جامعة الجيلالي بونعامة خميس مليانة

كلية العلوم الإنسانية والاجتماعية

قسم العلوم الإنسانية

شعبة : علم المكتبات والتوثيق

مذكرة مقدمة لنيل شهادة الماستر تخصص: إدارة المؤسسات الوثائقية والمكتبات

تحت عنوان:

أمن المعلومات بمصلحة أرشيف للصندوق الوطني للتقاعد لولاية تيسمسيلت

من إعداد:

- عدة فاطمة

لجنة المناقشة

		رئيسا
أ. بوصحرا سعاد	جامعة جيلالي بونعامة – خميس مليانة	مشرفا
		مناقشا

السنة الجامعية: 2019- 2020


بسم الله الرحمن الرحيم

شكر وعرفان

بسم الله الرحمن الرحيم

قال تعالى(وأما بنعمة ربك فحدث)

و قال عز وجل(وإذا تأذن ربكم لئن شكرتم لأزيدنكم ولئن كفرتم إن عذابي لشديد)

قال رسول الله صلى الله عليه وسلم : لا يشكر الله من لم يشكر الناس

الحمد الله وشكر له على ما هداني إياه وتعليمه لي ما لم أعلم، وأصلي وأسلم على صفوة خلقه وعلى من اهتدى بهدية إلى يوم الدين:

تحية تبعث روح العرفان الجميل والامتنان الكبير إلى كل من ساهم في إنجاز هذا البحث وجعله يرى شمس الأفق

إلى كل من جعل هذا العمل يلبس ثوب النجاح

إلى الذي قال فيهما الرحمن (واخفض لهما جناح الذل من الرحمة وقل ربي ارحمهما كما ربياني صغيرا)

إلى أساتذتنا الكرام الذين ساندونا خلال مسارنا الدراسي الجامعي والذين ساهموا في تكويننا من قريب أو بعيد خاصة الأستاذة المشرفة بوصحرا سعاد التي لم تبخل علينا بالنصائح والتوجهات طيلة فترة إشرافها علينا أو خلال التدريس فقد كانت سندا لي بتوجهاتها بالإضافة إلى الارشيفي منصور خوجة الذي قدم لي كل المساعدات التي كانت ضرورية لإتمام مذكرتي رغم الظروف الصعبة في ظل جائحة كرونا .

إهداء

بسم الله رحمان الرحيم

الحمد الله الذي بنعمته تتم الصالحات وبعونه

قمت بهذا العمل المتواضع الذي أهديه إلى:

- ❖ إلى من كانت ضياءا لي في ظلمات الحياة إلى التي جعلت الجنة تحت أقدامها أمي جنتي الغالية
- ❖ إلى من كان سندي طيلة سنين عمري وسهر على نجاحي وكان سر فلاحي من كان أولى مدرس لي في الحياة: ابي العزيز عبد القادر
- ❖ إلى من لا تستطيع الكلمات وصفهم لأنهم منبع الحب و الحنان و معنى الصداقة والصدق: توأمي فاطمة ،صديقة طفولتي أمينة ،لبنة الفتاة التي جمعتني بها الأيام،ندى اختي و سندي،نصيرة مصدر الضحك،نسرين رمز الهدوء،فايزة شعار للسعادة،
- ❖ إلى كل عائلتي عدة و بوعلام وإلى إخوتي طيب،محمد،ياسين،نور الدين
- ❖ و أخواتي :هدى،حنان ،ليلى،مريم و أولادهم من كبيرتهم هنونة إلى صغيرهم فاروق
- ❖ إلى من سوف يقاسمني و يشاركني درب و مشوار حياتي : جمال
- ❖ إلى كل من ساهم في وصولي إلى هذا العمل المتواضع
- ❖ إلى كل طالب علم ومثقف وباحث...
- ❖ إلى من شاركني وقاسمني لبلوغ هذا العمل من زملاء
- ❖ إلى كل طلبة علم المكتبات والعلوم الوثائقية.
- ❖ إلى كل من يحمل لي ذرة حب واحترام في قلبه
- ❖ وإلى كل هؤلاء أهدي ثمرة هذا العمل

راجية من الله عز وجل أن يبقي دائما وردة علم تتفتح لكل باحث عن الحقيقة

البطاقة الفهرسية

عدة ، فاطمة

أمن المعلومات بمصلحة الأرشيف للصندوق الوطني للتقاعد لولاية تيسمسيلت -الجزائر/ عدة فاطمة؛ إشراف :بوصحرا سعاد – [د.ط][د.ن]،2020 .- ورقة 143،جداول ،أشكال ،الصور؛30 سم

بيبليوغرافيا : ص : 118 - 125. الملاحق ص: 126- 143

مذكرة ماستر: علم المكتبات تخصص إدارة مؤسسات وثائقية : جامعة خميس مليانة : 2019-2020

بوصحرا سعاد إشرافا

مستخلص :

تهدف هذه الدراسة إلى معرفة مدى تحقيق و مساهمة أمن المعلومات في حفاظ على سريته بمصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد لولاية تيسمسيلت و ذلك من خلال الدراسة الميدانية التي أجريت على مستواها ،باستخدام المنهج الوصفي ،بالإضافة إلى المقابلة و التقييم بمعيار إيزو 27002 كأدوات لجمع البيانات ،كما أسفرت هذه الدراسة بمجموعة من النتائج أهمها:

- المؤهلات البشرية و الإمكانيات المادية التي تتوفر في مصلحة الأرشيف مؤسسة الصندوق الوطني للتقاعد تعتبر غير كافية في تحقيق الأمن المعلوماتي على مستواها
- وجود تطبيق جزئي لمعيار إيزو 27002 العالمي لأمن المعلومات داخل مؤسسة الصندوق الوطني للتقاعد بلا معرفة مسبقة منهم بأنه معيار دولي لأمن المعلومات
- تتوفر مصلحة أرشيف الصندوق الوطني للتقاعد على حماية أمن معلوماتها من المهددات و الأخطار التي تتعرض لها

الكلمات المفتاحية :

أمن المعلومات ؛ الأرشيف؛ مركز الصندوق الوطني للتقاعد؛ ولاية تيسمسيلت

Extracted

This study aims to find out the extent to which information security is achieved and contributed to maintaining its confidentiality within the archives of the National Pension Fund Foundation for the state of Tesmeselt through the field study conducted at its level using the descriptive method in addition to the interview and evaluation based on the iso 27002 standard as a tool for collecting data on this subject as this study came out with a set of results, the most important of which

.1The human qualifications and material capabilities of the Archives of the National Pension Fund Foundation are sufficient in achieving information security at their level.

.2A partial application of ISO 27002 to information security within the National Pension Fund foundation without their knowledge that it is a global information security standard

.3The existence of protection against the threats and risks to the Foundation of the National Pension Fund for the State of Tesmeselt

Keywords:

Information Security; Archive; National Pension Fund Center,Tismeselt State

قائمة الجداول

قائمة الجداول:

قائمة الأشكال

قائمة الأشكال:

قائمة الصور

قائمة الصور

قائمة المختصرات

الكلمة	اختصارها
د.ط	بدون طبعة
ع	عدد
م	مجلد
ص	صفحة
ط	طبعة
تر	ترجمة

قائمة المحتويات

قائمة المحتويات :

الفصل الثاني: الأرشيف، المفاهيم والأطر النظرية

الفصل الثالث: الجانب التطبيقي، أمن المعلومات بمصلحة أرشيف الصندوق الوطني للتقاعد

مقدمة

مقدمة :

شهدت مؤسسات المعلومات خلال العقدين الأخيرين تطورات عميقة وشاملة في شكلها وتسييرها، وكان منتج هذا التأثير المتسارع تكنولوجيا المعلومات والاتصال، فقد ساهم في تحديث الربط ونقل المعلومات عبر عدة شبكات كشبكة الانترنيت والشبكة الداخلية والمحلية وغيرها، وأتاح فرص ربط فروع المؤسسة وأجزائها لتكون كيانا واحدا حتى وان كانت على مستوى العالم، وقد مست التطورات الحديثة كذلك طرق انشاء معلومات في صيغة الكترونية وهو الوسيط الوحيد الذي يمكنه العمل في هذه البيئة المعاصرة.

إن المؤسسات الأرشيفية المعاصرة هي أكثر نظم المعلومات التزاما بالمعايير المناسبة لما تشغله من حيز علمي وتاريخي محافظ للإرث الإنساني المعرفي، وتعتبر أكثر المؤسسات حاجة إلى هذه البيئة وتمثل لها نقطة مهمة تدفعها سواء أكانت عامة أو خاصة إلى العمل عبر الشبكات، ونظم التسيير المتكاملة، وقواعد البيانات، حيث سيؤدي هذا إلى توفر بيئة الكترونية للجميع و ادارة بلا ورق وتخفيض تكاليف التخزين. وتتمتع الوثائق الالكترونية بخصائص عديدة كالتنقل السريع، واستخدام البرمجيات، وتسريع اتخاذ القرارات وغيرها، فبالرغم من أنها يافعة المنشأ، إلا أن العالم تقبلها بسرعة وهي لا تزال عرضة للنقد فيرى الكثير من الأشخاص والباحثين أن هنالك تخوفا أمنيا تحمله.

وقد واجه الأرشيفيون والمختصين بالأرشيف في البداية مسألة استخدام التقنيات الحديثة في مجال الارشيف مع كثير من الشكوك، ومعظم هذه الشكوك تتعلق بأمن الوثيقة الالكترونية، فمن المعروف أن صور الوثيقة الورقية المحفوظة الكترونيا قد تتعرض للتخريب او التزوير المتعمد أو غير متعمد، وكذلك إلى تقادم الأجهزة والنظم والبرمجيات القارئة لها، فيضطر التقنيون إلى نقلها إلى نظم جديدة، وقد يتعرض كذلك النظام إلى فقد بيانات التشغيل الأساسية فتحدث اخطاء تجبر ادارة الارشيف إلى اعادة تحميله مجددا، وتعتبر الهجمات السبرانية أو المقرصنة للأنظمة أكبر المخاوف لأي كيان ارشيفي أو اي كيان أخر يستخدم النظم الالكترونية.

ولتغطية هذه النقائص وإعادة منح الثقة للوثيقة الإلكترونية، فقد تقدم خبراء في البرمجيات وصناع نظم الحماية إلى صياغة مصطلح أمن المعلومات ،حيث تراكمت مجموعة خبراتهم وتجاربهم لسد الثغرات العديدة لأنظمة المعلومات الالكترونية وتقديم وسائل حماية تسمح بتخفيض مستوى المخاطر الناتجة عن استخدام الوسائل الحاسوبية في حفظ الوثائق وانجاز الأعمال وغيرها في بيئة معلومات آمنة، ولعل هذه الطريقة هي الأكثر موثوقية لدى الأفراد ومؤسسات المعلومات .

رغم وجود وسائل الحماية في الجانب الالكتروني وتوفر معايير خاصة بها ودراسات دائمة تتابع المجال، إلا أن المعلومات والتي هي جوهر أي الوثيقة قد تفقد مصداقيتها عند استخدامها من قبل

المستفيدين منها أو حتى الأرشيف، فهنالك ثقة دائمة في الوثيقة الورقية الرسمية أو التاريخية فلا يمكن تزويرها ولا تحتاج إلى وسيط لقراءتها وهي مادية حيث يفضلها الجميع من حيث لمسها وتحسسها، وهي بهذا المقام تتفوق الوثيقة التقليدية على نظيرتها الالكترونية حتى وان كانت نسخة عنها. وهذا ليس سببا يجعل مؤسسات الأرشيف تبتعد عن الرقمنة وصناعة الوثائق الالكترونية فهي كذلك مصدر للمعلومات، ويعبر استخدامها عن مواكبة التطور وتحسين متابعة طلبات البحث وغيرها من الفوائد.

كما ان المعايير العالمية التي توفر الأمن للمعلومات بالتعامل معها بشكل واضح و مباشر من طرف المؤسسات يزيد من نسبة تحقيق الأمن للمعلومات و إعطائها مصداقية اكثر و بالتالي يمكن الوصول إلى منظومة معلوماتية ،مأمنه و ذات مرجع عالمي معمول به .

