباط بيرسون	0.283-
	المعنوية	0.100
	الدلالة	غير معنوي

من خلال الجدول (4.22) يتضح أن قيمة معامل الارتباط بيرسون بلغت – 0.238 و هي غير دالة احصائيا عند مستوى معنوية (0.05) و لذلك نقبل بالفرضية العدمية " **لا تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية** " و هذه النتيجة تؤكد أن مستوى الأمن في المؤسسات الجزائرية محل الدراسة لا يتأثر بطبيعة التهديدات المادية التي تتعرض لها.

الجدول (4.23) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالتهديدات المادية

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
التهديدات المادية	0.283[a]	0.080	0.052	1.312

من خلال نتائج نموذج الانحدار فان مستوى الأمن في المؤسسات الجزائرية يتأثر و يفسر بنسبة 8 % من خلال التهديدات المادية التي تتعرض لها المؤسسة و هي قوة تفسيرية ضعيفة ما يدفعنا لقبول الفرضية العدمية " **لا تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية** "

- **الفرضية الفرعية الثانية :** تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية

$\mathbf{H_{01.2}}$: "لا تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية "

$\mathbf{H_{a1.2}}$:" تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية "

الجدول (4.24) : مصفوفة الارتباط بين التهديدات البرمجية و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
التهديدات البرمجية	معامل الارتباط بيرسون	0.067
	المعنوية	0.702
	الدلالة	غير معنوي

من خلال الجدول (4.24) يتضح أن قيمة معامل الارتباط بيرسون بلغت 0.067 و هي غير دالة احصائيا عند مستوى معنوية (0.05) و لذلك نقبل بالفرضية العدمية " **لا تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية** " و هذه النتيجة تؤكد أن مستوى الأمن في المؤسسات الجزائرية محل الدراسة لا يتأثر بطبيعة التهديدات البرمجية التي تتعرض لها أنظمة المعلومات.

الجدول (4.25) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالتهديدات البرمجية

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
التهديدات البرمجية	0.067^{a}	0.004	0.026-	1.365

من خلال نتائج نموذج الانحدار فان مستوى الأمن في المؤسسات الجزائرية يتأثر و يفسر بنسبة 0.4 % من خلال التهديدات البرمجية التي تتعرض لها المؤسسة و هي قوة تفسيرية جد ضعيفة ما يدفعنا لقبول الفرضية العدمية " **لا تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية** "

- **الفرضية الفرعية الثالثة :** تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية

$\mathbf{H_{01.3}}$: " لا تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية "

$\mathbf{H_{a1.3}}$: " تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية "

الجدول (4.26) : مصفوفة الارتباط بين التهديدات التنظيمية و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
التهديدات التنظيمية	معامل الارتباط بيرسون	-0.479**
	المعنوية	0.004
	الدلالة	معنوي

** الارتباط معنوي عند مستوى الدلالة 0.01

من خلال الجدول (4.26) يتضح أن قيمة معامل الارتباط بيرسون بلغت - 0.479 و هي دالة احصائيا عند مستوى معنوية (0.01) و لذلك نرفض الفرضية العدمية و نقبل بالفرضية البديلة " **تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية** " و هذه النتيجة تؤكد أن مستوى الأمن في المؤسسات الجزائرية محل الدراسة يتأثر بطبيعة التهديدات التنظيمية التي تتعرض لها و لكن بدرجة متوسطة و الاشارة السالبة تدل على الارتباط العكسي أي أن التهديدات التنظيمية تؤثر عكسيا على مستوى أمن المعلومات في المؤسسات الجزائرية.

الجدول (4.27) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالتهديدات التنظيمية

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
التهديدات التنظيمية	0.479[a]	0.229	0.206	1.201

من خلال نتائج نموذج الانحدار فان مستوى الأمن في المؤسسات الجزائرية يتأثر و يفسر بنسبة 22.9 % من خلال التهديدات التنظيمية التي تتعرض لها المؤسسة و هذا يدل على أن هناك أثرا معتبرا للتهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية ما يدفعنا لرفض الفرضية العدمية و القبول بالفرضية البديلة " **تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية** "

نتائج الفرضية الرئيسية الأولى و فرضياتها الفرعية:
الفرضية الرئيسية الأولى : تؤثر طبيعة التهديد على مستوى أمن المعلومات في المؤسسة الجزائرية
لا تؤثر طبيعة التهديد على مستوى أمن المعلومات في المؤسسة الجزائرية (يتأثر مستوى الأمن بطبيعة التهديدات في المؤسسات الجزائرية بنسبة (0.6 %) - **الفرضية الفرعية الأولى** : لا تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية (بنسبة 8 %) - **الفرضية الفرعية الثانية** : لا تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية. (بنسبة 0.4 %) - **الفرضية الفرعية الثالثة** : تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية (بنسبة 22.9 %)

الفرع الثاني : اختبار الفرضية الرئيسية الثانية : تؤثر طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية

H_{02} : لا تؤثر طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

H_{a2} : تؤثر طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

1- معامل الارتباط Pearson

الجدول (4.28) : مصفوفة الارتباط بين طبيعة الحماية المطبقة و مستوى أمن المعلومات

		طبيعة الحماية التي تطبقها المؤسسة	مستوى أمن المعلومات في المؤسسة
طبيعة الحماية التي تطبقها المؤسسة	Pearson	1	0.855**
	مستوى المعنوية		0.000
	العدد	35	35
مستوى أمن المعلومات في المؤسسة	Pearson	0.855**	1
	مستوى المعنوية	0.000	
	العدد	35	35

(**) الارتباط معنوي عند مستوى معنوية 0.01%

من خلال الجدول (4.28) يتضح أن قيمة معامل **Pearson** بلغت (0.855) ما يدل على وجود علاقة ارتباط ذات دلالة احصائية بين طبيعة الحماية المطبقة و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم رفض الفرضية العدمية ، و قبول الفرضية البديلة " **تؤثر طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية**".

2- معامل التحديد

الجدول (4.29) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بطبيعة الحماية المطبقة

الأبعاد	معامل الارتباط R	معامل التحديد R-deux	معامل التحديد المعدل R-deux ajusté	الخطأ المعياري المقدر
1	0.855[a]	0.731	0.723	0.709

3- تحليل التباين ANOVA

الجدول (4.30) : تحليل التباين ANOVA للمتغير المستقل 2

مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة D	قيمة Sig
الانحدار	45.140	1	45.140	89.601	0.000[a]
الخطأ	16.625	33	0.504		
الاجمالي	61.765	34			

من خلال نموذج الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 73.1 % من خلال طبيعة الحماية المطبقة من طرف المؤسسة ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و طبيعة الحماية المطبقة علاقة معنوية ذات دلالة احصائية ، و عليه يتم رفض الفرضية العدمية و قبول الفرضية البديلة " **تؤثر طبيعة الحماية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة** " .

اختبار الفرضيات الفرعية

- **الفرضية الفرعية الأولى** : تؤثر طبيعة الحماية المادية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية

$H_{02.1}$: لا تؤثر طبيعة الحماية المادية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{a2.1}$: تؤثر طبيعة الحماية المادية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

الجدول (4.31) : مصفوفة الارتباط بين الحماية المادية المطبقة و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
الحماية المادية	معامل الارتباط بيرسون	0.615**
	المعنوية	0.000
	الدلالة	معنوي

** الارتباط معنوي عند مستوى الدلالة 0.01

من خلال الجدول (4.31) يتضح أن قيمة معامل **Pearson** بلغت (0.615) ما يدل على وجود علاقة ارتباط ذات دلالة احصائية بين الحماية المادية المطبقة و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم رفض الفرضية العدمية ، و قبول الفرضية البديلة " **تؤثر طبيعة الحماية المادية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية"**

الجدول (4.32) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالحماية المادية المطبقة

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
الحماية المادية	0.615[a]	0.378	0.359	1.079

من خلال جدول نموذج الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 37.8 % من خلال طبيعة الحماية المادية المطبقة من طرف المؤسسة و هي قوة تفسيرية هامة ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و الحماية المادية المطبقة علاقة معنوية ذات دلالة احصائية ، و عليه يتم رفض الفرضية العدمية و قبول الفرضية البديلة " **تؤثر طبيعة الحماية المادية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة** " .

- **الفرضية الفرعية الثانية :** تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{02.2}$: لا تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{a2.2}$: تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائريةٍ.

الجدول (4.33) : مصفوفة الارتباط بين الحماية البرمجية المطبقة و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
الحماية البرمجية	معامل الارتباط بيرسون	0.815**
	المعنوية	0.000
	الدلالة	معنوي

**الارتباط معنوي عند مستوى دلالة 0.01

من خلال الجدول (4.33) يتضح أن قيمة معامل **Pearson** بلغت (0.815) ما يدل على وجود علاقة ارتباط قوية ذات دلالة احصائية بين الحماية البرمجية المطبقة و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم رفض الفرضية العدمية ، و قبول الفرضية البديلة " **تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسة"**

الجدول (4.34) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بالحماية البرمجية المطبقة

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
الحماية البرمجية	0.815[a]	0.664	0.654	0.792

من خلال جدول نموذج الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 66.4 % من خلال طبيعة الحماية البرمجية المطبقة من طرف المؤسسة و هي قوة تفسيرية مرتفعة ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و الحماية البرمجية المطبقة علاقة معنوية ذات دلالة احصائية ، و عليه يتم رفض الفرضية العدمية و قبول الفرضية البديلة " **تؤثر طبيعة الحماية البرمجية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة "**

- **الفرضية الفرعية الثالثة** : تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{02.3}$: لا تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{a2.3}$: تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.

الجدول (4.35) : مصفوفة الارتباط بين تصنيف الموارد الحرجة للمؤسسة و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
تصنيف الموارد الحرجة	معامل الارتباط بيرسون	0.832**
	المعنوية	0.000
	الدلالة	معنوي

** الارتباط معنوي عند مستوى دلالة 0.01

من خلال الجدول (4.35) يتضح أن قيمة معامل **Pearson** بلغت (0.832) ما يدل على وجود علاقة ارتباط قوية ذات دلالة احصائية بين عملية تصنيف الموارد الحرجة و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم رفض الفرضية العدمية ، و قبول الفرضية البديلة " **تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسة "**

الجدول (4.36) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بعملية تصنيف الموارد الحرجة

النموذج	معامل الارتباط	معامل التحديد	معامل التحديد المعدل	الخطأ المعياري المقدر
تصنيف الموارد الحرجة	0.832[a]	0.692	0.683	0.759

من خلال نموذج الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 69.2 % من خلال عملية تصنيف الموارد الحرجة للمؤسسة و هي قوة تفسيرية مرتفعة ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و عملية تصنيف الموارد الحرجة علاقة معنوية ذات دلالة احصائية ، و عليه يتم رفض الفرضية العدمية

و قبول الفرضية البديلة " **تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية** "

- **الفرضية الفرعية الرابعة** : تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{02.4}$:لا تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية.

$H_{02.4}$: تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية.