وفي هذا الصدد فإن دراسة هذا المجال وتطبيقاته على مؤسسات المعلومات يعتبر أحسن وسيلة لمعرفة اتجاهات أمن المعلومات ونجاعته وتقبله، وعلى اثر ذلك فإن مؤسسة الأرشيف ومصالح الأرشيف لدى المؤسسات هي اكثر النماذج التي تخدم هذه الدراسة، ومن بين تلك النماذج نجد أمن المعلومات بمصلحة الأرشيف للصندوق الوطني للتقاعد لولاية تيسمسيلت كنموذج مناسبا لها، وعليه تم تقسيتها إلى **فصل تمهيدي** و **فصلين نظريين** و **فصل تطبيقي** بالمصلحة كالتالي :

الفصل التمهيدي :وخصص هذا الفصل حول اشكالية الدراسة والفرضيات المحتملة، مع ذكر اسباب اختيار الموضوع وأهمية وأهداف الدراسة والمنهج المتبع، والتعرف على أدوات جمع البيانات المستخدمة، والدراسات السابقة وصعوبات الدراسة.

الفصلين نظريين : **الأول** منهما تطرق إلى : مفاهيم عامة حول أمن المعلومات من مكوناته وعناصره الأساسية وكذلك مجالاته والتحيات التي تواجهها، وأهداف امن المعلومات والمعايير المتعلقة به. وأما **الفصل الثاني** : فقد خصص كمدخل للأرشيف والتعريف بهذا المجال العلمي ومبادئه وأنواعه وأعمار الارشيف وأهميته والجمعيات التي ترعاه وتأثره بالتكنولوجيا والأخطار التي تواجهه وكيفية الوقاية منها.

الفصل التطبيقي: وقد تم اخذ مصلحة الأرشيف بمؤسسة صندوق التقاعد الوطني لولاية تيسمسيلت كنموذج يخدم الدراسة، فتم التعريف بها وتحديد هيكلها التنظيم، كما اجريت عليها عملية جمع البيانات وتحليلها ومعالجتها والخروج بنتائج على ضوء الفرضيات مع وضع اقتراحات مناسبة. ووضع قائمة المراجع التي تم الاعتماد عليها .

الفصل التمهيدي:

أساسيات الدراسة

1. إشكالية الدراسة:

تعتبر المعلومات كنزا هاما للجميع سواء الأفراد أو المؤسسات لأنها تقدم المعرفة وتوصل إلى الحقائق فلذا لابد من حمايتها، ومن بين هذه المعلومات نخص بالذكر المعلومات الأرشيفية التي تعتبر الذاكرة الوطنية للدول، فقد كانت تحفظ في سجلات ورقية ومجلدات وعلب أرشيفية وتودع في مخازن الحفظ الخاصة بها(الأرشيف)غير أن هذه الطريقة للحفظ لم توفر الأمن لها لأنها كانت تتعرض لمجموعة من الأخطار والمشاكل في مقدمتها السرقة والتزوير والضياع بالإضافة إلى تلف الوثائق من كثرة الاستعمال وضيق المساحة المخصصة للحفظ داخل المؤسسات وكل هذه المشاكل التي تعرضت لها المعلومات في طرق التقليدية للحفظ أدى إلى ظهور ما يسمى بالبيئة الرقمية مع التطور التكنولوجي التي شملت جميع الميادين والمؤسسات فهي تساهم في القضاء على التهديدات التي كانت تتعرض لها المعلومات في القديم وجعلت عملية الحفظ لها أكثر خصوصية وأكثر تعقيدا من قبل باعتبار ما قدمه التقدم التكنولوجي الكبير وتطور وسائل الاتصال والتواصل المتنوعة والتي جعلت العالم الآن قرية صغيرة ومنفتح على بعضه بحيث أصبح أكثر ترابطا واستخداما للأجهزة الرقمية التي تستخدم في الاتصال عن طريق الانترنت واعتماده على الشبكات في إرسال شتى أنواع البيانات والمعلومات المهمة كل ذلك أدى إلى إحداث خطر تسرب هذه المعلومات وعلى سريتها ووصولها للأشخاص غير معنيين والمنافسين وجعلها قابلة للاختراق وبالتالي أصبحت الحاجة الملحة للحفاظ على أمن المعلومات في البيئة الرقمية أيضا، هذا الاخير الذي أصبح يعتبر تحديا هاما في تكنولوجيا الجديدة للمعلومات بحكم المكانة الهامة التي أصبحت تحتلها هذه الأخيرة في المجتمعات المتطورة ،والأمر الذي جعله يشهد تطورا مستمرا على الصعيد العلمي والتقني، إلا أنه يمكن القول بأن مهاجمة الشبكات وسرقة المعلومات أصبحت أكثر سهولة والجرائم الإلكترونية أكثر تعقيدا نتيجة لتقنيات التطور التكنولوجي الحديثة والشائعة والتي توفر عدد من الثغرات في سياسة أمن المعلومات لدى المؤسسات والشركات ،كون أمن المعلومات يعد من الركائز الضرورية في حماية الأفراد والمؤسسات من أي أضرار ناتجة كونها تعتبر مهمته وذلك بضمان سلامة وسرية وتوفر وسهولة الوصول للمعلومات لأصحابها وامكانية معالجتها ،ولهذا يجب ان يعار له اهمية بالغة وكبيرة من طرف الجميع سواء الأفراد من خلال توعيهم بأهمية وقيمة المعلومات في هذا العصر والمؤسسات على اختلاف طبيعة عملها ونشاطها بوضع سياسات وإجراءات أمنية قوية لحماية المعلومات بحيث يصعب اختراقها أو الوصول إليها من أي شخص كان سوى المصرح لهم بها كونها تعتبر الركيزة الأساسية لهذه المؤسسات

والشركات وبهذا يمكن توفير أمن لهذه المعلومات بحجبها وعدم تمكين سوى المصرح لهم بالوصول إليها واستغلالها، هذا ما يقودنا الى طرح السؤال الرئيسي التالي:

ما مدى تأثير الامن المعلوماتي في الحفاظ على منظومة المعلوماتية بمصلحة أرشيف مركز الصندوق الوطني التقاعد لولاية تيسمسيلت؟

ويندرج تحت هذا التساؤل الرئيسي مجموعة من التساؤلات الفرعية التالية:

1-1. التساؤلات الفرعية للدراسة:

- هل تتوفر مصلحة أرشيف مركز الصندوق الوطني للتقاعد لولاية تيسمسيلت على الإمكانيات المادية والكفاءات البشرية اللازمة لتحقيق الأمن المعلوماتي فيها؟
- هل تعتمد مصلحة الارشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت على معايير دولية في تحقيق أمن معلوماتها؟
- هل هناك معوقات تحول دون تحقيق أمن المعلومات في مصلحة ارشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت ؟

2-1. الفرضيات :

تعتبر الفرضيات إجابات مؤقتة لإشكالية الدراسة والتي تحتمل الصواب والتأكيد أو النفي وفي نهاية الدراسة وعلى هذا الأساس تتمثل الفرضيات في مايلي:

- **الفرضية الرئيسية**

- **يؤثر الأمن المعلوماتي إيجابا في الحفاظ على سرية المعلومات داخل مصلحة أرشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت.**

- **الفرضيات الفرعية:**

1. تتوفر المصلحة على الإمكانيات المادية والكفاءات البشرية اللازمة لتحقيق الامن المعلوماتي داخلها.
2. تعتمد مصلحة ارشيف للصندوق الوطني للتقاعد لولاية تيسمسيلت على معيار إيزو 27002 في تحقيق الأمن المعلوماتي داخلها.
3. تعتبر الفيروسات والبرمجيات الضارة من بين المعوقات التي تحول دون تحقيق أمن المعلومات في مصلحة أرشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت.

2- أهداف الدراسة:

1. تحديد نقاط القوة والضعف التي يمكن لها ان تؤثر في توفير الامن المعلوماتي داخل مصلحة الارشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت.

2. التعرف على المعايير التي تتبعها مصلحة الأرشيف للصندوق الوطني للتقاعد لتحقيق الامن لمعلوماتها.

3. تسليط الضوء على المؤهلات الإطار البشري العامل بالمصلحة ومدى سعيه في توفير الامن المعلوماتي فيها.

4. إبراز المعوقات التي تقف دون تحقيق الامن المعلوماتي داخل مصلحة الأرشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت.

5. إلقاء الضوء حول الإجراءات الوقائية اللازمة التي توفر للمصلحة معلومات ذات مصداقية.

3- أسباب اختيار الموضوع:

1. قلة الدراسات التي أجريت في الموضوع

2. التحسيس بأهمية الأمن المعلوماتي في مراكز الأرشيف ومدى توفير متطلباته اللازمة لتحقيقه داخل الإدارة.

3. الرغبة الشخصية في دراسة هذا النوع من المواضيع بحكم تخصصنا في علم مكتبات إدارة مؤسسات الوثائقية في الماستر.

4- منهجية الدراسة

4-1. المنهج المتبع:

لإنجاز أي دراسة مهما كانت نوعها تتطلب إتباع منهج بحث علمي معين والذي **هو** ((تلك القواعد والأنظمة العامة التي يتم وضعها من أجل الوصول إلى حقائق مقبولة حول الظاهرة، و بعبارة أخرى المنهج هو الطريق المؤدي إلى الكشف عن الحقيقة بواسطة مجموعة من القواعد العامة تهيمن على سير العقل وتحدد عملياته حتى يصل إلى نتيجة معلومة)) في هذه الدراسة قد اتبعنا:

1. المنهج الوصفي الذي وجدناه لمناسب لها كونه ((فهو يهتم بدراسة الظواهر والأحداث كما هي من حيث خصائصها وأشكالها والعوامل المؤثرة في ذلك فهو يدرس حاضر الظواهر والاحداث عن طريق توصيفها مع جميع الجوانب والأبعاد ويهدف لاستخلاص الحلول وتحديد الأسباب والعلاقات التي أدت إلى هذه الظواهر والأحداث وكذلك تحديد العلاقات مع بعضها والعوامل

الخارجية المؤثرة بها للاستفادة منها في تنبؤ بمستقبل هذه الأحداث والظواهر))[1]. ولان دراستنا هذه تتمحور حول الأمن المعلوماتي داخل مصلحة أرشيف الصندوق الوطني للتقاعد فان هذا المنهج يسمح لنا بإتباع اسلوب من أساليبه وهو دراسة حالة الذي يعتبر :أسلوب يقوم على دراسة حالة واحدة مثل دراسة فرد أو مجموعة أو مجتمع ويتم هذا من خلال جمع معلومات وبيانات تفصيلية عن الظاهرة حول الوضع الحالي والسابق للظاهرة ومعرفة العوامل التي أثرت وتؤثر عليها والخبرات الماضية لهذه الظاهرة[2]

الذي ساعدنا في جمع معلومات حول هذا الموضوع و وصف كل جوانب الامن داخلها و معرفة درجة الموثوقية و الحماية للمعلومات الأرشيفية

2. التقييم وفقا لمؤشرات معيار إيزو 27002 لأمن المعلومات على مستوى مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد لمعرفة ما هو محقق منها.

2-4. مجالات وحدود الدراسة:

لأنه لا تخلو أي دراسة من الحدود فقد تمثلت حدود دراستنا في:

- **الحدود المكانية:**

تتمثل في مصلحة الأرشيف الصندوق الوطني للتقاعد ولاية تيسمسيلت.

- **الحدود الزمنية:**

تمتد منذ اختيار الموضوع في شهر سبتمبر 2019 إلى غاية شهر سبتمبر 2020

- **الحدود البشرية:**

أما المجال البشري فقد شمل الموظفين العاملين بمصلحة الأرشيف الصندوق الوطني للتقاعد ولاية تيسمسيلت.

3-4. مجتمع الدراسة وعينتها:

5-3-1- مجتمع الدراسة :

ويقصد به:هو جميع الأفراد أو الأشياء أو الأشخاص الذين يشكلون موضوع مشكلة البحث.بالإضافة إلى أنه جميع العناصر ذات العلاقة بمشكلة الدراسة التي يسعى الباحث إلى أن يعمم عليها نتائج الدراسة. لذا فان الباحث يسعى إلى اشتراك جميع أفراد المجتمع ،لكن الصعوبة تكمن في أن عدد أفراد المجتمع قد يكون كبيرا، بحيث لا يستطيع الباحث إشراكهم جميعا))[3]

---

[1] دشلي،كمال،منهجية البحث العلمي،مديرية الكتب والمطبوعات الجامعية،2016،ص 16

[2] أبو الشامات غالية، أنواع مناهج البحث، جامعة الجزيرة الخاصة، ص 03.متاح على الرابط http://www.jude.edu.sy أطلع علية يوم 2020/06/25 على الساعة 11.09

[3] مهدي محمد جواد محمد أبو عال، مجتمع البحث وعينته. كلية التربية الأساسية، جامعة بابل،2018،متاح على الرابط: www.basiceducation.uobabylom.edu.iq أطلع عليه يوم 06.06.2020.على الساعة:23.36.

و يمثل مجتمع الدراستنا في إداريين العاملين بمصلحة الأرشيف بالإضافة إلى موظفي مصلحة التسيير الإلكتروني تابعة لمصلحة الأرشيف والمدير حيث يبلغ مجتمع الكلي للدراسة بحوالي....

2.3.5. عينة الدراسة:

العينة: هي جزء من المجتمع تتوفر فيه خصائص هذا المجتمع الذي سحبت منه من أجل دراستها بهدف التوصل إلى نتائج يمكن تعميمها على المجتمع بعد دراستها.[1]

وقد تمثلت عينة الدراسة في مكلف بالأرشيف ومدير المؤسسة

أدوات جمع البيانات :

سوف نعتمد في دراستنا على أدوات جمع البيانات والمتمثلة في ما يلي:

1.4.5. الملاحظة:

تعتبر إحدى أدوات البحث العلمي وغالبا ما تكون هي الخطوة الأولى التي يبدأ بها الباحث بحثه ومن ثم يستمر الباحث في متابعة تطورات الظاهرة أو مشكلة الدراسة....لذا تكون الملاحظة في بادئ الامر تلقائية لظاهرة المشكلة وما يثير انتباه الباحث واهتمامه بشكل بسيط تم تتطور لتتحول إلى ملاحظة علمية دقيقة ومنتظمة بحيث على الباحث تسجيل كل الأمور سواء عن طريق الصوت او الصور أو حتى الأرقام حول تلك الظاهرة المدروسة[2]

التي تساهم إسهاما هاما في البحث الوصفي وذلك بوصف كل ما هو موجود داخل مصلحة الأرشيف للصندوق الوطني للتقاعد وكيفية استخدام الموظفين للوسائل التي من شأنها أن توفر الأمن المعلوماتي داخل المصلحة بالإضافة إلى تعامل مع وثائق الإلكترونية في مصلحة أرشيف.

2.4.5 المقابلة :

تعتبر من أهم الوسائل لجمع المادة العلمية حول موضوع بحث، حيث تستخدم هذه الأداة وبصفة خاصة بالنسبة للعلوم الإنسانية والنظرية، وهي عبارة عن محادثة وجه لوجه بين الباحث والمبحوث غالبا ما يكون عنصرا مهما في موضوع البحث ويمتلك معلومات مهمة تعد بمثابة وثائق للباحث، تمكنه من الوصول إلى نتائج مفيدة لموضوع بحثه.[3] فقد يكون هذا الشخص المستهدف مسئولا كبير بحث تتم هده المقابلة بطرح مجموعة من الأسئلة من قبل الباحث ليجيب عليها الشخص المستهدف ويقوم الباحث بتحويل الإجابات إلى معلومات وبيانات قد تكون في غاية الأهمية كونها تمكن الباحث من الوصول إلى حقائق التي حصل عليها من المصدر مباشرة وعدم توفرها في المصادر المكتبة

[1] بركات عبد العزيز، مقدمة في التحليل الإحصائي لبحوث الإعلام. الدار المصرية اللبنانية،2017،ص 362

[2] العنبكي،طه حميد حسن، العقابي نرجس زابر ،أصول البحث العلمي في العلوم السياسية، دار لأمان،الرباط،2015،ص 37 .

[3] عناية، غازي، البحث العلمي، دار المناهج للنشر والتوزيع،عمان،الأردن،2014،ص 148.

والتي تعتبر هذه النتائج من أهم الأهداف الذي يسعى إليها الباحث بالإضافة إلى التعرف على ملامح أو تصرفات المبحوثين في مواقف معينة.[1]

أما فيما يخص مقابلة التي استعملتها في دراستي هذه فهي مقابلة مقننة التي تعتبر ((استبيان بمسمى آخر بحيث تتم من خلال قيام الباحث،بإعداد القائمة من الأسئلة قبل إجراء المقابلة، إلا أن ذلك لا يمنع من طرح أسئلة غير مخطط لها إذا ما رأى الباحث ضرورة لذلك))[2]

حيث ستمكننا هذه الأداة من جمع معلومات حول مدى الدرجة التي وصل إليها هذا المركز وبالأخص مصلحة الأرشيف في الحفاظ على سرية وامن المعلومات داخلها لتحقيق مصداقية وموثوقيتها. حيث سوف تتم هذه المقابلة مع الأرشيفي بالإضافة بمؤسسة الصندوق الوطني للتقاعد.

حيث كان يفترض أن تكون المقابلة مع عمال مصلحة الأرشيفي و المدير و لنظرا لأزمة الكورونا قد خول المدير رئيس مصلحة الموظف الأرشيفي الإجابة عن كل ا أسئلة بالنيابة عنه و موظفي المصلحة

5- الدراسات السابقة:

من الضروري فبل الشروع في بدأ في أي بحث جديد أو إنجاز أي مشروع تخرج يجب اطلاع على ما توصل إلية الباحثين في نفس الموضوع المراد دراسته وذلك لربح الوقت والاستفادة من تجارب الباحثين الاولين ،لأن الدراسات السابقة تكون بمثابة مرشد للباحث إلى الطريق الذي يجب أن يسلكه وذلك بتحديد له ما إن كان مشكلة بحثه قد تم دراستها بالقدر الكافي من قبل أم لا.

الدراسات العربية:

الدراسة لأولى:

بعنوان :رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية[3]

وقد تمحورت إشكالية الدراسة حول واقع أمن المعلومات في هيئة التحقيق والادعاء العام في المملكة العربية السعودية ؟

حيث وضع الباحث مجموعة من الاسئلة حاول الإجابة عنها من خلال بحثة ومنها نجد:

[1] العنكبي، طه حميد حسن، العقابي نرجس زابر؛ المرجع سابق، ص 39 38.

[2] إيكان سومية. أدوات البحث العلمي، جامعة حسيبة بن بوعلي، شلف. متاح على الرابط:
http://wwwuniv.dz. أطلع علية يوم 2020/06/26 على الساعة 14.56.

[3] أحمد بن علي عبد الله طارش، رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية الرياض .2015.مذكرة لنيل شهادة الماجستير: تخصص دراسات استراتيجية.

1.ما متوسط درجة سياسة أمن المعلومات في المقر الرئيس بهيئة التحقيق والإدعاء العام في المملكة العربية السعودية؟

2.ما متوسط درجة تقنيات الامن المعلوماتي في المقر الرئيس بهيئة التحقيق والإدعاء العام في المملكة العربية السعودية؟

3.هل توجد علاقة جوهرية بين عناصر أمن المعلومات في المقر الرئيس بهيئة التحقيق والادعاء العام في المملكة العربية السعودية؟

وللإلمام بهذا الموضوع تطرق الباحث إلى مفهوم الأمن المعلوماتي وأهدافه بالإضافة إلى الأخطار التي تهدده مع إبراز الأساليب المتبعة لمواجهة هذه التهديدات والأخطار ،و فيما يخص الجانب التطبيقي فقد طبق هذه الدراسة في هيئة التحقيق والادعاء العام في المملكة العربية السعودية فبين لنا مفهوم التحقيق والادعاء العام ثم انتقل إلى نشأة وتاريخ الهيئة بالإضافة إلى الهيكل التنظيمي لها ليدرس في الأخير واقع الأداء الامني والمعلوماتي بهيئة التحقيق والادعاء العام فيها.

تهدف هذه الدراسة إلى ا لتعرف على سياسة أمن المعلومات وتقنياته في مقر الرئيس بهيئة التحقيق والادعاء العام في المملكة العربية بالإضافة إلى معرفة العلاقة بين عناصر أمن المعلومات ورؤية منسوبي الهيئة لهذه العناصر، وتمثلت عينتها في مجموعة من العاملين في هيئة التحقيق والادعاء العام في المملكة العربية السعودية والبالغ عددهم 205 موظف ،حيث استخدمت الاستبيان كأداة لجمع البيانات بإتباع المنهج الوصفي.

وقد أسفرت هذه الدراسة على النتائج التالية:

1.تطبيق اجراءات سياسات أمن المعلومات والأمن المعلوماتي للموارد البشرية في مقر الرئيس بهيئة التحقيق والادعاء العام بنسبة مرتفعة.

2.وجود علاقة جوهرية بين عناصر أمن المعلومات في مقر الرئيس بهيئة التحقيق والادعاء العام مع بعضها البعض وهي تكاملية تتأثر ببغضها.

3.لا تختلف رؤية منسوبي بالمقر الرئيس لهيئة التحقيق والادعاء باختلاف خصائصهم الديمغرافية مع عناصر أمن المعلومات

الدراسة الثانية:

بعنوان: الأمن المعلوماتي في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة[1]

[1]القحطاني سليمان بن على بن وهف. امن المعلومات في ضوء التطور التقني والمعلوماتي الحديث في الشبكات اللاسلكية النقالة . العلمي الاول حول الجوانب القانونية والأمنية للعمليات الإلكترونية منظم المؤتمر: أكاديمية شرطة دبي .مركز البحوث والدراسات رقم العدد 4. تاريخ الانعقاد: 26 /2003/4 ،تاريخ الانتهاء 2003/4/28 الدولة: دبي، الأمارات العربية المتحددة

جاءت هذه الدراسة لتعالج إشكالية ما واقع الأمن المعلوماتي في البيئة الرقمية ؟وما هي السبل والإجراءات الأمنية لتحقيقه ؟

فتناولت الدراسة بداية بلحمة عن التطور التقني لعالم الشبكات والخدمات وامن الشبكات المحمولة والبعد الأمني لهذا التطور وفي القسم الثاني جاءت الدراسة لتناقش مخاطر أمن المعلومات وحلولها بالإضافة إلى توضيح مفهوم وضع السياسات الأمنية الجيدة لتأمين المعلومات في البيئة الرقمية الإلكترونية

أهداف هذه الدراسة تمثلت في النقاط تالية إلى :

- تعرف على واقع أمن المعلومات في بيئة الإلكترونية في ظل التطور التقني والمعلوماتي الحاصل.
- إبراز مخاطر التي يعاني منها امن المعلومات في بيئة الإلكترونية.
- ضرورة تطبيق سياسات الأمنية لتحقيق أمن المعلومات في بيئة الرقمية.
- تسليط الضوء حول أهمية توفير أمن معلوماتي في بيئة الإلكترونية نظرا للتطور التكنولوجي.

وفي الاخير خرجت هذه الدراسة بمجموعة من النتائج تمثلت في نقاط التالية:

1) ضرورة وضع سياسة أمنية لتطبيق الحماية للمعلومات في البيئة الرقمية للاتصالات
2) وجود مخاطر ومهددات تحول دون تحقيق الأمن المعلوماتي في البيئة الرقمية في اطار الاتصالات.
3) الإمكانيات المادية والبشرية تلعب دورا هاما في الوصول إلى الأمن المعلوماتي داخل مجال الاتصالات

الدراسة الثالثة:

بعنوان: دراسة علمية حول أمن المعلومات في المنظمات السعودية بجامعة الملك سعود بالرياض[1]

هدفت الدراسة استكشاف حالة أمن المعلومات والعمل على تحقيق فهم افضل للحقائق السائدة في هذا المجال داخل مملكة العربية السعودية، استخدمت الدراسة المنهج الاستقصائي باختيار 120 منظمة سعودية كعينة لها حيث تمت الدراسة على مستوى أربعة قطاعات رئيسية وقام الباحثون بتنظيم ورشة عمل لممثلين عن تلك المنظمات المختلفة، كما تم إعداد استبانة تم توزيعها على المشاركين كأداة لجمع البيانات

وأسفرت هذه الدراسة على نتائج التالية :

- أهمية سياسة أمن المعلومات في ضمان اتخاذ العوامل التحكم مناسبة ،كما تبين ان أغلب هذه القطاعات تمتلك هذه السياسة ويميل إلى تطبيقها

[1] سيد عرفان نبي، عبد الرحمن مرزا، خالد الغثبر.2010.دراسة علمية حول أمن المعلومات في المنظمات السعودية ،المملكة العربية السعودية: جامعة الملك سعود، مركز التميز لأمن المعلومات.