الجدول (4.37) : مصفوفة الارتباط بين عملية تسيير المخاطر و مستوى أمن المعلومات

البعد	المتغيرات	مستوى أمن المعلومات
عملية تسيير المخاطر	معامل الارتباط بيرسون	0.830**
	المعنوية	0.000
	الدلالة	معنوي

** الارتباط معنوي عند مستوى دلالة 0.01

من خلال الجدول (4.37) يتضح أن قيمة معامل **Pearson** بلغت (0.830) ما يدل على وجود علاقة ارتباط قوية ذات دلالة احصائية بين عملية تسيير المخاطر و مستوى الأمن في المؤسسات محل الدراسة ، و بذلك تم رفض الفرضية العدمية ، و قبول الفرضية البديلة " **تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية** "

الجدول (4.38) : نموذج الانحدار لاختبار مدى تأثر مستوى الأمن بعملية تسيير المخاطر

النموذج	معامل الارتباط	معامل الانحدار	معامل الانحدار المعدل	الخطأ المعياري المقدر
عملية تسيير المخاطر	0.830[a]	0.689	0.680	0.762

من خلال نموذج الانحدار نلاحظ أن مستوى الأمن يُفسَّر بحوالي 68.9 % من خلال عملية تسيير المخاطر و هي قوة تفسيرية مرتفعة ، و من خلال تحليل التباين ANOVA نجد أن العلاقة الانحدارية بين مستوى أمن المعلومات و عملية تسيير المخاطر علاقة معنوية ذات دلالة احصائية ، و عليه يتم رفض الفرضية العدمية و قبول الفرضية البديلة " **تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية** "

نتائج الفرضية الرئيسية الثانية و فرضياتها الفرعية:

الفرضية الرئيسية الثانية

تؤثر طبيعة الحماية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة بنسبة (73.1 %)

- **الفرضية الفرعية الأولى** : تؤثر طبيعة الحماية المادية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة (بنسبة 37.8 %)
- **الفرضية الفرعية الثانية** : تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسة. (بنسبة 66.4 %)
- **الفرضية الفرعية الثالثة** : تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسة (بنسبة 69.2 %)
- **الفرضية الفرعية الرابعة** : تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسة (بنسبة 68.9 %)

- **معاملات الانحدار المتعدد**

تحليل الانحدار المتعدد لتحديد أكثر الأبعاد و المتغيرات المستقلة تأثيرا على المتغير التابع.

1- نتائج تحليل الانحدار المتعدد لاختبار أثر أبعاد طبيعة التهديدات (المتغير المستقل 1) على مستوى أمن المعلومات (المتغير التابع)

الجدول (4.39) : نتائج تحليل الانحدار المتعدد لاختبار أثر أبعاد التهديدات على مستوى أمن المعلومات

Sig	T	Béta	Erreur standard	B	النموذج
0.000	5.356		1.044	5.590	الثابت
0.560	0.589-	0.100-	0.271	0.159-	تهديدات مادية
0.397	0.858	0.139	0.205	0.176	تهديدات برمجية
0.009	2.774-	0.471-	0.271	-0.752	تهديدات تنظيمية

من خلال الجدول أعلاه يتضح لنا أن ليس كل المتغيرات لها درجة تأثير و دالة احصائيا إذ بلغت قيمة معامل Béta لبعد التهديدات المادية (-0.100) و لبعد التهديدات البرمجية (0.139) و هي غير دالة احصائيا عند مستوى الدلالة (0.05) حيث أن مستوى دلالة الاختبار للبعد الأول بلغت (0.560)و البعد الثاني (0.397)و هي أكبر من مستوى المعنوية (0.05) ، في حين أن متغير التهديدات التنظيمية له تأثير و دال احصائيا إذ بلغت قيمة معامل Béta (-0.471) و هي دالة احصائيا عند مستوى الدلالة (0.05) حيث أن مستوى دلالة الاختبار بلغت (0.009) و هي أقل من مستوى المعنوية (0.05) و بالتالي فان التهديدات التنظيمية هي أكثر المتغيرات تأثيرا على مستوى أمن المعلومات في المؤسسة الجزائرية ، و نقصد بها سوء التسيير ، نقص الكفاءات ، ثغرات الأنظمة و هذا أمر منطقي فالتهديدات التنظيمية الداخلية هي أخطر من التهديدات البرمجية و المادية الخارجية.

و عليه يمكن كتابة نموذج الانحدار المتعدد كما يلي :

مستوى أمن المعلومات = 5.590 + (0.752–) * تهديدات تنظيمية

Y= –0.752 MG+5.590

Y : المتغير التابع (مستوى أمن المعلومات)

MG: المتغير المستقل (التهديدات التنظيمية)

نستنتج من هذا النموذج أن التهديدات التنظيمية هي أكثر التهديدات تأثيرا على مستوى أمن المعلومات في المؤسسات الجزائرية محل الدراسة فكلما انخفض مستوى هذه التهديدات ارتفع مستوى أمن المعلومات بمعنى العلاقة بين المتغير التابع و المستقل هي علاقة عكسية

2– نتائج تحليل الانحدار المتعدد لاختبار أثر أبعاد الحماية (المتغير المستقل 2)على مستوى أمن المعلومات (المتغير التابع)

الجدول (4.40) : نتائج تحليل الانحدار المتعدد لاختبار أثر أبعاد الحماية على مستوى أمن المعلومات

Sig	T	Béta	Erreur standard	B	النموذج
0.772	0.292–		0.475	0.139–	الثابت
0.829	0.218–	0.029–	0.147	0.032–	حماية مادية
0.118	1.611	0.323	0.242	0.389	حماية برمجية
0.043	2.113	0.388	0.222	0.468	تصنيف الموارد الحرجة
0.296	1.064	0.233	0.199	0.212	عملية تسيير المخاطر

من خلال الجدول نلاحظ أن كل المتغيرات غير دالة احصائيا عند مستوى دلالة 0.05 ما عدا المتغير " تصنيف الموارد الحرجة " الذي بلغ مستوى الدلالة له (0.043) و هي أقل من مستوى المعنوية 0.05 ، و على هذا سنقوم بالاعتماد على تحليل الانحدار المتعدد التدريجي لاستنتاج أفضل نموذج.

– نتائج تحليل الانحدار المتعدد التدريجي:

نتائج تحليل الانحدار المتعدد التدريجي أسفرت عن نموذجين يمكن اعتمادهما

الجدول (4.41) : نتائج تحليل الانحدار المتعدد التدريجي لاختبار أثر أبعاد الحماية المطبقة على مستوى أمن المعلومات

النموذج		B	Erreur standard	Béta	T	Sig
النموذج الأول	الثابت	0.144-	0.412		0.351-	0.728
	تصنيف الموارد الحرجة	1.004	0.117	0.832	8.608	0.000
النموذج الثاني	الثابت	0.424-	0.388	0.323	1.092-	0.283
	تصنيف الموارد الحرجة	0.603	0.178	0.499	3.381	0.002
	الحماية البرمجية	0.499	0.178	0.414	2.803	0.009

من خلال الجدول نلاحظ أنه تم استبعاد متغيرين من تحليل الانحدار المتعدد و هما الحماية المادية و تسيير المخاطر لأنها غير دالة احصائيا عند مستوى المعنوية (0.05) و بين لنا الجدول نموذجين :

النموذج الأول : تم استبعاد فيه 3 متغيرات و اعتماد متغير واحد فقط و هو " تصنيف الموارد الحرجة " لأن مستوى الدلالة فيه (0.000) أقل من 0.05 و نعبر عنه بالمعادلة التالية :

Y=–0.144+1.004*CRC

Y : مستوى أمن المعلومات (المتغير التابع)

CRC : تصنيف الموارد الحرجة (المتغير المستقل)

النموذج الثاني : تم استبعاد متغيرين في هذا النموذج و اعتماد متغيرين و هما " تصنيف الموارد الحرجة " و "الحماية البرمجية " لأن مستوى الدلالة فيهما أقل من 0.05 ، و نعبر عنه بالمعادلة التالية :

Y=–0.424+0.603*CRC+0.499*PL

Y : مستوى أمن المعلومات (المتغير التابع)

CRC : تصنيف الموارد الحرجة (المتغير المستقل)

PL : الحماية البرمجية (المتغير المستقل)

نستنتج من هذا النموذج أن "تصنيف الموارد الحرجة " و " طبيعة الحماية البرمجية " هما أكثر المتغيرات تأثيرا على مستوى أمن المعلومات في المؤسسات الجزائرية محل الدراسة فكلما ارتفع مستوى الحماية البرمجية و تصنيف الموارد الحرجة ارتفع مستوى أمن المعلومات بمعنى العلاقة بين المتغير التابع و المستقل هي علاقة طردية

3- نتائج تحليل الانحدار المتعدد لاختبار أثر طبيعة التهديدات (المتغير المستقل 1) و أثر طبيعة الحماية المطبقة (المتغير المستقل 2) على مستوى أمن المعلومات (المتغير التابع)

الجدول : (4.42) : نتائج تحليل الانحدار المتعدد لاختبار أثر طبيعة التهديدات و أثر طبيعة الحماية المطبقة على مستوى أمن المعلومات

Sig	T	Béta	Erreur standard	B	النموذج
0.137	1.524		0.940	1.432	الثابت
0.125	1.575 -	0.139 -	0.315	0.496 -	طبيعة التهديدات في المؤسسة
0.000	9.808	0.865	0.103	1.014	طبيعة الحماية المطبقة

المتغير التابع : مستوى أمن المعلومات

من خلال الجدول أعلاه يتضح لنا أن ليس كل المتغيرات لها درجة تأثير و دالة احصائيا إذ بلغت قيمة معامل Béta لمتغير التهديدات (-0.139) و هي غير دالة احصائيا عند مستوى الدلالة (0.05) حيث أن مستوى دلالة الاختبار لهذا المتغير (0.125)هي أكبر من مستوى المعنوية (0.05) ، في حين أن متغير الحماية المطبقة له تأثير و دال احصائيا إذ بلغت قيمة معامل Béta (0.856) و هي دالة احصائيا عند مستوى الدلالة (0.05) حيث أن مستوى دلالة الاختبار بلغت (0.000) و هي أقل من مستوى المعنوية (0.05) و بالتالي فان طبيعة الحماية المطبقة هي المتغير الوحيد الذي يؤثر على مستوى أمن المعلومات في المؤسسة الجزائرية ، بمعنى أن مستوى أمن المعلومات في المؤسسات الجزائرية لا يتأثر بطبيعة التهديدات التي يتعرض لها بل بطبيعة الحماية المطبقة فاذا كان مستوى الحماية مرتفع فان مستوى الأمن يكون مرتفع دون الأخذ بعين الاعتبار نوع التهديد.

و عليه يمكن كتابة نموذج الانحدار المتعدد العام كما يلي :

مستوى أمن المعلومات = 1.432 + 1.014 طبيعة الحماية المطبقة
Y=1.432+1.014P

Y : المتغير التابع (مستوى أمن المعلومات)

P: المتغير المستقل (طبيعة الحماية المطبقة)

نستنتج من هذا النموذج أن طبيعة الحماية المطبقة المتغير الأكثر تأثيرا على مستوى أمن المعلومات في المؤسسات الجزائرية محل الدراسة فكلما ارتفع مستوى الحماية المطبقة ارتفع مستوى أمن المعلومات و العكس صحيح ، و هذا ماتبينه نتائج البحث حيث أن مستوى الحماية المطبقة في المؤسسات الجزائرية محل الدراسة متوسط ، و مستوى الأمن في المؤسسات الجزائرية محل الدراسة متوسط كذلك.