- أهمية إرساء الوعي الأمني لدى العمال داخل المؤسسات وذلك من خلال القيام بتدريب المتخصصين والعاملين.
- اعتبار التحكم في الوصول إلى الشبكة أمر حاسما للأمن المعلومات وبينت أن المنظمات على علم وتطبيق لهذه القوانين وخاصة في الشبكات السلكية
- تتسم معالجة قضايا أمن المعلومات بالتميز بين حساسية المعلومات حيث بينت الدراسة اولويات المعالجة لهذه الثغرات وافترضت عدم المساواة في التعامل مع هذه المعلومات فليست كل المعلومات لها نفس القدر من الاهمية .

الدراسات الجزائرية:

الدراسة الأولى:

بعنوان :أمن المعلوماتي وسبل حمايته في الجزائر :دراسة حالة مؤسسة اتصالات الجزائر – سعيدة[1]

تضمنت هذه الدراسة الإشكالية لمتمثلة في : إلى أي مدى يمكن الحديث فيه على أمن المعلومات ومهدداته؟،و ماهي الطرق والتقنيات المتبعة من طرف مؤسسة اتصالات الجزائر لتأمين نظام معلوماتها؟

حيث تم التطرق في الجانب النظري إلى تقديم فصل حول إطار المفاهيمي حول تكنولوجيا المعلومات والاتصالات وأمن المعلومات تم انتقل إلى تقديم مهددات امن المعلومات وأساليب حمايتها

أما الدراسة الميدانية فقد شملت دراسة حالة مؤسسة اتصالات الجزائر بولاية سعيدة.

حيث هدفت هذه الدراسة إلى تسليط الضوء على مختلف الطرق والإجراءات اللازمة للحفاظ على أمن المعلومات من المخاطر التي تهدده ،مستخدما أداتين لجمع البيانات والتي تمثلت الأولى في المقابلة اما ثانية فهي الملاحظة التي تزامنت مع استخدام المنهج الوصفي بالإضافة إلى المنهج التاريخي ومنهج دراسة حالة.

كان من أبرز نتائجها ما يلي:

- يمثل العنصر البشري في أي مؤسسة أحد أهم الموارد وفي نفس الوقت مهدد وخطر على أمن المعلومات.
- انه من الصعب جدا بل من المستحيل الوصول إلى نظام آمن وسري لقاعدة ما بشكل كامل ولكن يمكن القول أننا نسعى للتوصل إلى درجة عالية من الثقة في نظام المعلومات.

[1] بغداد محمد. الامن المعلوماتي وسبل حمايته في الجزائر: دراسة حالة مؤسسة الاتصالات الجزائر –سعيدة- .جامعة سعيدة، 2018. مذكرة لنيل شهادة الماستر في علوم السياسة :تخصص تسيير وإدارة الجماعات المحلية: سعيدة.

- لا يمكن للوسائل التكنولوجية وحدها تحقيق درجة عالية من الأمان في نظام ما بل يجب أن يكون هناك مزيج من العديد من الطرق والأساليب والتقنيات الإدارية قانونية والبشرية.

الدراسة الثانية:

بعنوان : :الأمن المعلوماتي وسبل مواجهة مخاطر في التعامل الإلكتروني دراسة مقارنة[1]

جاءت هذه الدراسة لتعالج الإشكالية التي تتمثل في هل تعتبر الأمن المعلوماتي باستراتيجياته المتطورة سلاح مثالي لحماية المعطيات المخزنة رقميا من مخاطر والتهديدات الإلكترونية أم أنه كشف وانتهى الأمر عن قصور النسبي في توفير التدابير الوقائية ضد تلك التهديدات الأمنية؟

فكان الهدف من هذه الدراسة يتركز حول النقاط التالية:

1. التعرف على العمليات الرئيسية المتصلة بأمن المعلومات
2. التعرف على التوجهات الحديثة لمواجهة ومكافحة جرائم المعلومات والحد منها بوصفها جرائم ارتبطت بالتقنية العرف على المخاطر التي تتطلب الحماية وما نقاط الضعف والاعتداءات في البيئة المعلومات

كما أن هذه الدراسة توصلت الى مجموعة النتائج التي تمثلت في النقاط التالية:

1. تعتبر المعلومة في هذا العصر كنزا عظيم ولاسيما في ظل وجود تكنولوجيا المعلومات.
2. وجوب توفير قدر من الحماية يتناسب مع مستوى اهمية معلومات
3. أهمية العنصر البشري ودورة فعال في حماية المعلومة
4. عدم الاعتماد على التقنيات الأجنبية خاصة بأمن المعلومات وتطوير الحلول الوطنية او على الأقل وضع الحلول الامنية تحت اختيارات

التعليق على الدراسات السابقة:

إن الدراسات السابقة التي تم التطرق إليها لها علاقة جزئية بموضوع دراستي حيث أن الدراسة الأولى والثانية تناول جانب تقنيات أمن المعلومات بحيث أن الدراسة الاولى لأحمد بن علي عبد الله طارش فقد ركزت على تقنيات أمن المعلومات بصفة عامة ومدى مساهمتها في تحقيق الامن المعلوماتي داخل هيئة التحقيق والادعاء العام للمملكة العربية وذلك باستعمال الاستبيان كأداة لجمع البيانات، في حين أن الدراسة الثانية تناولت جانب تقنيات أمن المعلومات لكن من جانب تقنيات المعلومات الاتصالية في شبكة الاتصال بصفة خاصة، ومعرفة واقع الامن المعلوماتي في ظل هذه التطور التقني

[1] دردار نسيمة. الامن المعلوماتي وسبل مواجهة مخاطر في التعامل الإلكتروني دراسة مقارنة، جامعة أبو بكر بلقايد،2016..مذكرة لنيل دكتوراه. تلمسان .

في شبكة الاتصالات اللاسلكية النقالة ،أما الدراسات الثلاث المتبقية فقد ركزت العنصر البشري وذلك لأهمية الكبيرة باعتباره العصب المحرك لكل عمليات الخاصة بأمن المعلومات كونه انه هو من يقوم بتسيير هذه العمليات والتحكم في الوسائل والتقنيات الضرورية لتحقيق الأمن المعلومات أما فيما يخص دراستنا فقد مست تقريبا كل جوانب التي عولجت من قبل فيما جاء في الدراسات السابقة ولكل جوانب أمن المعلومات بداية بالإمكانيات المادية والبشرية الضرورية لتحقيق الأمن المعلومات مرورا بمعايير أمن المعلومات ومدى تجسيدها في مؤسسة الصندوق الوطني للتقاعد ،وصولا إلى مهددات أمن المعلومات وطرق مواجهتها. بالإضافة إلى أنو دراستنا أجريت في مؤسسة الصندوق الوطني للتقاعد التابعة للقطاع العمومي، كما تم الاعتماد على معيار إيزو 27002 لأمن المعلومات لمعرفة درجة الأمن مدى تطبيق هذا المعيار في المؤسسة الصندوق الوطني للتقاعد .بالإضافة إلى اختلاف سنه الدراسة حيث ان الدراسات السابقة تراوحت من عام 2003 إلى غاية 2018. في حين ان دراستي كانت في عام.2019. 2020.

أما نقاط التشابه فقد تمثلت في الجانب النظري لأمن المعلومات كون أن جميع الدراسات درست امن المعلومات من حيث تعريف وأهداف وأهمية ومهدداته ،بالإضافة إلى كون أن معظم الدراسات اتبعت المنهج الوصفي .

صعوبات الدراسة:

- تداخل بين موضوع أمن المعلومات والجريمة المعلوماتية
- ظهور فيروس كرونا وتزامنه مع فترة إجراء الدراسة وما ترتب عنه :

1. صعوبة التنقل إلى كل من المكتبات و مكان إجراء الدراسة
2. قلة دراسات التي تتحدث عن أمن المعلومات في مراكز الأرشيف باللغة العربية

الفصل الأول:

أمن المعلومات

تمهيد الفصل :

بالتطور العلمي والتكنولوجي زادت اهمية المعلومات وجمعها وتخزينها وبثها واسترجاعها ،فأصبح عالم اليوم يسير بطاقة المعلومات فلم تعد الحروب والمال هي المسير لعالمنا ،فهي تعتبر المحرك الاول للمجتمعات، وان حمايتها هو السبيل الوحيد لضمان الاستمرار في هذا الفضاء الذي يعرف بالفضاء الرقمي للمعلومات الذي أصبحت فيه المعلومات ترتب وتخزن في الحواسيب تحول العالم الى بيت عنكبوت،كل هذا أدى إلى إحداث خطر على تسرب هذه المعلومات ووصولها للأشخاص غير المعنيين بها أو المنافسين، وبالتالي أصبحت الحاجة الملحة للحفاظ على أمن المعلومات الذي يعني إبقاء معلوماتك تحت سيطرتك المباشرة والكاملة، أي بمعنى عدم إمكانية الوصول لها من قبل أي شخص آخر دون إذن منك، وان تكون على علم بالمخاطر المترتبة عن السماح لشخص ما بالوصول إلى معلوماتك الخاصةوعلى هذا الأساس تم استخدام مجموعة من التقنيات من أجل ضمان عدم اختراقها من قبل أي جهة كانت وهذا لضمان وصول المعلومات لصاحبها ومن له حق في الاطلاع عليها، يعتبر أمن المعلومات تحديا هاما في مجال التكنولوجيات الجديدة للمعلومات. وبحكم المكانة الهامة التي تحتلها هذه الأخيرة في المجتمعات الحديثة، توسع مجال أمن المعلومات حاليا إلى ميادين الأنظمة والمحتويات والخدمات، و ذلك بهدف الوقاية من الهجمات وتحديدها وتقليصها في هذه الميادين . وتتمثل مهمة أمن المعلومات في ضمان سلامة وسرية وتوفر وسهولة تعقب البيانات ومعالجاتها، وعليه تم معالجة لهذا الموضوع فقد ارتأيت ان تكون البداية بتعريف امن المعلومات وتم التعرف على التطور التاريخي له مرورا بالتعرف على عناصره ومكوناته ثم إنقلت إلى الحديث عن مجالاته،و تحديات الحماية الامنية له،وصولا إلى واهدافه مع التطرق إلى مهدداته واخطار التي يمكن ان يتعرض لها ،و بمعرفة هذه التهديدات لابد من التطرق إلى أساليب مواجهتها و الإجراءات والطرق اللازمة لحمايته، و الآليات الضرورية لتعزيزه واخيرا التطرق إلى المعايير والقوانين المتعلقة به

1- ماهية أمن المعلومات:

1-1 مفهوم الأمن:

1-1-1 لغة:

من مصدر أمن وأمن، يعيش في امن بمعنى طمأنينة ويسر ،و امان بمعنى اطمئنان بعد الخوف.[1] ولقوله صلى الله عليه وسلم ((نعم من دخل دار أبي سفيان فهو آمن ومن أغلق عليه بيته فهو آمن ومن دخل المسجد فهو آمن)

2-1-1 **اصطلاحا** :

لا يخرج استعماله عن الفقهاء عن المعنى اللغوي ضد الخوف ،و الأمانة ضد الخيانة ويقال تقع الأمنة في الأرض أي تمتلئ الأرض بالأمن فلا يخاف أحد من الناس أو الحيوان [2]

1-2- **مفهوم المعلومات:**

1-2-1- **لغة :**

مشتقة من العلم وعلم بالشيء علما أي عرفه واعلم الشيء جعله علامة وتعالم الجميع الشيء أي عرفوه والمعلم يراد به ما يستدل به على الطريق من أثره.[3]

وجاءت كلمة المعلومات للدلالة على التوقيت في قوله تعالى(الحج أشهر معلومات)[4] وكذلك وكلمة علم تعني أدرك الشيء بحقيقته.

1-2-2- اصطلاحا :

هي البيانات التي أجريت عليها معالجة معينة لترتيبها وتنظيمها وتحليلها من أجل الاستفادة منها كما يقول البعض إن كل رسالة قابلة للتوصيل للغير بأي وسيلة مهما كانت تعتبر معلومة.[5]

1-3- أمن المعلومات:

1-1-3 من الناحية الأكاديمية :

هو العلم الذي يبحث في نظريات استراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.[6]

---

[1] معجم المعاني الجامع، معجم عربي عربي.

[2] إبن المنظور. قاموس لسان العرب، دار المعارف ،تونس،1290.م .ص. 163

[3] ضرضام، جابر عطوش آل مواس. جريمة التجسس المعلوماتي . مصر: المركز العربي للدراسات والبحوث العلمية،2017 . ص. 23.

[4] سورة البقرة أية 196

[5] فتوح جمعة، صفاء، مسئولية الموظف العام في إطار تطبيق نظام الإدارة الإلكترونية. مصر : دار الفكر والقانون، 2014،ص. 117

[6] غادة، موسى عبد المنعم. أساسيات تكنولوجيا المعلومات والاتصال. مصر :دار المعرفة الجامعة،2016. ص. 22

2-1-3 من ناحية قانونية:

محل الدراسات وتدابير حماية، سرية، وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها واستغلال نظمها في ارتكاب الجريمة.[1]

3-1-3. من ناحية التقنية:

الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.[2] ومن هنا نستنتج ان أمن المعلومات هو علم قائم بحد ذاته يتطلب أدوات وإجراءات وتدابير وقائية.

1.1 مراحل تطور مفهوم الأمن المعلوماتي

لقد مر مفهوم أمن المعلومات بعدة مراحل بداية من مفهوم أمن الحواسيب وصولا لمفهوم أمن المعلومات ولقد صنف الحميدي وآخرون مراحله إلى ثلاث حقب زمنية على النحو التالي:

- **الستينات :**

في هذه المرحلة كانت الحواسيب هي كل ما يشغل العاملين، بالإضافة إلى كيفية تنفيذ البرامج، فلم يكن العاملين مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة، ولقد كان مفهوم الامن يدور حول تحديد الوصول او الاطلاع على البيانات من خلال منع أي جهة خارجية من التلاعب في الاجهزة، فظهر مصطلح أمن الحواسيب ،والذي يعني حماية الحواسيب وقواعد البيانات.

- **السبعينات:**

في هذه المرحلة تم الانتقال إلى مفهوم أمن البيانات، ويبدأ استخدام كلمات السر البسيطة للسيطرة على الوصول إلى البيانات، بالإضافة لوضع إجراءات حماية لمواقع الحواسيب من الكوارث، كما رافق ذلك اعتماد خطط لتخزين نسخ إضافية من البيانات والبرمجيات بعيدا عن مواقع الحواسيب.

- **الثمانينات والتسعينات :**

في هذه المرحلة ثم الانتقال لمفهوم أمن المعلومات، وذلك نظرا للتطورات في مجال تكنولوجيا المعلومات والتي سمح لأكثر من مستخدم للمشاركة في قواعد البيانات فأصبح من الضروري المحافظة على المعلومات وتكاملها وتوفر درجة موثوقيتها.[3]

---

[1] حسن، أيمن عبد الله فكري. الجرائم المعلوماتية. الرياض: مكتبة الملك فهد،1434 . ص. 117

[2] خالد ممدوح، إبراهيم. أمن المعلومات الإلكترونية. الإسكندرية : الدار الجامعية، 2008. ص. 27.

[3] آن سعيد، إبراهيم عبد الواحد. سياسات أمن المعلومات وعلاقتها بفعالية نظم المعلومات الإدارية. مذكرة ماجستير، تخصص: إدارة أعمال، جامعة الأزهر. غزة،2015. ص15 .16

1-3- عناصر الأمن المعلوماتي:

1-3-1- سرية المعلومات :

وهذا الجانب يشمل جميع التدابير اللازمة لمنع إطلاع غير مصرح لهم باطلاع على المعلومات الحساسة أو السرية وبمعنى التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك[1]. ومن امثلة هذه المعلومات التي يجب سريتها المعلومات الشخصية للأفراد، الميزانية المالية للشركات قبل إعلانها، المعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.[2]

1-3-2- سلامة المعلومات:

ويقصد بها لحماية المعلومات من التغيير والتأكد من أن المحتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره في أي مرحلة من مراحل المعالجة أو سواء في مرحلة التبادل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع.

1-3-3- ضمان الوصول إلى المعلومات :

أن الحفاظ على سرية المعلومات وسلامتها أمر مهم ولا ريب، ولكن هذه المعلومات تصبح بدون قيمة إذا كان من يحق له الاطلاع عليها لا يمكنه الوصول إليها أو ان الوصول إليها يحتاج وقت ويتخذ المهاجمون وسائل شتى لحرمان المستفيدين من الوصول إلى المعلومات ومن هذه الوسائل حذف المعلومات نفسها أو مهاجمة الأجهزة التي تخزن المعلومات فيها وشلها عن العمل، بالتالي يجب التأكد من استمرارية عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات تقديم الخدمة لمواقع المعلوماتية وإن مستخدم المعلومات لن يتعرض لمنع من استخدامه لها أو الدخول لها[3]

1-3-4- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:

ويقصد به ضمان عدم انكار الشخص الذي قام بتصرف ما متصل المعلومات أو مواقعها إنكار انه هو الذي قام بهذا التصرف بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت ما.[4]

1-4- المكونات الأساسية لأمن المعلومات:

1-4-1- أمن الأفراد والإدارة :

وهي الإجراءات التي من شأنها الحفاظ على أمنية مركز الحاسبة وأخطار الأشخاص الغير مخولين من ذلك، التحكم بدخول الأفراد، استعمال هوية ممغنطة...الخ

---

[1] الظاهر، نعيم إبراهيم. طريق نحو الحكومة الإلكترونية. الأردن: عالم الكتب الحديث، 2014. ص 82.

درار نسيمة ،الامن المعلوماتي وسبل مواجهة مخاطر في التعامل الإلكتروني دراسة مقارنة، شهادة لنيل دكتورا في قانون الخاص، جامعة أبو بكر بلقايد، تلمسان .2016.ص 58 [2]

لظاهر نعيم إبراهيم، المرجع السابق ص83 [3]

[4] جمال محمد لينا، الجرائم الإلكترونية. دار خالد الحياني للنشر والتوزيع،عمان،2010،ص 66.

1-4-2- أمن المعلومات والوثائق في مركز الحاسبات :

إن الوثائق والحوامل الإلكترونية (الأقراص فلاش ديسك ..إلخ)ذات السرية العالية يجب حفظها في مواقع خاصة كما ان تصنيفها من حيث أهميتها وسريتها يعتبر من الوسائل المساعدة في هذه الوثائق

1-4-3- أمن بناية مركز الخوادم:

يعني بهذا البند موقع مراكز الحاسبات والتصميم الهندسي لبناية هذه المراكز وكذا اختيار القاعة المخصصة لوضع الأجهزة ومتطلبات الحماية الأمنية لها ثم متطلبات الحماية والأمن للمبنى ككل.

1-4-4- أمن الأجهزة البيئية الخاصة بمركز الخوادم :

يعني هذا البند بأمن أجهزة حفظ الطاقة والتبريد ووسائل الإطفاء الذاتي للحريق وما له علاقة بالأجهزة البيئية.

1-4-5- أمن الاتصالات الخاصة بالحاسبات الإلكترونية:

تعتبر الاتصالات في الوقت الراهن عصب الشبكات وحمايتها بالأولوية بما كان، ويندرج في نطاق أمن الاتصالات تأمين خطوط الاتصال وأجهزته وحمايتها من الاختراق والتجسس.

1-4-6- أمن انظمة التشغيل والبرمجيات :

تسعى المؤسسات لاتخاذ إجراءات واحتياطات أمنية لضمان سلامة أنظمة التشغيل[1]

البرمجيات وجعلهما يمتلكان أساليب دفاعية ضد محاولات التدخل غير المشروعة أو تخريب بكافة أشكاله، ومن بين الإجراءات المتخذة في هذا الجانب استعمال كلمات السر او المرور، جدول الصلاحيات ،التوثيق والنسخ الاحتياطي.

1-4-7- أمن أجهزة الحاسبات الالكترونية :ويقصد بها الإجراءات المتخذة في تأمين الأجهزة الطرفية وملحقاتها المادية كالطابعات وقارئ الأقراص المتعمدة.[2]

2- أمن المعلومات بين القدرات والتحديات

2-1. مجالات الأمن المعلوماتي :

يتمحور أمن المعلومات في عدة مجالات نذكرها في النقاط التالية والتي تتمثل فيما يلي:

2-1.1. أمن حفظ البيانات والمعلومات :و تشمل على ما يلي:

- **مكان حفظ :**

من خلال وجودها في مواقع آمنة مثل مراكز المعلومات والتي يجب ان تخضع لرقابة دقيقة بحيث لا يصل إليها إلا من هو مصرح له من خلال بوابة آمنة.

---

[1] مقراني، قدور. تقييم مدى مساهمة أمن المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات: دراسة حالة مؤسسة اتصالات الجزائر. ماستر أكاديمي طور الثاني: تدقيق ومراقبة التسيير، جامعة قاصدي مرباح ورقلة الجزائر،2015. ص.14

[2] مقراني، قدور، المرجع نفسه. ص 15.

- **طريقة حفظ :**

وذلك بإتباع التقنيات المتقدمة في انظمة تشفير المعلومات المحفوظة بمختلف أنواع التشفير بالإضافة إلى برامج خاصة مساعدة للتشفير ومن اشهرها.

- **المواد التي تحفظ عليها البيانات :**

من خلال الحفظ على انسب وسائط تخزين مناسبة في بيئات الحفظ المناسبة.

2.1-2 أمن نقل المعلومات والبيانات:

قديما كانت تستخدم آليات النقل الفيزيائي المباشر للبيانات وتحاط بسرية وحماية وتتم ببطيء نسبي لكنها كانت وأكثر أمنا وبعد التقدم التقني اصبحت آليات النقل الحديثة حيث تميزت بسرعة في نقل المعلومة والدقة هي الأنسب عند أخد الاحتياطات اللازمة في العمليات نقل البيانات ولذا نرى في هذا يهتم بالبيئات الآمنة لنقل البيانات والمعلومات من خلال:

- التطبيقات المستخدمة والبروتوكولات مناسبة.
- أمن نظم الاتصالات وبيئات النقل المستخدمة.

2-1-3. البحث عن مصادر الخطر المتوقعة على المعلومة لمكافحتها:

تعتبر مصادر الخطر على أمن المعلومات كثيرة جدا ولعل من اهمها خطورة الوصول إليها وبالتالي يتم تسريب المعلومات او إتلافها ويمكن لهؤلاء ان يستعينوا بالعديد من الوسائل التي توصلهم للمعلومات وتمكنهم من اتلافها وذلك بعدة طرق ومن بينها :الاختراق او الفيروسات.[1]

2-2. تحديات التي يواجهها أمن المعلومات:

1. التحديات القانونية :

نقص التشريعات القانونية في هذا المجال إلى جانب عجز معظم هذه القوانين عن التمييز بين القيمة الحقيقة للمعلومات والقيمة المادية للأوساط التي استخلصت منها المعلومات.

2. التحديات الفنية :

نقص التحديثات والتطويرات في الكثير من اجراءات الحماية المتبعة حاليا سواء ما يتعلق بإجراءات الحماية للوصول غير مخول أو إجراءات التشفير.

3. التغاضي عن الكثير من المخاطر والانتهاكات أو التصغير من شأنها إذا كان تأثيرها على العمليات اليومية العادية ضئيل ومحدود.

4. التحديات التقنية :

1. تتمثل في الحاجة إلى المعدات والبرمجيات وإلى تطوير الإمكانيات في هذا المجال
2. افتقار المعايير والمقاييس العالمية الموحدة. و قلة الرقابة من الجهات المختصة في ذلك.