خلاصة الفصل

من خلال الدراسة الميدانية على مستوى 35 مؤسسة جزائرية منها الصناعية و منها الخدمية تم التوصل إلى النقاط التالية :

- مستوى أمن المعلومات على مستوى المؤسسات الجزائرية متوسط.
- مستوى أمن المعلومات في المؤسسات الخدمية مرتفع عن المستوى في المؤسسات الصناعية.
- لا يوجد وظيفة مسؤول أمن المعلومات في أغلب المؤسسات الجزائرية.
- أغلب التهديدات التي تتعرض لها المؤسسات الجزائرية هي تهديدات داخلية أكثر منها خارجية.
- التهديدات التي تتعرض لها المؤسسات الجزائرية هي تهديدات تنظيمية بالدرجة الأولى تليها التهديدات البرمجية ثم المادية.
- درجة الموافقة على طبيعة الحماية بكل أنواعها : المادية و البرمجية و تصنيف الموارد الحرجة و تسيير المخاطر كانت متوسطة ما أدى إلى استنتاج و الوصول إلى أن مستوى أمن المعلومات في المؤسسات الجزائرية متوسط.
- تعتمد المؤسسات الجزائرية في حماية أنظمتها المعلوماتية على مضادات الفيروس و جدران الحماية بالدرجة الأولى .
- كانت نتائج الفرضيات كالتالي :

- **لا تؤثر طبيعة التهديد على مستوى أمن المعلومات في المؤسسة الجزائرية (يتأثر مستوى الأمن بطبيعة التهديدات في المؤسسات الجزائرية بنسبة (0.6 %)**
- **تؤثر طبيعة الحماية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات محل الدراسة بنسبة (73.1 %)**

و عليه فان طبيعة الحماية المطبقة المتغير الأكثر تأثيرا على مستوى أمن المعلومات في المؤسسات الجزائرية محل الدراسة فكلما ارتفع مستوى الحماية المطبقة ارتفع مستوى أمن المعلومات و العكس صحيح ، و هذا ماتبينه نتائج البحث حيث أن مستوى الحماية المطبقة في المؤسسات الجزائرية محل الدراسة متوسط ، و مستوى الأمن في المؤسسات الجزائرية محل الدراسة متوسط كذلك.

الخاتمة العامة

الخاتمة

نتائج الدراسة

نتائج اختبار الفرضيات

التوصيات

آفاق الدراسة

❖ الخاتمة :

أمن المعلومات هو مفهوم شامل و عام يحمل تحت طياته العديد من أنواع الحماية نظرا لتعدد و تنوع الأجهزة و الأدوات التي تحمل المعلومات ، و لكن طريقة تطبيقه داخل المؤسسة هو أمر جد معقد ، خصوصا مع ظهور النظريات الاقتصادية التي تنادي بضرورة اشراك العمال في عمليات اتخاذ القرار و اطلاعهم على كل نشاطات المؤسسة لتحقيق نتائج أفضل ، فيحصل التضارب بين أن تتخذ المؤسسة سياسة مفتوحة واضحة المعالم و بين انتهاجها لسياسة متحفظة نوعا ما تحاول فيها حماية ارثها خصوصا المعلوماتي منه ، و هنا تظهر فعالية المؤسسات في التحكم و التسيير الجيد دون التفريط أو الافراط في أي جانب من الجانبين ، و المتخصصين في أمن المعلومات أو كل من يملك رصيد جيد من المعلومات و المهارات في هذا المجال يستطيع حل هذه المعادلة في اشراك العمال و تحسيسهم بجو العمل الجماعي دون افشاء أسرار المؤسسة أو معلوماتها الاستراتيجية.

و جاء هذا البحث لمعالجة موضوع أمن المعلومات من مختلف جوانبه انطلاقا من الاشكالية التالية : **ما هو مستوى أمن المعلومات في المؤسسة الجزائرية ؟و ما مدى تأثره بالتهديدات الواقعة و طبيعة الحماية المطبقة؟** حيث تم التطرق في **الفصل الأول** للجانب النظري للموضوع و التعرف على مفهوم أمن المعلومات و علاقته بالمفاهيم المشابهة له كالأمن الاقتصادي ، أمن نظم المعلومات ، الأمن الالكتروني ....و توصلنا إلى أن أمن المعلومات هو مفهوم أشمل و أعم من الأمن الالكتروني أو المعلوماتي ، حيث يعبر عنه أنه حماية معلومات المؤسسة بأي طريقة و مهما كان نوعها ، سواء الكترونية أو ورقية، أما في **الفصل الثاني** فحاولنا التطرق لمختلف التهديدات و سبل الوقاية منها ، و أشهرها هي التهديدات المعلوماتية التي تكون إما عن طريق البرامج الخبيثة كالفيروسات و القنابل المنطقية و الدودة....أو نتيجة ثغرات في الأنظمة يستطيع المعتدي أن يستغلها لشن هجمات ، و إما عن طريق القرصنة المعلوماتية بمعنى استخدام النظام بطريقة غير شرعية عن طريق التصنت أو الدخول غير المرخص أو انتحال الشخصية .. هذا النوع من التهديدات تواجهه المؤسسة عن طريق تطبيق الحماية البرمجية و التي تتمثل عادة في تحميل أو تركيب برامج مضادة كمضادات الفيروس أو الجدران النارية أو استخدام آليات التشفير و التحقق من الهوية .. ،كما نجد نوع آخر من التهديدات و هو التهديدات المادية المتمثلة عموما في أعمال السرقة و التخريب أو تكون طبيعية كالتعرض لفيضانات أو حرائق تقضي على كل تجهيزات و أنظمة المؤسسة ، و لكن تبقى أصعب التهديدات و أخطرها هي الصادرة من العامل البشري الداخلي ، و التي يصعب اكتشافها و ينتج عنها آثار مدمرة ، إذ لا يمكن منع العمال من التجول و الانتقال داخل المؤسسة ، إلا أنه يمكن

الحد من ذلك بعض الشيء عن طريق انتهاج المؤسسة لإستراتيجية فعالة في تطبيق أمن المعلومات ، و هذا ما تم التطرق إليه في **الفصل الثالث** ، و أول خطوة في ذلك هو إعداد سياسة أمن واضحة تحدد المهام الرئيسية لكل عامل خصوصا موظفي المعلوماتية و منع إفشاء المعلومات التي تحددها المؤسسة على أنها حساسة ، و تنشر كل النقاط الأساسية لسياستها الأمنية بين العمال و تبيان العقوبات المطبقة على كل مخالف ، إضافة إلى التكوين الجيد و التحسيس للعمال و رفع الوعي و الثقافة الأمنية لديهم ، و تدريبهم على طرق حماية ما لديهم من أجهزة و معلومات داخل أو خارج المؤسسة ، و خصص **الفصل الرابع** للجانب التطبيقي ، لاسقاط ما تم دراسته في الجانب النظري على المؤسسات الجزائرية محل الدراسة.

❖ نتائج الدراسة :

نتائج الجانب النظري :

من خلال دراستنا لهذا الموضوع في ثلاث فصول نظرية خلصنا إلى النتائج التالية :

- الأمن الاقتصادي يمثل المفهوم العام لأمن المعلومات على مستوى الدولة ككل ، فعلى مستوى الدولة نقول الأمن الاقتصادي ، و على مستوى المؤسسة نقول أمن المؤسسة و أكثر دقة أمن المعلومات.

– أمن المعلومات هو مصطلح حديث تم تداوله من عدة زوايا و لعل أشمل و أوفر تعريف له هو ما ينظر له من جميع الزوايا :

- فمن زاوية أكاديمية (علمية): هو العلم الذي يبحث في نظريات و استراتيجيات و سياسات توفير الحماية للمعلومات من المخاطر التي تهددها و من مختلف أنشطة الاعتداء التي يمكن أن تتعرض لها.
- من زاوية تقنية (عملية) : فهو مجموعة الوسائل و التدابير و الاجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من البيئة الداخلية أو الخارجية.
- من زاوية قانونية : أمن المعلومات هو محل دراسات و تدابير حماية سرية و سلامة المحتوى و توفر المعلومات و مكافحة أنشطة الاعتداء عليها و استغلال نظمها في ارتكاب الجريمة.

- و على ضوء التعريفات التي تطرقنا لها خلال البحث يمكن القول أن أمن المعلومات هو كل السياسات و الإجراءات المطبقة بهدف حماية المعلومات عن طريق توفير الأمن لكل المكونات المادية من محلات و أجهزة و المكونات التقنية كالبرمجيات و الشبكات و الاتصالات و كل التكنولوجيات المستعملة في تداول المعلومات ،

دون نسيان أهم عنصر و هو العنصر البشري الذي كلما زادت حمايته تطور تعامله مع المعلومات لأن التقنية مهما بلغت مستوياتها لا يمكن أن تحل محل العنصر البشري

- الأمن المعلوماتي أو الأمن الالكتروني ما هو إلا جزء من أمن المعلومات ، فالأول هو حماية المعلومات داخل الوسائل التقنية و الالكترونية ، أما أمن المعلومات فيتعامل مع المعلومات اين ما وجدت ، فبرغم الاعتماد التقني للمؤسسات في التعامل مع المعلومات إلا أنه لا يمكن التغاضي عن الأنظمة التقليدية التي مازالت بعض المؤسسات تعتمدها.
- مصادر التهديدات التي تتعرض لها المؤسسات و الأنظمة هي إما طبيعية (الكوارث) أو بشرية (داخلية أو خارجية) سواء متعمدة أو أخطاء ، و تنفذ من قبل عدة أنواع من الأشخاص فنجد مثلا : المخترقين (الهاكر و الكراكر) ، المحتالين ، المستخدمين الخبيثين ، الجواسيس أو الارهابيين تدفعهم مجموعة من الدوافع و التي تكون إما عامة كالدوافع الاستراتيجية أو الايديولوجية أو المالية أو السياسية أو دوافع شخصية كالانتقام أو التسلية أو اثبات القدرات.
- هناك نوعان من التهديدات ، أولا الناتجة عن اعتداءات كزرع البرامج الضارة (الفيروس ، الدودة ، حصان طراودة ، القنابل المنطقية) ، القرصنة أو الاختراق (التصنت ، سرقة الهوية ، رفض الخدمة ، التزوير و التعديل) و الاعتداء المادي (كالسرقة و التدمير و الهندسة الاجتماعية) ، ثانيا التهديدات الناتجة عن ثغرات أمنية سواء على المستوى المادي أو على المستوى التكنولوجي.
- حماية أنظمة المعلومات من التهديدات يجب أن تكون منظومة متكاملة ، و تنقسم الحماية إلى ثلاث أنواع : الحماية البرمجية (الجدران النارية ، مضادات الفيروس ، التشفير ، مراقبة الدخول ، أنظمة كشف التدخل ، الشبكة الافتراضية ، التحديثات) و الحماية المادية (أمن موقع المنظمة ، أمن تجهيزات نظم المعلومات ، و انتباه العامل البشري لتصرفاته و تحركاته) و أخيرا الحماية القانونية للممتلكات غير المادية و المتمثلة في الحماية الفكرية.
- تطبيق الأمن داخل المؤسسة يتطلب إعداد استراتيجية لأمن المعلومات تهتم فيها المؤسسة بالجانب التنظيمي المتمثل في إعداد السياسة الأمنية مرفقة بكل وثائقها من دستور و قواعد و دلائل مع توزيع المهام و المسؤوليات المتعلقة بالأمن .
- وجود مسؤول عن أمن المعلومات أمر جد مهم في ظل الاستخدام الواسع لأنظمة المعلومات و كثرة التهديدات ، فهو الذي يسير عملية الحفاظ على المعلومات و كيفية تناقلها .

- من الضروري على المؤسسة توفير التكوين لعمال المعلوماتية و كل من يتعامل مع معلومات حساسة أو نظم المعلومات في كيفية التعامل مع هذه الأخير ، و تكثيف حملات و دورات التحسيس لرفع الوعي الأمني.
- لمواجهة التهديدات لا يكفي توفير الحماية البرمجية و المادية و القانونية ، و إنما على المؤسسة إعداد خطة لتسيير المخاطر تبدأ بدراسة النطاق و البنية التحتية و عناصر الخطر ثم تحليل و تقييم هذه المخاطر و من ثم ترتيبها حسب درجة خطورتها و احتمالية تكرارها و أخيرا اختيار طريقة المعالجة المناسبة .
- مخططات استئناف/استمرارية النشاط أدوات جد مهمة في معالجة المخاطر و مواجهة الأزمات و تنقذ المؤسسة من عدة سقطات.
- معيار الايزو 27001 الخاص بأمن نظم المعلومات يعتبر كدليل لأفضل الممارسات في مجال الأمن ، يقدم للمؤسسة خطوات مجربة و فعالة في التطبيق ، و يساعدها في تقييم وضعيتها الأمنية ، خصوصا أنه يطبق عن طريق دورة PDCA الفعالة.