[1] العامري، اسامة موسى. اتجاهات إدارة المعلومات. عمان، دار أسامة للنشر والتوزيع،2010. ص.58.59.60. 61.62

3. نقص مؤهلين وأخصائيين وخبراء في أمن المعلومات.[1]

2-3. أهداف أمن المعلومات:

- التأكد وبصفة مستمرة أن المعلومات متوفرة وبعيدة عن أي تهديد يعرضها للتلف أو السرقة.
- التأكد من سرية المعلومات والذي يهدف إلى أن تكون هذه المعلومات في معزل عن تدخل أي شخص غير مصرح له بالاطلاع عليها سواء كان من داخل الهيئة أو من خارجها.
- نزاهة المعلومات وذلك عندما تكون مستخرجة من نظام معلوماتي دقيق وموثوق.[2]
- الهدف الرئيسي لأمن المعلومات هو حماية نظام المعلومات ومكوناته في المؤسسة والتأكد من عدم تعرضها للمخاطر وإتاحتها لأشخاص غير معنيين بها.
- التكامل في الحفاظ على المعلومات بصورتها الأصلية دون السماح لأي شخص بالعبث فيها. [3]
- التأكد من صحة المعلومات بهدف مراجعة المعلومات المتوفرة للتأكد من سلامتها من أي خطأ
- عليها بقصد او بدون قصد، سواء كان هذا الخطأ من العاملين عليها أومن الأجهزة نفسها.
- التوفر بشكل دائم للمعلومات والأنظمة الحاسوبية والعمليات الأمنية بحيث تعمل بشكل سليم عند الحاجة لها، وذلك بعد تطبيق العمليات الخاصة بأمن المعلومات.[4]
- حفظ فعالية وكفاءة نظم المعلومات.
- تسهيل استغلال تكنولوجيا المعلومات بأقصى طاقاتها وإمكانياتها.
- حماية حقوق واهتمامات كل المعتمدين في التعامل معها.[5]

2-4. مهددات وأخطار أمن المعلومات:

2-4-1. المخاطر المادية:

هي المخاطر الناجمة عن الوصول المادي لمكونات نظام أمن المعلومات أو تلف في الموارد المتاحة لأمن المعلومات وتشمل الضرر الذي تسببه الطبيعة من كوارث طبيعية محتملة على المنشأ المعلوماتية أو السرقة أو الحريق وغيره من الحوادث الطارئة مما يتسبب في ضرر دائم للبيانات التي تحويها هذه المنشأة ويمكن تقسيمها إلى قسمين رئيسين:

---

[1] مأمون العزب، أمن المعلومات في فضاءات الانترنت الأشياء، مجلة التقدم العلمي، ع 99. كويت، 2017. ص. 12.

[2] أحمد حسني صالح عوض الله. أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعات الأردنية. مذكرة دكتورا، جامعة السودان للعلوم والتكنولوجيا، 2018.ص 51.

[3] طارس، أحمد بن علي عبد الله. رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية. مذكرة الماجستير: الدراسات الاستراتيجية .جامعة نايف العربية للعلوم الأمنية،الرياض،2015،ص41.

[4] طارس، أحمد بن علي عبد الله، المرجع نفسه.ص42.

[5] أحمد حسني صالح عوض الله. المرجع السابق. ص 51.

❖ **مخاطر الطبيعية :**

يقصد بها الكوارث الطبيعية التي ليس للإنسان أو التجهيزات الفنية دخل في حدوثها كالزلازل والبراكين والفيضانات والصواعق والحرائق وموجات الغبار العاتبة، و قد تلحق مثل هذه الكوارث أضرار كبيرة بأنظمة المعلومات وقد يؤدي إلى انقطاع الخدمات الإلكترونية نهائيا في حال إصابة المراكز الرئيسية لتقديم المعلومات من خلال الخدمات.[1]

❖ **المخاطر البيئية الطارئة :**

تحدث هذه المخاطر من خلال اختراق مقاييس الأمن الطبيعية نتيجة سوء استخدام للمكونات المادية لنظام أمن المعلومات مثل أجهزة التكييف أو بسبب غبار والأتربة وغيرها من العوامل التي تؤثر عن أماكن تخزين المعلومات من الاهتمام المباشر في الأماكن المخصصة لها أو غير المباشرة من خلال نقاط الربط الجوهرية خارج نظام أمن المعلومات أما إمدادات كهرباء أو قنوات الاتصال عن بعد ويمكن أن تؤدي إلى تعطيل العمل وتوقفه لفترات طويلة مما يؤثر على أمن وسلامة المعلومات.[2]

2.4.2. **المخاطر التقنية (الفنية)**

وهي التهديدات الناجمة عن القصور والأخطاء الفنية في مختلف انظمة أمن المعلومات والتي يغلب عليها الطابع الفني دون أن يكون هناك أي تدخل بشري أو تكون بسب كارثة طبيعية ومنها:

▪ **تهديدات غيوب التشغيل والتصميم:**

وتشمل عيوب التصميم في الأجهزة والبرامج والشبكات وأدوات الربط والتخزين أو أي مكون آخر من مكونات الأنظمة المعلوماتية وهنا تبرز أهمية تصميم البيئة التحتية لتقنية المعلومات وأمن المعلومات كالبنية التحتية لخوارزميات التشفير ومفاتيحه ولا تقل أخطار عيوب التشغيل عن أخطار عيوب التصميم في إمكانية النفوذ إلى المعلومات بصفة غير شرعية أو التسبب في فقدانها بسبب خطأ التشغيل قد يكون بسيطا ومن الأمثلة عن ذلك فتح منافذ اتصال بدلا من إغلاقها أو نسخ المعلومات إلى أماكن خاطئة أو توجيهها إلى غير وجهتها الصحيحة ناهيك عن التهديدات المتعلقة بأخطاء النسخ الاحتياطي كأخذ نسخة احتياطية لجزء من المعلومات فقط أو استعادة معلومات قديمة بدل من المعلومات الحديثة عند إجراء عملية الاستعادة للمعلومات التي سبق أخذ نسخة احتياطية لها.

▪ **تهديد التشتت المعلومات:**

إذا كانت معلومات المنشأة مشتتة ومخزنة في أماكن كثيرة ويجري التعامل معها من خلال شبكات متعددة بتعدد أماكن وجود هذه المعلومات وهو ما يتسبب في ضعف منظومة أمن المعلومات وتشتتها وكذلك زيادة تكاليف توفيرها وإدارتها والسيطرة عليها ويؤدي هذا الأمر إلى نوع من تناثر وتعدد

[1] الطائي، محمد عبد المحسن. إدارة أمن المعلومات. عمان: دار الثقافة للنشر والتوزيع، 2010. ص 55.

[2] فاروق، عزة عبد المعبود، الجوهري، حسن طه محمد طه. أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم مكتبات والمعلومات، مج 6 ،ع 12 ،يونيو 2019.ص 11.12.

تطبيق مفاهيم أمن المعلومات وقد يتسبب في وجود ولو ثغرة أمنية واحدة في الأماكن يمكن النفاذ من خلالها إلى كامل منظومة المعلومات في المنشأة.[1]

- **خلل في المعدات:**

تضمن أعطال أجهزة الحاسوب والطرفيات والتجهيزات الشبكية المرتبطة بالنظام وهذا النوع من الأعطال يتسبب في توقف النظام عن العمل وحجب الخدمة عن المستفيدين.[2]

- **أخطاء البرمجيات :**

قد تحتوي البرمجيات المستخدمة لأمن المعلومات على العديد من الأخطاء الأمر الذي ينعكس على امن المعلومات وبالتالي على دقة المخرجات وصحة المعالجة التي يقوم بها النظام ويتم ذلك عن طريق استخدام برامج غير أصلية أو نسخ مقلدة منها بطريقة غير شرعية.

- **أخطاء البيانات:**

يتعلق بأخطاء إدخال البيانات في نظام أمن المعلومات بحيث يتم إدخال البيانات غير صحيحة مما ينعكس على دقة المعلومات المستخرجة في عمليات الاسترجاع.[3]

2.4.3. **المخاطر البشرية :**

ترتبط غالبا بجهل وقلة وعي عمال المؤسسة أكثر من رغبتهم في إلحاق الضرر بها وعادة ما تنتج هذه التهديدات من الاستعمال الشخصي من قبلهم لأجهزة المعلوماتية المخصصة، للعمل وهذا ما يعرضها إلى خطر الإصابة بالبرامج الخبيثة .[4]

التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو عمليات التجميع للبيانات أو إدخالها للنظام أو في عمليات تحديد الصلاحيات للمستخدمين، لأن أمن المعلومات أولا وأخيرا على يعتمد على أمانة الأفراد المتعاملين معه فلا يكفي التأكد من أخلاقيات الموظف وأهميته عند تشغيله بل يجب أن تستمر مراقبته لأن التغيير السلوكي متوقع في أي وقت وكذلك يجب عدم الاعتماد على موظف واحد بأي حال من الاحوال وإن كان لابد من ذلك فيجب أن يشمل ذلك الموظف على مراقبة دقيقة وتوثيقا لأعماله وأن يكون هنالك تدريب لمساعدين لهم وعند انتهاء خدمات أي موظف يجب سحب صلاحيته قبل فترة كافية فهنالك عدة حوادث انتقام من موظفين أنهيت خدماتهم[5]

وتشمل تهديدات التي تصدر من العنصر البشري في:

---

[1] القحطاني، ذيب بن عايض. أمن المعلومات. الرياض : مدينة الملك عبد العزيز للعلوم والتقنية ،2015. ص..61.62.

[2] شوابكة، عدنان عواد. دور إجراءات الأمن المعلومات في الحد من مخاطر أمن المعلومات في جامعة الطائف. في: مجلة دراسات وأبحاث، مج 11،ع 04،أكتوبر 2019.ص 169.

[3] قدايفة، أمينة. استراتيجية أمن المعلومات ،محاضرة: .جامعة أمحمد بوقرة بومرداس، الجزائر ص 168.

[4] نوفيل، حديد، كريبط، حنان، أمن المعلومات ودورة في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة . المؤسسة،ع03، 2014. ص. 190.

[5] بربار، نور الدين. دور الأمن المعلوماتي في تفعيل نشاط الصيرفة الإلكترونية. مجلة الاقتصاد والتنمية ،ع 02، 2014،ص 17. 18

- **التصرفات الخاطئة من قبل العاملين:**

▪ يضم هذا النوع الأفعال والتصرفات غير المتعمدة والتي يتم أداءها بواسطة الأفراد موثوق بهم داخل المنظمة ومرخص لهم التعامل مع أنظمة المعلومات حيث تؤدي أفعالهم إلى حدوث أخطاء ومشكلات عند تعاملهم مع هذه الأنظمة ويعود ذلك إلى عدة عوامل منها قلة الخبرة والتدريب الكافي للعمل في نظام المعلومات ومن بين هذه الأفعال نجد:

- عرض المعلومات الحساسة ،
- إدخال، حذف أو تعديل المعلومات عن طرق الخطأ[1]

- **الأفعال المتعمدة (المدروسة):**

التهديدات التي تهدف إلى إلحاق الضرر بالمنشأة وأنظمة المعلوماتها ومواردها وتتمثل في:

1- **أفعال تعدي المقصودة:**

يمثل هذا النوع فئة واسعة من الأنشطة البشرية والإلكترونية التي يمكن أن تؤثر سلبا على سرية وخصوصية المعلومات ،و عندما يصل أحد الأفراد غير مرخص لهم على المعلومات التي تعمل المنظمة على حمايتها يعتبر هذا التصرف تعدي مقصود ويعتبر مرتكبه مثل المجرم.

2- **أفعال الابتزاز المقصودة:**

يمثل هذا النوع من الأفعال المعتمدة مهددا للسرية عن طريق استخدام المعلومات كوسيلة للضغط على المنشأ أو ابتزازها من أجل تحقيق غرض معين خاص بالجاني مثلا :أن يقوم شخص بالحصول على معلومات حساسة جدا عن المنظمة ثم يهدد بإفشائها إذا لم يدفع له مبلغ مالي ما.

3- **أفعال التخريب المقصودة:**

ينشأ هذا النوع من المهددات من وجود أفراد أو عدة أفراد يريدون تخريب أو تدمير نظام الحاسوب

أو أداء عدد من الأفعال الضارة بأصول المنشأة المعلوماتية وسمعتها مثلا :تعريض موقع الويب للتخريب أو إلحاق الضرر به ومثل ذلك الفعل يؤدي إلى التأثير على صورة المنشأ وفقدان الكثير من أرباحها وعملائها نتيجة لفدان الثقة فيها من قبل الزبائن.