النتائج الخاصة بالجانب التطبيقي :

- غياب مصلحة أو مسؤول أمن المعلومات أو حتى مصلحة نظم المعلومات بأغلب المؤسسات الجزائرية .
- مستوى أمن المعلومات في المؤسسات الجزائرية هو متوسط بصفة عامة .
- مستوى أمن المعلومات في المؤسسات الصناعية مختلف تماما عنه في المؤسسات الخدمية خصوصا المالية كالبنوك و التأمينات و أيضا في شركات الاتصال ، فلو اقتصرت الدراسة على المؤسسات الصناعية فقط لخلصت إلى أن مستوى الأمن في المؤسسات الجزائرية جد متدني ، و لكن ما رفع المستوى بصفة عامة هو دراسة مستوى الأمن في المؤسسات الخدمية التي تعتبر أفضل و أحرص نسبة لسابقتها.
- تطبق المؤسسة الوطنية للأشغال البترولية الكبرى الأمن وفق معايير عالمية.
- لا يتأثر مستوى الأمن في المؤسسات الجزائرية بالتهديدات المادية و البرمجية ، و انما فقط بالتهديدات التنظيمية المتمثلة أساسا في سوء التسيير و نقص الكفاءات في مجال الأمن ، و ترك ثغرات مفتوحة أمام المهددين لاستغلالها، و غياب اليقظة و الوعي و الثقافة الأمنية و هذا أمر منطقي فالتهديدات المادية و البرمجية يمكن مواجهتها بتركيب أحدث البرامج و الآليات ، و لكن ما الجدوى منها إذا غاب حسن التسيير .
- تدني مستوى أمن المعلومات في المؤسسات الجزائرية راجع إلى نقص الكفاءات البشرية و غياب اليقظة.
- يتأثر مستوى الأمن في المؤسسات الجزائرية بطبيعة الحماية المطبقة ، فكلما ارتفع مستوى الحماية سواء المادية أو البرمجية أو تصنيف المعلومات الحساسة أو عملية تسيير المخاطر ارتفع مستوى أمن المعلومات و العكس

صحيح ، و هذا ما يفرض على المؤسسة الجزائرية أن تحرص كل الحرص في اختيار و تطبيق أفضل الطرق لحماية ممتلكاتها المادية و المعلوماتية و رفع الوعي و الثقافة الأمنية.

- أكثر العوامل تأثيرا في مستوى الأمن في المؤسسات الجزائرية هو تصنيف الموارد الحرجة ، فكلما اعتمدت المؤسسة عملية تصنيف جيدة لمعلوماتها الحساسة و طبقت عليها حماية خاصة كلما ارتفع مستوى أمن المعلومات.
- الحماية البرمجية هي أيضا من العوامل المؤثرة على مستوى أمن المعلومات في المؤسسة ، و من أكثر أنواع الحماية البرمجية اعتمادا من طرف المؤسسات برامج مكافحة الفيروسات تليها الجدران النارية.
- عدم اهتمام المؤسسات الجزائرية بأمن المعلومات يعود إلى عدة أسباب أهمها : غياب المنافسة بين المؤسسات الجزائرية خصوصا الصناعية ، غياب الثقافة و الوعي.

❖ نتائج اختبار الفرضيات :

الفرضية الأولى : فيما يخص الفرضية الأولى الخاصة بتأثير طبيعة التهديدات على أمن المعلومات في المؤسسات الجزائرية فقد توصلت الباحثة إلى ما يلي :

- لا تؤثر التهديدات المادية على مستوى أمن المعلومات في المؤسسات الجزائرية.
- لا تؤثر التهديدات البرمجية على مستوى أمن المعلومات في المؤسسات الجزائرية.
- تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية.

و **عليه تم قبول الفرضية الأولى جزئيا ، حيث تم قبولها بالنسبة للتهديدات التنظيمية ، و رفضها بالنسبة للتهديدات المادية و البرمجية ، و عليه يمكن التوصل إلى النتيجة التالية : تؤثر التهديدات التنظيمية على مستوى أمن المعلومات في المؤسسات الجزائرية.**

الفرضية الثانية : فيما يخص الفرضية الثانية الخاصة بتأثير طبيعة الحماية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية فقد توصلت الباحثة إلى ما يلي :

- تؤثر طبيعة الحماية المادية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.
- تؤثر طبيعة الحماية البرمجية المطبقة على مستوى أمن المعلومات في المؤسسات الجزائرية.
- تؤثر عملية تصنيف الموارد الحرجة و المعلومات الحساسة للمؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.
- تؤثر عملية تسيير المخاطر على مستوى أمن المعلومات في المؤسسات الجزائرية.

و عليه تم قبول الفرضية الثانية : تؤثر طبيعة الحماية المطبقة من طرف المؤسسة على مستوى أمن المعلومات في المؤسسات الجزائرية.

❖ **التوصيات** : اعتمادا على نتائج الدراسة يمكن تقديم مجموعة من التوصيات التي قد تساهم في تحسين مستوى أمن المعلومات على مستوى المؤسسات الجزائرية :

- على المؤسسة الجزائرية مواكبة التطورات الحاصلة في البيئة التكنولوجية و تطوير نظم معلوماتها .
- الاهتمام بجانب توفير الأمن لنظم معلومات المؤسسة و كل الموارد الحساسة التي تمتلكها و ذلك بإتباع العديد من الخطوات :
- تغيير الذهنية التقليدية للمسؤولين و العمال التي تعمل بشكل روتيني ، و الانفتاح على التطورات العالمية و مواكبة العصر و ذلك من خلال دورات التحسيس و التوعية لنشر الثقافة الأمنية بحيث يصبح أمن المعلومات ثقافة داخل المؤسسة و ليس مجرد آليات مطبقة ، بعد ذلك يأتي دور التكوين عل استخدام آليات الأمن و كيفية التعامل مع المعلومات الحساسة و تدريب العمال على ذلك.
- اعتماد المؤسسة الجزائرية على سياسات أمنية مكتوبة ، ما يسهل عملية تطبيق أمن المعلومات على مستوى المؤسسة كما يسهل عملية المراقبة و المحاسبة ضد أي تجاوز.
- الاستثمار في الجانب البشري أكثر منه في الجانب المادي ، و اختيار أحسن الكفاءات للتعامل مع أنظمة المعلومات ، و ابتكار طرق تسيير حديثة تتلاءم مع بيئة المؤسسة و البيئة الخارجية في نفس الوقت.
- الاهتمام بالمعايير العالمية الخاصة بأمن المعلومات و أهمها معيار الايزو 27001 الذي يعتبر الدليل و المرشد في هذا المجال.
- الاهتمام بجانب البحث و التطوير، خصوصا في مجال التعامل مع أنظمة المعلومات لأن الأمر حساس، و رفع ميزانيته.
- تهيئة بيئة أنظمة المعلومات من خلال توفير أحدث الأنظمة و برمجيات الحماية ، و تطوير قواعد البيانات و تصميمها بطريقة تسهل الوصول إليها و توفر لها الحماية من أي اعتداء في نفس الوقت ، و هي معادلة صعبة تتطلب جهدا من المؤسسة لتحقيقها.
- تقوية العلاقة بين الجامعة و المؤسسة و اهتمام الادارات العليا للمؤسسات بالنتائج التي تسفر عنها الأبحاث الجامعية و أخذها بعين الاعتبار.
- توفير مراكز لتعليم أساسيات أمن المعلومات و التدريب عليه بشكل عملي.

- ادراج أمن المعلومات كمادة أساسية في المناهج المعتمدة في كليات الاقتصاد و علوم التسيير و حتى في الكليات الأخرى.

❖ **آفاق الدراسة** : من خلال نتائج هذا البحث يمكن اقتراح أبحاث أخرى من أجل تعزيز النتائج المتوصل اليها ، حيث يمكن :

– تطبيق نفس الدراسة بنفس المتغيرات على عينة أخرى من المؤسسات من أجل القدرة على تعميم الدراسة على كل المؤسسات الجزائرية.

–تطبيق نفس الدراسة على عينة من المؤسسات الصناعية و عينة من المؤسسات الخدمية و المقارنة بين مستوى أمن المعلومات في كليهما.

و من العناوين المقترحة :

- دراسة مقارنة بين مستوى أمن المعلومات في المؤسسة الصناعية و بين مستوى أمن المعلومات في المؤسسة الخدمية.
- دراسة مقارنة بين مستوى أمن المعلومات في المؤسسات الجزائرية و بين مستوى أمن المعلومات في المؤسسات الأجنبية أو العربية.

كما يمكن تسليط الضوء على أحد متغيرات الدراسة و من العناوين المقترحة :

- تأثير العامل البشري على مستوى أمن المعلومات في المؤسسة الجزائرية.

المراجع

- **اللغة العربية**

أ- الكتب

1. أبو مغايض يحي بن محمد، **الحكومة الإلكترونية: ثورة على العمل الإداري التقليدي**، مكتبة العبيكان، الرياض، 2004.

2. ادوارد.ب، بورودزيكيس: ترجمة أحمد المغربي، **إدارة المخاطر و الأزمات الأمنية**، دار الفجر للنشر و التوزيع، القاهرة ، 2008.

3. أسامة سمير حسين، **الاحتيال الالكتروني – الأسباب و الحلول** -، الجنادرية للنشر و التوزيع، الطبعة الأولى، 2011.

4. الشدي طارق عبد الله، **آلية البناء الأمني لنظم المعلومات**، دار الوطن للطباعة و النشر و الإعلام، الرياض، 2000.

5. الشعلان فهد أحمد، **إدارة الأزمات: الأسس–المراحل – الآليات**، جامعة نايف العربية للعلوم الأمنية، الرياض، الطبعة 2، 2002.

6. العبود فهد بن ناصر، **الحكومة الإلكترونية بين التخطيط و التنفيذ**، السلسلة الثانية، مكتبة الملك فهد الوطنية الرياض، 2005.

7. القاسم محمد بن عبد الله، **سياسات أمن المعلومات**، سلسلة اصدارات مركز البحوث و الدراسات، كلية الملك فهد الأمنية، الرياض، 2005.

8. ايمان السامرائي، هيثم الزغبي، **نظم المعلومات الإدارية**، دار الصفاء للنشر و التوزيع، عمان، الأردن، الطبعة الاولى، 2004.

9. ثابت عبد الرحيم ادريس ، **نظم المعلومات الادارية في المنظمات المعاصرة** ، دار الجامعة ، الإسكندرية ، دون طبعة ، 2005.

10. حسن مظفر الرزو ، **الفضاء المعلوماتي** ، مركز دراسات الوحدة العربية ، الطبعة الأولى ، بيروت ، 2007.

11. خالد بن سليمان الغثبر ، مهندس محمد بن عبد الله القحطاني ، **أمن المعلومات بلغة ميسرة** ، مكتبة الملك فهد الوطنية ، الرياض ، الطبعة الأولى ، 2009 .

12.: ذيب بن عايض القحطاني ، **أمن المعلومات** ، مدينة الملك عبد العزيز للعلوم و التقنية ، الرياض ، 2015 .

13. زكي حسن الوردي، مجبل لازم المالكي، **المعلومات و المجتمع**، الوراق للنشر و التوزيع، الطبعة الأولى، 2006.

14. سائد أحمد الخولي، **حقوق الملكية الصناعية**، دار مجدلاوي ، عمان ، الطبعة الأولى ، 2004.