4- **أفعال السرقة المقصودة:**

يمثل هذا النوع من الأفعال تهديد كبيرا للمنظمة حيث تتعرض مكونات نظم المعلومات للسرقة وربما ما يتعرض للسرقة مكون مادي مثل تغيير في ذاكرة الحاسوب أو المعالج وقد يكون مكون

[1] الدنف. أيمن محمد فارس. واقع إدارة أمن نظم المعلومات في الكليات تقنية بقطاع غزة وسبل تطويرها. ماجستير إدارة الأعمال جامعة الإسلامية غزة ،2013،ص 68.

إلكتروني مثل البرامج أو البيانات ويمكن التحكم في السرقة المادية بسهولة بإحكام الإغلاق للأبواب واستخدام أجهزة التنبيه ولكن يصعب التحكم في السرقة الإلكترونية.[1]

ويشمل الأمن البشري في أي منشأة معلوماتية بشكل عام على:

- **المستخدمون:** هم المستفيدين من المعلومات الموجودة في المنشأة المعلوماتية.
- **مستعملي الخدمات المعلوماتية:** هم الأشخاص الذين يديرون نظام المعلومات.
- **المبرمجين:** هم المسئولين عن برمجيات الحاسوب المتعلقة بأمن المعلومات
- **الزائرين:** الأشخاص الذين لهم حق الاطلاع فقط على المعلومات دون التدخل فيها.
- **مهندسي المعلومات:** هم المنوط لهم بتشغيل تطبيقات المعلوماتية وإصلاح الأخطاء [2]

يكون التهديد الداخلي عن قصد وذلك لعدة أسباب:

- إثبات الشخص مهاراته الفنية وقدراته على تنفيذ الهجوم الالكتروني :هناك أشخاص يشعرون بالفخر إذا ما تمكنوا من اختراق مواقع على شبكة الانترنت أو وصلوا إلى قواعد بيانات محمية.
- **عدم الرضا :**

مهما كانت مسبباته فإن التقنيات الحديثة جعلت من مهاجمة نظم المعلومات أمر يشعر بالانتقام للذات ويشعر بالبهجة في نفس الشخص الذي نفذ الانتقام.

- **تحقيق المكاسب المالية:**

عن طريق سرقة معلومات واستخدامها ا لاحقا لابتزاز الجهة معينة لدفع فدية مالية.[3]

2.4.4. **المخاطر الإلكترونية:**

تقع مخاطر الإلكترونية في الغالب من قبل أشخاص ليس لهم علاقة به أو صلاحيات الدخول وتكون هذه الاعتداءات عبارة عن قرصنة المعلومات واختراق الضوابط الأمنية للنظام بهدف الحصول على المعلومات لها طابع السرية حيث تكمن خطورة تلك المخاطر في عدم معرفة من قام بالاختراق وماهي حدود قدرته في التخريب بالإضافة إلى عدم معرفة الهدف من وراء هذه الاختراقات.[4]

منذ وقت قريب كانت المخاطر الإلكترونية تتعلق بتقنيات الحاسب الآلي ونظم المعلومات وما يتعلق بالمعالجة الآلية للمعلومات حيث كانت تدور هذه المخاطر حول التلاعب في البيانات المدخلة

---

[1] بغداد، محمد. الأمن المعلوماتي وسبل حمايته في الجزائر. مذكرة ماستر تخصص تسيير وإدارة الجماعات المحلية. جامعة سعيدة،2018.ص 52.55

[2] جوهري عزة فاروق عبد المعبود، طه محمد طه حسن. أمن المعلومات رقمية وسبل حمايته في ظل التشريعات الراهنة .في مجلة المركز العربي للبحوث والدراسات في علوم مكتبات والمعلومات. مج 6،ع 12،يونيو 2019.ص 11.12.

[3] نوفيل حديد، كريبط حنان، أمن المعلومات ودورة في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة ،المؤسسة، ع03، 2014، ص 190.

[4] القحطاني، منصور بن سعيد. مهددات الأمن المعلوماتي وسبل مواجهتها: دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية المملكة العربية السعودية. رسالة ماجستير :تخصص تسيير وإدارة الجماعات المحلية، جامعة نايف،الرياض،2008.ص 55.

للحساب الآلي والاعتداءات التي تقع على المخرجات وسرقة البيانات عن طريق الاختراق يمكن تصنيفها إلى ثلاث أنواع وهي الجريمة المحوسبة ،سوء استخدام لجهاز الحاسب الآلي، الجرائم المتعلقة بالحاسب الآلي.[1]

2.4.5. مهددات البنية التحتية:

1.2.4.5 القرصنة

القرصنة: يمكن هنا أن نعرف مفهومين يتعلقان بها وهما :

- القرصان بمعنى أي شخص يحاول الوصول غير المشروع إلى أنظمة الحاسوب
- المخرب اي شخص الذي يستفيد من المعلومات التي يقدمها القرصان للقيام بأفعال تخريبية عدائية.[2]
- بحيث تعتبر عملية الدخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية بقصد المساس بالسرية أو المساس بسلامة المحتوى عن طريق القيام بتعديل أو تخريب أو إلغاء له ،ومن أمثلتها القيام بعمليات قرصنة المواقع الإلكترونية أو بتعطيل الحواسيب الخادمة من خلال إغراقها بالبيانات.[3]

يقوم بعمليات القرصنة أشخاص هواة ومحترفون تم تعريفهم بـ :

((أشخاص لهم القدرة على التعامل مع أنظمة الحاسب الآلي والشبكات بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة الحماية ويمكن تصنيفهم إلى فئتين))[4] هما:

1- **الهاكر:**

هو خبير في اختراق أجهزة الكمبيوتر وهو شخص ماهر في التعامل مع الشبكات بدافع الفضول وهو غير مؤذي وذلك لمجرد سعادته بالتغلب على التحدي المتمثل في التغلب على نظام الحماية والامن التي تستعمله المؤسسة.

2- **كراكرز:**

شخص يخترق النظم الأمنية بغرض السرقة أو إفساد البيانات أي أن هدفه تخريبي وإجرامي.[5]

---

[1] معاذ. أحمد عبد الرزاق. أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة سودان :جامعة أم درمان الإسلامية معهد البحوث والدراسات العالم الإسلامي . أطروحة ماجستير،2016

[2] شهيدي، أمحمد بن الدين محمد. أمن الشبكات من مخاطر التهديدات الالكترونية ودوره في تعزيز التجارة الالكترونية جامعة أدرار، 2006.ص8

[3] فيصل محمد عبد الغفار. الحرب الإلكترونية، دار الجنادرية للنشر والتوزيع،عمان.2016.ص 10.

[4] بغداد محمد. ،المرجع السابق. ص 48.

[5] بالمفلح، فاتن سعيد. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى. السعودية: جامعة الملك عبد العزيز. متاح على الرابط http://www.kau.edu.sa تاريخ الاطلاع 2019/11/12.على الساعة:22.10ص 05.

❖ **دوافع المجرم المعلوماتي : (كراكرز، الهاكرز)**

1. العبث أو اللهو:

من الصعب التفريق بين دوافع العبث واللهو وتحقيق المصلحة الشخصية فهما وجهان لعملة واحدة الاولى تعني بضرورة وجود الثانية، فهما من الدوافع المتوفرة في أغلب الجرائم المعلوماتية.[1]

2. الرغبة في الانتقام:

قد يكون المقدم على ارتكاب الجريمة المعلوماتية له الرغبة في الانتقام، فهو من الغرائز البشرية فكثير من الأفراد يفصلون من عملهم تعسفا، فإذا كان ذلك الشخص حائزا على المعلومات متعلقة بسير النظام المعلوماتي وكان على قدر من الكفاءة في مجال المعلوماتية فتجده يرتكب جريمة رغبة منه بالانتقام من المؤسسة.

3. تحقيق الربح المادي:

تعتبر من الدوافع الرئيسية لدى مجرمي المعلوماتية فأمر اكتشاف ثغرة في نظام المعلوماتي هو السبيل المباشر لغرض تحقيق منفعة مالية بصفة غير مباشرة.

4. الدافع الإيديولوجي: La Activismes

ظهر مصطلح هاكتيفيزم من خلال الدمج بين المصطلحين هما الهاكرز Hackers والنشاط Activisme وذلك على يد مجموعة c ult of the Dead Cow سنة 1994 بحيث يقومون بتعطيل كل المواقع الالكترونية التي تدعو إلى العنصرية مع الدفاع على مبادئ احترام الحرية الاتصالية فهم يتولون الدفاع عن الفئة الضعيفة داخل البيئة الالكترونية.

2.2.4.5. **الاختراق:**

هو القدرة على الوصول إلى هدف معين بطريقة غير مشروعة عن طريق ثغرات أمنية في نظام الحماية الخاص، فحينما يتم الدخول إلى الجهاز يعتبر المخترق هنا هاكر أما عندما تتم عملية التخريب والحذف والسرقة وانتهاك سرية وخصوصية فهنا يعتبر كراكرز.

وعليه فالاختراق هو قيام أي شخص بمحاولة الوصول إلى أي جهاز أو شبكة خاصة بمجال بحث ما وهذا باستخدام برامج فك الشفرة وكسر كلمات المرور والحواجز الأمنية لاكتشاف مواطن الضعف والقوة بالجهاز أو شبكة المعلومات التي تتصل بها.[2]

■ **أنواع الاختراق:**

1. اختراق الخادم والأجهزة الرئيسية:

ويكون المؤسسات أو الجهات الحكومية وذلك عن طريق اختراق الجدار الناري بعملية

[1] ربيعي، حسين. المجرم المعلوماتي –شخصيته وانصافه. مجلة العلوم الانسانية جامعة محمد خيضر بسكرة، ع40، جوان 2015، ص291.292

[2] بن ضيف الله، فؤاد. أمن المعلومات ضرورة معرفية أم ترف تكنولوجي. مذكرة دكتورا. جامعة باجي مختار، عنابه ص 158.

تدني المحاكاة والتي تعني انتحال شخصية للدخول إلى النظام إذا أن عنوان IP يحتوي على عناوين المرسل والمرسل إلية وهذه العناوين تشكل مادة أساسية وثغرة كبيرة للمخترقين

2. **اختراق الأجهزة الشخصية :**

واستراق ما تحتويه من معلومات من معلومات وتعد هذه الطريقة شائعة جدا من قبل الهواة والمخترقين.

3. **التعرض للبيانات أثناء انتقالها :**

من خلال التعرف على شفرتها في حال كونها مشفرة وهذه الطريقة شائعة لدى المخترقين الذي يحاولون سرقة أرقام بطاقات الائتمان البنكية وكشف الأرقام السرية لها. [1]

3.2.4.5. التزوير:

هو التعديل بطريقة ما في البيانات لصالح المخترق أو من يعمل لصالحه مما يسبب مشاكل للمؤسسة فإنه يمكن أن ينطوي على تعديل بمهارة بإضافة بيانات أو تعرض لنظام الحوسبة مثل تعديل في المعاملات أو إدخال ملفات إضافية على قاعدة البيانات.[2]

3.2.4.5. الاقتحام أو التطفل:

إن عملية اعتراض المعلومات التي يتم نقلها من قبل الأطراف من قبل طرق غير شرعية وغير مصرح له هي نوع من عملية كشف وفضح سرية المعلومات حيث يقوم هذا الشخص غير مصرح به بالتصنت واستراق السمع أو يقوم بعملية تصفح لملف ما أو نظام معلومات وهذا النوع من الخرق الأمني يسمى بخرق الأمني الخاص وذلك لأنه لا يشمل عملية تغيير البيانات. إن عملية التصنت السلكية على المكالمات الهاتفية هي أيضا نوع من أنواع التطفل وفيها يتم مراقبة شبكة الاتصالات وكشف كافة المعلومات والأسرار [3] ويذكر ثلاث أصناف وهم :

1. **المتنكر** :

وهو فرد غير مخول باستخدام الحاسوب ويخترق السيطرة بالوصول للنظام للاطلاع على امتيازات المستفيدين وهو على الدوام يكون من خارج المؤسسة.