15. سعد غالب ياسين،**تحليل و تصميم نظم المعلومات**،دار المناهج للنشر،عمان،الأردن،الطبعة الاولى،2000.

16. سعد غالب ياسين، **أساسيات نظم المعلومات الإدارية و تكنولوجيا المعلومات**،دار المناهج،عمان،2009.

17. سميحة القليوبي ، **الملكية الصناعية** ، دار النهضة العربية للطبع و النشر و التوزيع ، القاهرة ، 2005

18. عامر قندلجي و آخرون ، **مصادر المعلومات التقليدية و الإلكترونية** ، دار اليازوري العلمية، عمان، 2009

19. عبد الرحمن الصباح ، عماد الصباغ ، **مبادئ نظم المعلومات الإدارية الحاسوبية** ، دار زهران للنشر و التوزيع، عمان ، 2008.

20. عبد العال الديربي ، محمد صادق اسماعيل ، **الجرائم الالكترونية – دراسة قانونية قضائية** – ، المركز القومي للإصدارات القانونية ، الطبعة الأولى ، 2012.

21. عمر محمد حماد ، **الاحتكار و المنافسة غير المشروعة** ، دار النهضة العربية ، 2009

22. غيطاس جمال محمد ، **عصر المعلومات : القادم مذهل أكثر** ، مركز الخبرات المهنية للإدارة ، مصر ، 2007.

23. محمد الفيومي ، **مقدمة الحاسبات الإلكترونية و تطبيقاتها في نظم المعلومات المحاسبية** ، مؤسسة شباب الجامعة ، الإسكندرية ، 1992.

24. محمد دباس الحميد، ماركو ابراهيم نينو ، **حماية أنظمة المعلومات** ، دار الحامد للنشر و التوزيع، الطبعة الأولى،2007.

25. محمد دباس الحميد ، ماركو ابراهيم نينو ، **حماية انظمة المعلومات** ، دار الحامد للنشر و التوزيع ، عمان ، الأردن ، 2009

26. محمد لعقاب ، **مجتمع الإعلام و المعلومات** ، دار هومة للنشر و التوزيع ، الطبعة الأولى ، الجزائر ، 2003.

27. محمد عبد العليم صابر ، **نظم المعلومات الإدارية** ، دار الفكر الجامعي ، الإسكندرية ، 2003.

28. مجد الدين خمش ، **العولمة و تأثيراتها في المجتمع العربي** ، دار مجدلاوي ، عمان، 2011

29. مدحت أبو النصر،**قواعد و مراحل البحث العلمي**، مجموعة النيل العربية ، الطبعة الأولى، القاهرة ، 2004.

30. منال محمد الكردي ، طلال ابراهيم العيد ، **مقدمة في نظم المعلومات الإدارية : المفاهيم الأساسية و التطبيقات** الدار الجامعية الجديدة ، الإسكندرية ، 2003.

31. نهلا عبد القادر المومني ، **الجرائم المعلوماتية** ، دار الثقافة للنشر و التوزيع ، الطبعة الاولى ، عمان ، 2008.

32. وليد عبد الرحمن خالد الفرا ، **تحليل بيانات الاستبيان باستخدام البرنامج الاحصائي** spss ، الندوة العالمية للشباب الاسلامي ، إدارة البرامج و الشؤون الخارجية ، 1430هـ

ب- الرسائل و الأطروحات

33. أيمن محمد فارس الدنف ، **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة و سبل تطويرها** ، رسالة ماجستير ، كلية التجارة ، جامعة غزة ، 2013

34. عبد الرحمن القوي ، **تكنولوجيا المعلومات و الإتصال و أثرها على إدارة الموارد البشرية** ، رسالة ماجستير في العلوم التجارية ، غير منشورة ، جامعة محمد بوضياف ، المسيلة، الجزائر ، 2007.

35. محمد بن عبد الله بن علي المنشاوي ، **جرائم الانترنت في المجتمع السعودي** ، رسالة ماجستير في العلوم الشرطية ، أكاديمية نايف العربية للعلوم الأمنية ، الرياض ، 2003

ج- الملتقيات و المؤتمرات

36. جامعة الدول العربية ، المركز العربي للبحوث القانونية ، الإجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات المنعقد في 7/5 -03- 2012 بيروت ، لبنان أنظر :http://carjj.org/node/1242

37. دياب موسى البداينة ، **الجرائم الالكترونية** : المفهوم و الأسباب ، الملتقى العلمي : الجرائم المستحدثة في ظل المتغيرات و التحولات الاقليمية و الدولية ، عمان ، الأردن ، 2014

38. زايري بلقاسم ، بلحسن الهواري ، **اقتصاديات الأفكار الرقمية و قضايا الحماية الفكرية لها** ، الملتقى الدولي حول اقتصاد المعرفة ، كلية الاقتصاد و التسيير ، جامعة بسكرة ، نوفمبر 2005.

39. سعيد علي حسن القليطي ، **التخطيط الاستراتيجي لتحقيق الأمن الاقتصادي و النهضة المعلوماتية** بالمملكة العربية السعودية ، مؤتمر تقنية المعلومات و الأمن الوطني ، الرياض ، 2007

40. عبد الله بن شائع بيهان ، **ثقافة أمن المعلومات** ، الملتقى الدولي الثالث لأمن المعلومات و الاتصالات ، سوريا، 2007.

41. مشروع وثيقة نحو مجتمع معلومات عربي ، إطار خطة العمل المشترك ، المؤتمر العربي رفيع المستوى للتحضير للقمة العالمية لمجتمع المعلومات ، القاهرة 18/16 يونيو 2003.

42. نايل الحجايا ، **التحول الالكتروني في الجامعات و أثره في التعليم الالكتروني** ، المؤتمر الدولي الأول لتقنيات المعلومات و الاتصالات في التعليم و التدريب ، الحمامات ، تونس ،7-2012/05/10

د-المجلات و المعاجم

43. عزاوي عمر و عجيلة محمد ، **مؤسسات المعرفة و ثقافة المؤسسات الاقتصادية** ، رؤية مستقبلية ، مجلة الباحث ،كلية الحقوق و العلوم الاقتصادية ، جامعة ورقلة ، العدد الرابع ، 2006.

44. أحمد صالح الهزايمة ، **دور نظم المعلومات في اتخاذ القرارات في المؤسسات الحكومية** ، مجلة جامعة دمشق للعلوم الاقتصادية و القانونية ، المجلد 25 ، العدد الأول ، 2009.

45. تركي راجي الحمود و آخرون ، **التخطيط لمواجهة الطوارئ الخاصة بأنظمة المعلومات المحاسبية في المصارف التجارية الأردنية** ، مجلة جامعة الملك عبد العزيز : الاقتصاد و الادارة ، العدد 2 ،الأردن ، 2017.

46. مأمون العزب ، أمن المعلومات في فضاءات انترنت الأشياء ، مجلة التقدم العلمي ، العدد 99 ، مؤسسة الكويت للتقدم العلمي ، أكتوبر 2019

47. أسعد حمود السعدون ، الأمن الاقتصادي : القديم و الجديد ، جريدة أخبار الخليج البحرينية ، عدد يوم الثلاثاء 11 ماي 2010.

48. معجم الحاسبات ، الطبعة الموسعة ، مجمع اللغة العربية ، مصر ، 1995.

49. مقدمة عن سياسات و معايير أمن المعلومات ، المركز القومي للمعلومات – قسم الجودة و التطوير – الاصدارة الأولى ، فبراير 2010 ، جمهورية السودان .

د- الدلائل و المنشورات:

50.يونس عرب ، **نظام الملكية الفكرية لمصنفات المعلوماتية** ، الدليل الالكتروني للقانون العربي ، ArabLawInfo ، أنظر : www.arablawinfo.com

الرسوم و النماذج الصناعية و اتفاق لاهاي ، منشور الويبو رقم (A) 429 ، المنظمة العالمية للملكية الفكرية

51.**إطار سياسات و إجراءات أمن المعلومات** "الدليل الارشادي لسياسات و إجراءات أمن المعلومات للجهات الحكومية السعودية "، المركز الوطني الارشادي لأمن المعلومات ، الطبعة الأولى ، 1436 ، السعودية .

52.ضمان أمن المعلومات للمديرين التنفيذيين : " دليل تأمين شبكات و أنظمة معلومات المؤسسات التجارية الدولية طبقا لأسس منظمة التعاون الاقتصادي و التنمية 2002 نحو ثقافة أمنية " ، غرفة التجارة الدولية ، منظومة الأعمال العالمية ، باريس 2003 .

53.علاء محمد حسونة عابد ، بيان سعيد عبد الكريم وهبة ، السياسات الإدارية لأمن المعلومات. أنظر http://www.cst.ps/ar/?404;http://www.cst.ps:80/mfarra/ISM/Ola&Bayan.ppt

- **اللغة الفرنسية**

A– Ouvrages

54. Alain Bonnet, Jean-Paul Haton ,**systèmes experts vers la maitrise technologique** , Inter édition , 1986.

55. Alain Desroches ,Alain Leory , Frédérique Vallée , **la gestion des risques « principes , et pratique »** , 3 éme édition , Lavoisier , Paris , 2015 .

56. Alain Yger , Jacques-Arthur Well , Mathématique L3-Mathématique appliquées, ED Pearson, France , 2009 .

57. Alexandre Fernandez- Toro **, sécurité opérationnelle** , -conseil pratique pour sécuriser le système d'information- , Eyrolles , 2eédition , 2016 .

58. Alphone Etienne ETOGA , **Définir un modèle générique de l'ISMS**, Travail de diplôme , Haute école de gestion de Genève , Genève , 2006

59. André CHARDONNET – Dominique THIBAUDON , **le guide du PDCA de Deming** « progrès continu et management », Editions d'Organisation , 2003 .

60. André Vaucamps, CISCO : **Sécurité des routeurs et contrôles du trafic réseau**, éditions ENI , 2010.

61. Arnaud Pelletier et Patrick Cuenot , **Intelligence Economique** ,mode d'emploi – Maitrisez l'information stratégique de votre entreprise,édition Pearson,France,2003.

62. BALANTZIAN Gérard , **les systèmes d'information** : art et pratique , édition d'organisation , Paris ,2002.

63. Bernard Foray , **la Fonction RSSI « guide des pratiques et retours d'expériences »** , ed Dunod , Paris , 2010.

64. Charron Jean-Luc et SEPARI Sabine , **organisation et gestion de l'entreprise** , 2éme édition , Edition Dunod , Paris , 2001.

65. Christian Harbulot, **manuel d'intelligence économique**, presse universitaires de France, 1er édition, paris, 2012.

66. Dario Moura Vicente , **La propriété intellectuelle en droit international privé**, Adagp : Académie de droit international de la Haye , Paris , 2009.

67. DAYAN Armand, **manuel de gestion**, volume 1 , Edition :Ellipses, paris, 1999.

68. Daniel Linlaud , **sécurité de l'information « Elaboration et gestion de la politique de l'entreprise suivant l'iso 17799** , AFNOR , France , 2003 .

69. Didier Godart , **sécurité informatique : risques , stratégies et solutions** , 2éme édition , éditions des CCI de wallonie s.a , Belgique ,2005 .

70. Y.Dupuy, M.Kalika, C.Marmuse, J.Trahand , **les systèmes de gestion** , Edition Vuibert , paris, 1989.

71. Eric Delbecque , Jean-Renaud Fayol , **Intelligence économique** , ED Vuibert , paris, 2012 .

72. Eric Filiol , **les virus informatiques : théorie, pratique et applications** , deuxième éditions , Springer , Paris , 2009

73. Eric Léopold, Serge Lhoste, **la sécurité informatique**, éditions Puf, 3éme édition, Aout, 2007 .

74. Ghilhem Fabre , **Propriété Intellectuelle** , contrefaçon et innovation – les multinationales face à l'économie de la connaissance- , Publication des Universités de Rouen et du Havre , 2009 .

75. Hubert Bitan , **Droit des créations immatérielles –logiciels , bases de données , autres œuvres sur le web 2.0** , éditions Lamy , France , 2010 .

76. Hubert Bitan , **Protection et contrefaçon des logiciels et des bases de données** , éditions Lamy , 2006 .

77. Jean –François Carpentier, **la sécurité informatique dans la petite entreprise** ,ED ENI, France, 2009 .

78. Jean François Carpentier , **la sécurité informatique dans la petite entreprise « état de l'art et bonnes pratiques »,** éditions Eni , France , 2éme édition, 2012.

79. Jean-Marc Royer , **Sécurisé l'informatique de l'entreprise : enjeux , menaces, prévention et parade** , édition ENI ,2004.

80. Jean Paul Louisot , **gestion des risques** (100 question pour comprendre et agir), éditions AFNOR , 2010

81. Jean Gerbier , **organisation et fonctionnement de l'entreprise** , Edition Tec Doc-Lavoisier , paris , 1993.

82. Jean Menthonnex, **Sécurité et Qualité informatiques-Nouvelles Orientation**, CERSSI , Presses Polytechniques et Universitaires Romandes , Suisse , 1995 .

83. Jérôme Del Duca , Alexandre Planche , **la sécurité informatique** « organisez la sécurité du SI de votre entreprise » , éditions Eni , France, 2012 .

84. Kenneth Laudon et Jane Laudon , **Management des systèmes d'information** , édition Pearson, 9éme édition , France, 2006.

85. Kenneth Laudon et Jane Laudon , Eric Fimbel , Serge Costa , **Management des systèmes d'information** , édition Pearson , 11éme édition , 2010 .

86. LAMDAN Sadek , **à la découverte de l'informatique** , 3éme édition , Edition Berti , Alger , 2001.

87. LAMIZET Bernard et SILEM Ahmed, **dictionnaire encyclopédique de sciences de l'information et de la communicatio ,** Edition Ellipses, Paris ,1997.

88. Laurent Bloch , Christophe Wolfhugel , **Sécurité informatique : principe et méthodes** , 3eme édition, ed Eyrolles, 2011.

89. Laurent Bloch , Christophe Wolfhugel , **Sécurité informatique : principe et méthode à l'usage des DSI ,RSSI et administrateurs** , 2eme édition, ed Eyrolles, paris 2009.

90. LE MOIGNE jean louis , **les systèmes de décision dans les organisations, Edition : P.U.F** , Paris , 1974.

91. Marie-Florc Célarier , Delphine Marie-Vivien , **les droits de propriété intellectuelle :guide pratique ,** éditions Cirad ,France , Janvier 2002 .

92. Michel Berteau , Eric Doyen et autres , Livre Blanc : **Benchmark des outils SMSI** , club 27001 , 1ere édition , novembre 2013 .

93. Michel Ferrary et yvon pasqueux , **management de la connaissance** , Edition Economica , Paris, 2011.

94. Michel-Henry Bouchet , Alice Guillon le Fraper du Hellen, **intelligence économique et gestion des risques** , ed pearson education , France, 2007 .

95. Michel Lafitte, **Sécurité des systèmes d'information et maitrise des risques,** édition Revue Banque, 2003.

96. Nicolas Moinet , **la boite à outils de la sécurité économique**, ED Dunod , Paris , 2015

97. Patrick Boulet, **Management de la sécurité de système d'information** , Ed Lavoisier , Paris, 2007

98. PAULET jean pierre , **dictionnaire d'économie**, Edition Eyrolles , Paris, 1992.

99. Pierre Carrier et autres , **bases de donnés dans le développement de système** , Edition Gartan morin , Canada , 1991.

100. Philippe Atelin , **Réseaux informatiques-notions fondamentales**-, troisième édition , édition ENI , France , 2009 .

101. Philippe Gillet ,**Virtualisation des systèmes d'information avec VM ware – Architectures,Projet,Sécurité et retours d'expérience -**,Editions ENI,France, 2009.

102. Philippe Gloaguen , **Le guide de l'intelligence économique** , Le guide du routard, Hachette Livre , 2012 .

103. Philippe Mathon et Frédéric Esnouf , ISA server 2004 : **protégez votre système d'information** , éditions ENI , France , 2005 .

104. Pierre-Luc REFALO , **la sécurité numérique de l'entreprise** « l'effet papillon du hacker » , Groupe EYROLLES , Paris , 2013

105. Robert Reix , **systèmes d'information et management des organisations** , 4éme édition , Edition Vuibert , Paris , 2002.

106. Tanguy HUGUES, **protéger mon ordinateur** :manuel de sécurité informatique , 1er édition , édition Lulu , 2009 .

107. Tom Gallagher, Bryan Jeffries, Lawrence Landauer, **Chasser les failles de sécurité , les meilleures pratiques pour tester la sécurité de vos logiciels** , édition microsoft ,Janvier 2007.

B- Rapport

108. « intelligence économique et stratégie des entreprises » , rapport du commissariat général au plan , travaux présidés par Henri Martre , la documentation française , 1994.

109. Rapport Carayon 2003 : « intelligence économique , compétitivité et cohésion sociale » publié par le portail de l'IE , centre national de ressources et d'information sur l'intelligence économique et stratégique , le 09/02/2013 , voir : http://www.portail-ie.fr/

110. L'insécurité économique est une crise mondiale : un rapport de l'OIT montre comment et ou l'indice de la sécurité économique est lié au bonheur.voir : https://www.ilo.org/public/french/protection/ses/download/docs/happiness.pdf

111. ISO 27001 management de la sécurité de l'information , rapport technique , librairie technique , scientifique et industriel , NORMADOC , PARIS , 2016.

C- Guides

112. Le guide du routard , le guide de l'intelligence économique , HACHETTE , livre (hachette tourisme) , 2014.

113. Jean Pierre Legendre,« intelligence économique » guide pratique pour les PME , rapport 2006 du CIE du MEDEF , Paris , novembre ,2006.

114. Introduction à la sécurité des systèmes d'information , guide pour les directeurs d'établissement de santé , direction générale de l'offre de soins , novembre , 2013.

115. La Protection des Informations Sensibles des entreprises , Guide Pratique du MEDEF , Paris , janvier 2013 .

116. Menaces sur les systèmes informatique « Guide N 65 », bureau conseil de la direction centrale de la sécurité des systèmes d'information , paris , version du 12 septembre 2006 .

117. Robert Longeon ,Jean-luc Archimbaud , guide de la sécurité des systèmes d'information à l'usage des directeurs , Centre National de la Recherche Scientifique (CNRS) , Paris ,1999 .

118. Sylvie Domenech , Manuel Marciaux et Dominique Charnassé , Guide des bonnes pratiques en matière d'intelligence économique , Service de Coordination a l'Intelligence Economique , 2009.

119. Guide pratique du Medef , la protection des informations sensibles des entreprises , paris, janvier ,2013.

D- Document, Revues , Articles

120. Abbes Rharrab , Audit sécurité des systémes d'information , licence professionnelle , université mohammed V Agdal , Maroc , 2010 .

121. Directive sur la sécurité de l'information gouvernementale , loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics

et des entreprises du gouvernement , chapitre G 1.03,a.20 , decret 7-2014 du janvier 2014 , conseil du trésor , Québec, 23.01.2014.

122. Document « Maitrise et protection de l'information » ,CLUSIF – **CLU**b de la **S**écurité de l'**I**nformation **F**rançais - , Paris , 2006

123. Edward Humphreys , revue ISO/CEI 27001 pour les PME , 2009.

124. François Fillon , Actions de l'état en matière d'intelligence économique, république Française, Paris le 15/09/2011, voir :www.economie.gouv.fr/ , visité le13/12/2012.

125. Hugo Etiévant , Normes de sécurité : les méthodes d'analyse des risques , article publié le 18 aout 2006, vu sur le site https://cyberzoide.developpez.com/securite/methodes-analyse-risques/ Le 13/06/2019 à 10h.55

126. Joseph ILLAND, politique de sécurité des systèmes d'information(PSSI), document d'orientation de sécurité des systèmes d'information, Centre National de la Recherche Scientifique (CNRS),2006.

127. La sécurité économique au quotidien en 22 fiches thématiques , Délégation interministérielle à l'intelligence économique , Avril 2014 , Fiche 4. Voir : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/outils/fiches/22-fiches-rassemblees.pdf

128. la veille stratégique « du concept à la pratique » IAAT :Institut Atlantique d'Aménagement des Territoires , note de synthèse , juin 2005 , voir : www.iaat.org.

129. Laurent Bellefin , L'ISO 27000 nouveau nirvana de la sécurité ? , Solucum group , Livre Blanc , paris.

130. Les virus informatiques, Espace menace-groupe virus, CLUB de la Sécurité des Systèmes d'Information Français (CLUSIF), 2005. Vu sur le site : http://www.leprovostjm.com/docs/virusinformatiques.pdf Le 25/01/2016 à : 05.57

131. Marilyn Thibault , Guylaine Marcoux et autres , politique sur l'accès , la sécurité de l'information et la protection des renseignements personnels , version du janvier 2010 , société d'habitation du Québec ,.

132. Matthieu Bennasar , Julien Brigaud , Létitia Combes , Sensibilisation à la sécurité de l'information 2.0 , livre blanc , Lexis , Paris .

133. Nicolas Mayer , Jean philippe Humbert , la gestion des risques pour les systèmes d'information , centre de recherche public Henri Tudor , Article paru dans le magasin MISC n24 , 2006

134. Politique de sécurité des systèmes d'information de l'état – version 10-publication de l'agence nationale de la sécurité des systèmes d'information , 17/07/2014 ,paris .

135. Pierre E.Edorh , Sécurisation globalisée des systèmes d'information de gestion , 4-Modules-T97 , 2006 .

136. Politique de sécurité des systèmes d'information de l'état , version 1.0 , Agence National de la Sécurité des Systèmes d'Information , Paris , 2014 .

137. Politique sur l'accès , la sécurité de l'information et la protection des renseignements personnels , Québec , 2010 .

138. Sécurité Economique « les bonnes pratiques pour votre entreprise », Comité Opérationnel Défensif de l'Intelligence Economique de Lorraine , DRIRE Lorraine .

139. Sécurité économique , portail de l'IE , centre national de ressources et d'information sur l'intelligence économique et stratégique , TROYES, 24-26 septembre 2014 , voir : http://www.portail-ie.fr/lexiques/read/44

140. Stéphane Rouhier , étude « protection de l'information –enjeux, gouvernance et bonnes pratiques», Cigref, 2008.

141. **Susan.M.Caldwell** et autres ,Manager la sécurité d'information , une recommandation,la revue n 85 , Février 2007 .voir :

http://www.isaca.org/chapters6/paris/b%C3%A9n%C3%A9fices/documents/s%C3%A9curit%C3%A9/85_pp11_18.pdf

142. Thierry Boileau , mise en œuvre de la SSI de SUSS Micro Optics par l'approche processus iso/IEC 27001, mémoire présentée en vue d'obtenir le diplôme d'ingénieurs , CNAM, Conservatoire National des Arts et métiers , centre régionale associe de Lyon ,Hal « archives ouvertes », 2010 .

- **اللغة الإنجليزية**

A- Books

143. Alain calder , **ISO 27001/ISO27002** , A pocket guide , second edition , IT Gouvernance Publishing , 2013

144. Bagad, V.S, Management Information Systems , 3rd revised edition , India Technical Publication Pune , 2008.

145. Bodnar , Jeorge and Wiliam , Hipwood Accounting Information System , new jersy , Prentice Hall , 1995.

146. Laudon, K.C et Laudon, J.P , Management Information System , 6th ed, Prentice-Hall International , new jersy , 2005.

147. Laudon, Kemeth, Laudon, jane, Management Information Systems , Managing the Digital Firm , 9th edition , new jersy :Prentice Hall Inc , 2010.

148. Pierce,c, collected papers of Charles Sanders Pierce , MA: Harvard University Press , 1958.

149. Whitman Michael , Mattod Herbert , Principles of Information Security , 4th edition , Boston : cengage learning / course-technology , 2011.

150. George Sadowsky, James x.Dempsey, Alan greenberg, Barbara J.Mack, Alan Schwartz, Information Technology Security Handbook , the International Bank for Reconstruction and Development, Washington, 2003.

151. See :Cisco systems ,inc :Indiana, cisco press, cisco networking academy, first year companion guide , 2nd ed, 2001.

152. " Internal threat-Risks and countermeasures", 15/12/2001 in : http://www.sans.org/rr/papers/60/475.pdf

153. Sigurjon Thor Arnason , Keith D.Willett , how to achieve 27001 certification " An example of applied compliance management " ,Averbach publications , 2008.

154. Australian National Audit Office(2006). IT Security Management Audit Report No.23 2005-2006, www.anao.gov.au/uploads/documents/2005- 06_Audit_Report_23.pdf

المواقع الالكترونية :

155. Layered DMZ Network Security Architecture Design , February 2018 , voir: https://www.sunnyhoi.com/layered-dmz-network-security-architecture-design/

156. Définitions de l'intelligence économique , voir : http://www.actulligence.com/ressources/définitionsde-l'intelligence-économique , visité le 13/12/2012

157. **https://mustafasadiq0.com/2014/09/30** **vu le : 15/09/2018**

الملاحق

جامعة أبو بكر بلقايد – تلمسان-

كلية العلوم الاقتصادية و علوم التسيير

قسم علوم التسيير

الاستمارة Questionnaire

سيد(ت)ي السلام عليكم :

الاستبيان الذي بين أيديكم يتضمن مجموعة من الأسئلة خاصة بموضوع تحضير أطروحة دكتوراه تحت عنوان **مستوى أمن المعلومات في المؤسسة الجزائرية و مدى تأثره بطبيعة التهديدات و طبيعة الحماية المطبقة**.

و للوصول إلى نتيجة ذات مصداقية نرجو منكم سيد(ت)ي الإجابة بكل دقة و صراحة و موضوعية .

بما أن هذا الاستبيان صمم لأغراض البحث العلمي فقط ، فإن المعلومات المقدمة ستحاط بالسرية التامة.

ضع علامة (×) أمام الاجابة المختارة . شكرا على مساهمتكم.

Monsieur

Après les salutations, permettez de mettre a votre disposition le présent questionnaire contenant un ensemble de questions concernant la préparation d'une thèse de doctorat sous le titre: **Le niveau de sécurité de l'information dans l'institution algérienne et l'ampleur de l'impact des menaces et la nature de la protection à ce niveau** .

je vous saurais reconnaissant pour y avoir répondus avec objectif et précision sur toutes les questions énumérées ci-après, afin d'atteindre un résultat crédible. Étant donné que ce questionnaire est conçu uniquement à des fins de recherche scientifique, les informations fournies seront strictement confidentielles.

Placez un (x) devant la réponse sélectionnée. Merci pour votre contribution.

المشرف :أ.د بوشيخي عائشة

الباحث: فيلالي أسماء

Axe de données générales — محور البيانات العامة

1. Informations personnelles — 1- المعلومات الشخصية :

الجنس : ذكر(masculin) ☐ أنثى(féminin) ☐

السن (âge) :

2. Informations fonctionnelles: — 2- المعلومات الوظيفية

- التحصيل العلمي :

ثانوي secondaire ☐ جامعي universitaire ☐

دراسات عليا étude supérieurs ☐ آخر autres ☐

.....

- التخصص العلمي :..... Spécialité scientifique .....
- عدد سنوات الخبرة:..... Années d'expérience..... .....
- الوظيفة:..... Fonction.....

3- معلومات حول الموضوع :

أ- هل يتواجد بالمؤسسة فريق أو مسؤول عن أمن المعلومات و أمن أنظمة المعلومات؟

a- L'organisation dispose-t-elle d'une équipe ou un responsable de la sécurité de l'information et de la sécurité des systèmes d'information?

نعم oui ☐ لا non ☐

- إذا نعم : مسؤول الأمن المعلوماتي هو على أي مستوى ؟

مستوى الادارة العامة ☐ مستوى ادارة أنظمة المعلومات ☐

مستوى ادارة المخاطر ☐ من خارج المؤسسة ☐

- Si oui: L'agent de sécurité de l'information est à quel niveau?

Au niveau de l'administration générale ☐

au niveau de la direction «gestion des risque » ☐

au niveau de la direction des systèmes d'information ☐

de l'extérieur ☐

المحور الأول : طبيعة أمن المعلومات داخل المؤسسة						
الرقم	العبارات	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
01	الإدارة العليا واعية و محسسة بما يكفي بطبيعة التهديدات التي تتعرض لها نظم المعلومات La haute direction est suffisamment consciente et sensible à la nature des menaces pesant sur les systèmes d'information					
02	الادارة العليا واعية بأهمية و ضرورة توفير الأمن لأنظمة المعلومات La haute direction est consciente de l'importance et de la nécessité d'assurer la sécurité des SI					
03	اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية Les mesures de protection appliquées par l'institution se tiennent au courant de l'évolution de l'environnement technologique					
04	المؤسسة تخصص ميزانية خاصة لإدارة عملية أمن نظم المعلومات Il existe un budget spécial pour gérer le processus de sécurité des systèmes d'information					
05	المصاريف التي تصرف على تطبيق أمن المعلومات ضرورية و تساهم في حماية المؤسسة و تطورها . Les dépenses consacrées à la mise en œuvre de la sécurité de l'information sont nécessaires et contribuent à la protection de l'institution et de son développement					
06	المؤسسة تعتمد سياسة أمنية مكتوبة و يعرفها الجميع La société adopte une politique de sécurité écrite que tout le monde connaît					
07	قواعد و مبادئ السياسة الأمنية محددة و واضحة Les règles et les principes de la politique de sécurité sont spécifiques et clairs					
08	الموظفون ذوي ثقافة أمنية و واعون بمسؤولياتهم Personnel doté d'une culture de sécurité et conscient de ses responsabilités					

09	المؤسسة تقوم بدورات تكوينية و تحسيسية حول موضوع أمن المعلومات L'organisation organise des cours de formation et de sensibilisation sur le thème de la sécurité de l'information					
المحور الثاني : طبيعة التهديدات						
الرقم	**العبارات**	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
10	التهديدات التي تتعرض لها المؤسسة هي من مصادر داخلية Les menaces pesant sur l'institution proviennent de sources internes					
11	التهديدات التي تتعرض لها المؤسسة هي من مصادر خارجية Les menaces pesant sur l'institution proviennent de sources externes					
12	التهديدات التي تتعرض لها المؤسسة هي من طرف العمال Les menaces qui pèsent sur l'institution proviennent des travailleurs					
13	التهديدات التي تتعرض لها المؤسسة هي من طرف المتدربين Les menaces qui pèsent sur l'institution proviennent de stagiaires					
14	التهديدات التي تتعرض لها المؤسسة هي من طرف الزوار Les menaces qui pèsent sur l'institution proviennent des visiteurs					
15	التهديدات التي تتعرض لها المؤسسة هي من طرف المنافسين Les menaces qui pèsent sur l'institution proviennent de concurrents					
16	التهديدات التي تتعرض لها المؤسسة هي من طرف غرباء (هاكر ، كراكر....) Les menaces qui pèsent sur l'institution proviennent d'étrangers (Hacker, Kraker, etc.).					
17	التهديدات التي تتعرض لها المؤسسة عبارة عن سرقة Les menaces qui pèsent sur l'institution sont le vol..					

		موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
18	التهديدات التي تتعرض لها المؤسسة عبارة عن دخول غير مصرح Les menaces qui pèsent sur l'entreprise sont les accès non autorisés.					
19	التهديدات التي تتعرض لها المؤسسة عبارة عن هندسة اجتماعية(التفتيش في المهملات ، الخداع...) Les menaces qui pèsent sur l'institution sont l'ingénierie sociale					
20	التهديدات التي تتعرض لها المؤسسة عبارة عن برامج خبيثة : فيروس ، دودة ، حصان طراودة..... Les menaces pesant sur l'entreprise sont des programmes malveillants: virus, ver, cheval de Troie					
21	التهديدات التي تتعرض لها المؤسسة عبارة عن قرصنة معلوماتية : التصنت ، رفض الخدمة ، التزوير .... Les menaces pesant sur l'organisation sont le piratage d'informations: écoute indiscrète, déni de service, contrefaçon...					
22	التهديدات التي تتعرض لها المؤسسة ناتجة عن سوء التسيير و نقص الكفاءات البشرية في مجال أمن المعلومات Les menaces pesant sur l'organisation résultent d'une mauvaise gestion et du manque de ressources humaines dans le domaine de la sécurité.					
23	التهديدات التي تتعرض لها المؤسسة ناتجة عن ثغرات أمنية في الأنظمة و البرامج Les menaces pesant sur les systèmes d'information d'entreprise sont causées par des failles de sécurité dans les systèmes et les logiciels					
24	التهديدات التي تتعرض لها المؤسسة ناتجة عن بساطة أنظمة الحماية Les menaces pesant sur l'entreprise sont causées par la simplicité des systèmes de protection					
25	التهديدات التي تتعرض لها المؤسسة ناتجة عن غياب اليقظة داخل المؤسسة Les menaces qui pèsent sur l'institution sont dues au manque de vigilance de l'institution					

26	التهديدات التي تتعرض لها المؤسسة هي بدافع الانتقام Les menaces qui pèsent sur l'institution sont motivées par la vengeance					
27	التهديدات التي تتعرض لها المؤسسة هي بدافع الحصول على المال Les menaces qui pèsent sur l'institution sont motivées par l'argent					
28	التهديدات التي تتعرض لها المؤسسة هي بدافع المنافسة Les menaces pesant sur l'entreprise sont dues à la concurrence					
29	التهديدات التي تتعرض لها المؤسسة غير متعمدة Les menaces pesant sur l'entreprise ne sont pas intentionnelles					

المحور الثالث : طبيعة الحماية المطبقة داخل المؤسسة

الرقم	العبارات	موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
30	المؤسسة تعتمد على كاميرات المراقبة لحماية الموقع و التجهيزات L'institution s'appuie sur des caméras de surveillance pour protéger le site et les équipements					
31	المؤسسة تعتمد على مراقبة الدخول عن طريق حمل الشارات و مرافقة الزوار لمنع أي تجاوزات L'organisation s'appuie sur le contrôle d'accès en portant les badges et en accompagnant les visiteurs pour prévenir tout abus.					
32	المؤسسة تعتمد على كاشف الحريق و الاطفاء الآلي لحماية موقعها La société s'appuie sur le détecteur d'incendie et les extincteurs pour protéger son emplacement.					
33	المؤسسة تعتمد على أجهزة الانذار عند أي تدخل غير مسموح لحماية موقعها L'organisation s'appuie sur des dispositifs d'alarme en cas d'interférences suspectes pour protéger son emplacement					
34	المؤسسة تعتمد على مضادات الفيروس لحماية أنظمتها المعلوماتية L'organisation s'appuie sur des antivirus pour protéger ses systèmes d'information					

		موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
35	المؤسسة تعتمد على الجدران النارية لحماية أنظمتها المعلوماتية L'organisation s'appuie sur des pare-feu pour protéger ses systèmes d'information					
36	المؤسسة تعتمد على برامج لتشفير كل البيانات و الاتصالات و التطبيقات المتنقلة و المخزنة لحمايتها من التصنت L'entreprise adopte des programmes pour crypter toutes les données, communications et applications mobiles et stockées					
37	المؤسسة تعتمد على أنظمة كشف التدخل لحماية أنظمتها المعلوماتية من أي دخول غير مصرح L'organisation s'appuie sur des systèmes de détection d'intrusion pour protéger ses systèmes d'information contre les accès non autorisés					
38	المؤسسة تعمل على تحديث برامج الحماية دوريا L'organisation met à jour les programmes de protection périodiquement					
39	المؤسسة تقوم باختبار أنظمة الحماية دوريا لاكتشاف الثغرات L'organisation teste périodiquement les systèmes de protection pour détecter les failles					
40	تتم معالجة الثغرات المكتشفة فورا Les failles détectées sont traitées immédiatement					
41	الموارد الحرجة و الحساسة للمؤسسة معرّفة Les ressources critiques de l'entreprise sont identifiées					
42	المؤسسة تصنف المعلومات السرية و الموارد الحرجة لديها حسب أهميتها و درجة الخطورة التي قد تتعرض لها L'organisation classe les informations confidentielles et les ressources critiques en fonction de leur sensibilité et du degré de risque auquel elles peuvent être exposées					
43	المعلومات الحساسة في المؤسسة يتم الاحتفاظ بها الكترونيا Les informations sensibles dans l'organisation est maintenue électroniquement					
44	فريق الأمن يعتمد طرق النسخ الاحتياطية المخزنة و الرجوع إليها في حالة الكوارث					

					L'équipe de sécurité s'appuie sur les méthodes de sauvegarde stockées et référencées en cas de sinistre	
					فريق الأمن يدرس التهديدات التي قد يتعرض لها أي مورد L'équipe de sécurité de l'information examine les menaces pesant sur les ressources sensibles	**45**
					فريق الأمن بقيم احتمال تعرض الموارد الحرجة للخطر L'équipe de SI évaluent la probabilité de survenance des risques sur les ressources critiques	**46**
					فريق الأمن المعلوماتي يدرس درجة خطورة التهديد الذي تتعرض له الموارد الحرجة L'équipe de SI évaluent l'impact (gravité) des risques pesant sur les ressources critiques	**47**
					فريق الأمن يحدد مستوى الخطر المقبول L'équipe de sécurité détermine le niveau de risque acceptable	**48**
					فريق الأمن يعتمد طرق دولية لتحليل و تقييم المخاطر L'équipe de sécurité adopte des méthodes internationales d'analyse et d'évaluation des risques (Mehari, Ebios,….)	**49**
					المؤسسة لديها مخططات لاستئناف العمل بعد حدوث أي طارئ La société dispose d'un plan de secours en cas de catastrophe majeure	**50**

- هل تعرضتم لتهديدات إلكترونية أو مادية عرضت أنظمة المعلومات للخطر؟ ما هو نوع التهديد ؟ و ما هو مصدره ؟ و ما كانت دوافعه؟
- Avez-vous fait face à des menaces électroniques ou physiques qui ont compromis les systèmes d'information? Quel genre de menace? Quelle est sa source? Quels étaient ses motifs?

……

……

……

……

- كيف تعاملتم مع الأمر ؟ * Comment avez-vous géré cela؟

……

……

……

……

……

- هل المؤسسة تدرج وظيفة أمن المعلومات ضمن هيكلها التنظيمي ؟ ضمن أي مصلحة ؟

- L’institution incorpore-t-elle la fonction de sécurité de l’information dans sa structure organisationnelle? Sous quel niveau?

……

……

……

……

- هل المؤسسة تعتمد معايير أمن دولية لتطبيق سياسة أمن المعلومات ؟ ما هي؟

- L'institution adopte-t-elle des normes de sécurité internationales pour mettre en œuvre la politique de sécurité de l'information?

……

……

……

قيمة معامل الثبات " ألفا كرونباخ "

1- المحور الأول :

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,959	9

2- **المحور الثاني :**

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,616	20

3- المحور الثالث :

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,970	21

4- الكلية :

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,949	50

معامل الارتباط "بيرسون" بين المتغير التابع و المتغيرات المستقلة

Corrélations

		طبيعة امن المعلومات في المؤسسة	طبيعة التهديدات في المؤسسة	طبيعة الحماية المطبقة في المؤسسة
طبيعة امن المعلومات في المؤسسة	Corrélation de Pearson	1	-,080	,855**
	Sig. (bilatérale)		,647	,000
	N	35	35	35
طبيعة التهديدات في المؤسسة	Corrélation de Pearson	-,080	1	,045
	Sig. (bilatérale)	,647		,799
	N	35	35	35
طبيعة الحماية المطبقة في المؤسسة	Corrélation de Pearson	,855**	,045	1
	Sig. (bilatérale)	,000	,799	
	N	35	35	35

**. La corrélation est significative au niveau 0.01 (bilatéral).

معامل التحديد للمتغير المستقل 1 (طبيعة التهديدات)

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,080[a]	,006	-,024	1,36368

a. Valeurs prédites : (constantes), المؤسسة في التهديدات طبيعة

تحليل التباين

ANOVA[b]

Modèle		Somme des carrés	Ddl	Moyenne des carrés	D	Sig.
1	Régression	,398	1	,398	,214	,647[a]
	Résidu	61,367	33	1,860		
	Total	61,765	34			

a. Valeurs prédites : (constantes), المؤسسة في التهديدات طبيعة

b. Variable dépendante : المؤسسة فى المعلومات امن طبيعة

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		A	Erreur standard	Bêta		
1	(Constante)	4,040	1,776		2,274	,030
	طبيعة التهديدات في المؤسسة	-,286	,619	-,080	-,462	,647

a. Variable dépendante : المؤسسة في المعلومات امن طبيعة

معامل التحديد للمتغير المستقل 2 (طبيعة الحماية)

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,855[a]	,731	,723	,70978

a. Valeurs prédites : (constantes), المؤسسة في المطبقة الحماية طبيعة

تحليل التباين ANOVA

ANOVA[b]

Modèle		Somme des carrés	ddl	Moyenne des carrés	D	Sig.
1	Régression	45,140	1	45,140	89,601	,000[a]
	Résidu	16,625	33	,504		
	Total	61,765	34			

a. Valeurs prédites : (constantes), المؤسسة في المطبقة الحماية طبيعة

b. Variable dépendante : المؤسسة في المعلومات امن طبيعة

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		A	Erreur standard	Bêta		
1	(Constante)	,053	,356		,150	,882
	طبيعة الحماية المطبقة في المؤسسة	1,008	,106	,855	9,466	,000

a. Variable dépendante : المؤسسة في المعلومات امن طبيعة

نتائج تحليل الانحدار المتعدد التدريجي لاختبار أثر أبعاد الحماية المطبقة على مستوى أمن المعلومات

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		A	Erreur standard	Bêta		
1	(Constante)	-,144	,412		-,351	,728
	تصنيف الموارد الحرجة	1,004	,117	,832	8,608	,000
2	(Constante)	-,424	,388		-1,092	,283
	تصنيف الموارد الحرجة	,603	,178	,499	3,381	,002
	الحماية البرمجية	,499	,178	,414	2,803	,009

a. Variable dépendante : المؤسسة في المعلومات امن طبيعة

Variables exclues[c]

Modèle		Bêta dans	t	Sig.	Corrélation partielle	Statistiques de colinéarité
						Tolérance
1	الحماية المادية	,152[a]	1,229	,228	,212	,605
	الحماية البرمجية	,414[a]	2,803	,009	,444	,355
	تسيير المخاطر	,438[a]	2,408	,022	,392	,246
2	الحماية المادية	-,019[b]	-,139	,890	-,025	,441
	تسيير المخاطر	,230[b]	1,067	,294	,188	,166

a. Valeurs prédites dans le modèle : (constantes), الحرجة الموارد تصنيف

b. Valeurs prédites dans le modèle : (constantes), البرمجية الحماية ,الحرجة الموارد تصنيف

c. Variable dépendante : المؤسسة في المعلومات امن طبيعة

نتائج تحليل الانحدار المتعدد لاختبار أثر طبيعة التهديدات و أثر طبيعة الحماية المطبقة على مستوى أمن المعلومات

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		A	Erreur standard	Bêta		
1	(Constante)	1,432	,940		1,524	,137
	طبيعة التهديدات في المؤسسة	-,496	,315	-,139	-1,575	,125
	طبيعة الحماية المطبقة في المؤسسة	1,014	,103	,865	9,808	,000

a. Variable dépendante : المؤسسة في المعلومات امن طبيعة

الفهرس العام

الملخص

تهدف هذه الدراسة إلى تحليل مستوى أمن المعلومات على مستوى المؤسسات الجزائرية ، و مدى تأثره بطبيعة التهديدات التي تتعرض لها المؤسسة بصفة عامة ، و نظام المعلومات بصفة خاصة ، ومدى تأثره أيضا بطبيعة الحماية المطبقة.

خلصت الدراسة التي تمت على مستوى 35 مؤسسة إلى أن مستوى أمن المعلومات في المؤسسات الجزائرية متوسط، و أنه يتأثر بطبيعة الحماية المطبقة، بحيث كلما ارتفع مستوى الحماية و تطورت أيضا الوسائل و الاستراتيجيات الخاصة بالحماية كلما ارتفع مستوى أمن المعلومات، و عليه بما أن مستوى الحماية المطبقة متوسط فإن مستوى أمن المعلومات متوسط أيضا، أما بالنسبة للتهديدات فتوصلت الدراسة إلى أن أمن المعلومات في المؤسسات الجزائرية لا يتأثر بطبيعة التهديدات التي تتعرض لها المؤسسات وأنظمتها ، ما عدا التهديدات التنظيمية المتمثلة خصوصا في كفاءة العامل البشري على مستوى المؤسسة .

الكلمات المفتاحية : أمن المعلومات ، نظام المعلومات ، التهديدات ، الذكاء الاقتصادي ، المؤسسة الجزائرية.

Résumé :

Le but de cette étude est d'analyser le niveau de sécurité de l'information au niveau des institutions algériennes, et de déterminer dans quelle mesure cette sécurité est affectée d'abord par les menaces qui pèsent sur l'institution et ses systèmes d'information et ensuite par la nature de la protection appliquée.

L'étude, menée au niveau de 35 entreprises, a révélé que le niveau de sécurité de l'information dans les entreprises algériennes est moyen et qu'il est affecté par la nature de la protection appliquée: plus le niveau de protection est élevé, plus les moyens et les stratégies de protection sont développés, plus le niveau de sécurité de l'information est élevé. Les données ont révélé que la nature des menaces pesant sur les institutions et leurs systèmes n'affectait pas la sécurité des informations dans les entreprises algériennes, à l'exception des menaces organisationnelles, notamment en ce qui concerne l'efficacité du facteur humain au niveau de l'entreprise.

Mots-clés: sécurité de l'information, système d'information, menaces, intelligence économique, fondation algérienne

Abstract :

The purpose of this study is to analyze the level of information security at the level of Algerian companies, the extent of its impact on the nature of the threats to the company in general, and the system of information in particular, as well as its impact on the nature of the protection applied.

The study, conducted at the level of 35 companies, revealed that the level of information security in Algerian companies is average and that it is affected by the nature of the protection applied: the higher the level of protection, the more protection means and strategies are developed, the higher the level of information security. The data revealed that the nature of threats to institutions and their systems did not affect the security of information in Algerian institutions, with the exception of organizational threats, particularly with regard to the effectiveness of the human factor at the national level of the company.

.

Keywords: Information Security, Information System, Threats, Economic Intelligence, Algerian Foundation