2. **الفضولي:**

هو مستفيد مخول يصل إلى البيانات وملفات والبرامج أو هو المخول له بالوصول لكنه يسيء الاستخدام من أجل مصلحته الشخصية وهو بصورة عامة من داخل المؤسسة.

---

[1] العوادي،أوس مجيد غالب. الأمن المعلوماتي السبيراني. مركز البيان للدراسات والتخطيط،2016،ص 20.

[2] أمن المعلومات في المؤسسات. في:مجلة تكنولوجيا الاتصالات والمعلومات،2017.متاح على الرابط:
http://www.titmag.net.ye أطلع عليه يوم :2019/09/07.على الساعة 11.29

[3] الطيطي، خضر مصباح إسماعيل. أساسيات أمن المعلومات،2010.متاح على الرابط :
http://www.books.goole.dz أطلع علية يوم :2020/01/25 .على الساعة :13.20.ص32.

3. **المستخدم السري:**

هو مستخدم يسطر على الاشراف للنظام ويستخدمها من أجل تغيير التدقيق وسيطرة الوصول او للتهرب من مجموعة التدقيق ويمكن أن يكون من خارج أو داخل المؤسسة.[1]

5.2.4.5 **عرقه وحجب الخدمة:**

يقصد به هنا الإضرار المادي بالنظام لمنع تقديم الخدمة حيث يقوم المهاجم في هذه الحالة باستخدام برامج تقوم بإرسال عدد هائل من حزم البيانات العبثية بهدف منع أجهزة شبكة المعلومات من العمل وبالتالي حجب الخدمة عن المستخدمين الشرعيين مما تؤدي إلى أذى شديد وخسارة كبيرة وهذا النوع من الهجوم لا يستفيد منه القائم به ولا يجني من وراءه أي مكسب[2] .

1. **الهندسة الاجتماعية:**

تعتبر فن اختراق العقول وهي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما ،بحيث تستخدم أحيانا ضمن احتيال الأنترنت لتحقيق الغرض المنشود من الضحية حيث تهدف إلى طرح أسئلة بسيطة أو تافهة ومن ثم تهدف إلى فإنها تخرق العقل بدلا من التركيز على الجهاز الآلي وتتعلق بالبحث عن قيام الفرد بعمل محدد[3]

بحيث يحتوي هذا الأسلوب على عدة تقنيات وهي:

- **التوأمة الشريرة :**

أي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضار به.

- **سرقة الهوية:**

ادعاء جهة ما بأنها جهة أخرى معروفة للمستخدم حيث يتم منه طلب بتقديم المعلومات بشكل مباشر.

- **التصيد :**

ويقصد منه وصول رسالة مزيفة من جهة لطلب معلومات أو التحقق منها ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.[4]

---

[1] مسعودي، عبد الهادي، الأعمال المصرفية الإلكترونية : Electronic Banking،اليازوري،2016،ص 120. متاح على الرابط: http://www.books.google.dz أطلع عليه يوم 17/02/2020. على الساعة 20.15.

[2] قماز، شعيب، صحراوي،عبد العزيز. الحكومة الإلكترونية ومساعي استتباب الأمن المعلوماتي: الإمارات العربية المتحدة نموذجا. مجلة الحقوق والعلوم السياسية.ع 11 جانفي 2019.ص 300.

[3] عبد الصادق، عادل. الفضاء الإلكتروني والثورة في شؤون أجهزة الاستخبارات الدولية. القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، 2013.ص 20.

[4] الفتال، حميد ناصر، صادق، دلال. أمن المعلومات. عمان: دار اليازوري للنشروالتوزيع،2008.ص 15

7.2.4.5 الفيروسات والبرمجيات الضارة:

1. **البرمجيات الضارة :**

هي برامج متخصصة لتسهيل التسلل غلى نظام أو الشبكة بهدف تدميرها وما ان يتم تثبيت البرمجية الضارة فعنه يصعب إزالتها كما إنها تحتوي على عدة تقنيات أهمها:

- **.برامج التجسس:**

هي برنامج تقوم بتتبع والتجسس على سلوك الجهاز من الكتابة الى مراقبة المواقع التي يزورها.[1]

المستخدم للحاسوب ولذلك سرقة المعلومات السرية ،كما انها غير مصمم لتدمير الحاسوب فهي برامج تدخل لجهاز الحاسوب بدون اذن وتقوم بالتخفي وكما انها تسبب تغيرات غير مرغوب بها وليست متوقعة بالنسبة للمستخدم مثلا :تسبب بإظهار مشاكل في الجهاز مثل عدم قدرة المستخدم الكتابة على القرص الصلب.[2]

ومن أنواعها نجد:

1. **مسجلات ضربات المفاتيح:**

هو عبارة عن نظام أو برنامج يقوم بمراقبة وتسجيل كل حرف يتم كتابته بواسطة لوحة المفاتيح كما يمكن أن يقوم أيضا بالتقاط وتسجيل لقطات للشاشة يمكن تصنيفها إلى نوعين هما:

- **Hardware keylogger:**

عبارة عن جهاز صغير يتم وصله بين لوحة المفاتيح ومنفذ في جهاز الحاسب ويقوم بتسجيل كل حرف يتم كتابته بواسطة لوحة المفاتيح.

- **Key cobra:**

يسجل كمية كبيرة من ضربات المفاتيح ويمكن أن يسجل أكثر منم مليون صفحة ويقوم بحفظها وتنظيمها داخل ملف نظام.[3]

❖ **طرق الحماية من البرنامج التجسس:**

1) استخدام برامج خاصة للبحث عن البرامج التجسس.
2) تحديث نظام التشغيل والبرامج المهمة بشكل دوري.
3) الحرص على عدم تثبيت البرامج المجانية لأنها تكون غالبا مصحوبة ببرامج التجسس.[4]

---

[1] الشنيفي، نوف علي. البرامج التجسسية spyware أنواعها وطرق الحماية منها. بوابة كنانة اونلاين،2011،متاح على الرابط : http://www.kenanaonline.com أطلع عليه يوم:2020/03/19 على الساعة:19.54.

[2] الشنيفي، نوف علي؛ المرجع نفسه.

[3] طويلة، جميل حسين. البرمجيات الخبيثة، MALWARE سوريا ص 10.13.14

[4] الشنيفي، نوف علي، البرامج التجسسية spyware أنواعها وطرق الحماية منها، المرجع السابق.

▪الفيروسات:

تم إطلاق اسم الفيروسات على عائلة متنوعة من البرامج الماكرة وهي Malware وهي مشتقة من عبارة Malicieuses-logic software ويمكن تصنيفها إلى اربعة فئات رئيسية وهي الفيروسات والدودة وأحصنة طروادة بالإضافة إلى برامج الإنزال [1]

الفيروس هو عبارة عن برنامج تطبيقي دخيل يتم تصميمه من قبل أحد المخربين لتحقيق هدف محدد يرتكز في إحداث ضرر معين في نظم الجهاز.[2]

وهي تتمثل في الأنواع التالية:

❖ **أنواع الفيروسات :**

●حصان طروادة :

هي عبارة عن برامج فيروسية لديها القدرة على الاختفاء داخل برامج أخرى اصلية للمستخدم بحيث عندما تعمل البرامج الاصلية ينشط الفيروس وينتشر ليبدأ اعماله التخريبية ،وهو مختلف عن الفيروس في انه لا يتكاثر ولا يلتصق بالملفات وغنما هو برنامج مستقل بذاته يحمل في طياته توقيت واسلوب استقاظه وهو يؤدي إلى تعديل هذه البرامج وتزوير المعلومات ومحو بعضها وقد يصل الامر إلى تدمير النظام بأكمله وهذه البرامج هي في الأساس من الناحية التقنية برمجيات اختراق وتخسس تهدف إلى جمع المعلومات والبيانات كاسم المستخدم وكلمات السر الخاصة به وغيرها ومن تم إرسالها إلى صاحب البرنامج أو مصممه.[3]

●برامج الإنزال :

فقد صممت لمراوغة برامج مكافحة الفيروسات وتعتمد على التشفير غالبا لمنع اكتشافها ولحظة حدوث أمر معين على الحاسب لكي تنطلق وتلوثه بالفيروس المحمول في طياتها وينتمي مفهوم قنبلة الحاسب إلى هذه الفئة إذ تبني القنابل ضمن البرمجيات الماكرة كواسطة لتنشيطها حيث تبرمج لتنشط عند حدوث حدث معين مثلا فيمكن برمجة قنبلة مثلا لمسح كافة الملفات ذات الامتداد DOC من القرص الصلب في ليلة رأس السنة الميلادية، فيمكن أن تنتظر القنبلة إلى أن يتم تشغيل برنامج معين عشرين مرة مثلا وعندها تمسح الملفات الخاصة بهذا البرنامج فهي تعتبر مجرد برامج جدولة زمنية ماكرة[4]

---

[1] عبد الجبار يوسف خليل يوسف. مدى فاعلية إجراءات الرقابة في توفير أمن المعلومات الإلكترونية. المرجع السابق ص29.28

[2] Mehideb Sara، Smartphone application in the economic sphère متاح على الرابط :

http://www.books.google.dz أطلع عليه يوم :2020/02/05. على الساعة : 15.03 .ص 48.

[3] بورباية، صورية. قواعد الأمن المعلوماتي. مذكرة لنيل شهادة دكتورا في العلوم :تخصص علوم قانونية، الجامعة جيلالي يابس، سيدي بلعباس،2015،ص 45.

[4] الجنيهي، منير محمد، الجنيهي، ممدوح محمد. :المرجع السابق. ص 47

- **الدودة :**

تشبه الفيروسات فهي لها القدرة على الانتشار من جهاز إلى آخر ولكنها على خلاف الفيروسات فهي لا تحتاج مساعدة من أي شخص للانتقال فهي تستغل إي ملف يتم نقله من جهاز إلى آخر فيما يعرف بالانتقال غير المدعوم ،لما القدرة على التكاثر والانتشار بكمية كبيرة كما لها القدرة على الانتشار عبر الشبكة ،صممت لكي تعمل كنفق أو مدخل إلى الجهاز مما يسمح للهاكرز بالتحكم في هذا الجهاز.[1]

7.2.4.5 الاصطياد الإلكتروني:

يعتبر من أهم وأكثر التقنيات انتشارا وشيوعا الغاية منه سرقة البيانات الشخصية السرية عن طريق إرسال رسائل البريد الإلكتروني لغرض انتحال شخصية أحد المصارف أو منظمة معينة وإلهام الضحية بجدية الطلب وأهميته بحيث لا يكون الاصطياد الإلكتروني برسائل البريد الإلكتروني فقط بل تتعداها إلى تطبيقات التراسل الإلكتروني الأخرى كالرسائل النصية القصيرة بحيث يكون محتوى الرسالة على انه هناك مشكل في حسابه البنكي أو يدعوه لتحديث بياناته ويكون هذا البريد مرفق برابط إلكتروني مزيف يشابه عنوان موقع المؤسسة ويعد الضغط على الرابط تنبثق نافذة لإدخال بياناته الشخصية سواء اسم المستخدم أو كلمة المرور وبهذا قد يكون أعطى بياناته للمهاجم يدرك العديد من المستخدمين اليوم هذا النوع من السرقة للمعلومات ويتجنبون قدر الإمكان النقر على روابط مزيفة ولكن ليس الجميع حذرا ولا يزال هذا النوع من الهجوم فعالا إلى يومنا هذا.[2]

❖ **طرق اختراق أمن المعلومات في الشبكات الإلكترونية: (Hacking)**

ويقصد به الوصول غير المصرح به للشبكة أو نظام المعلومات المحاسبي لهدف معين وتتمثل في:

- **سرقة كلمة السر :**
- عن طريق اختراق الشبكة وسرقة المعلومات الشركة بسرقة كلمة السر الخاصة بالمعدين داخلها
- التعرض للاختراق أثناء معالجة الاختراق سابق
- **هجمات حقن قواعد البيانات:** من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم إذا تمكن المختال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها.[3]

---

[1] فتحي، أسامة. فيروسات الحاسب، 2008متاح على الرابط :
http://www.download.internet-pdf-ebook.com تاريخ الاطلاع: 5/03/2020 على الساعة:13.32.ص 09.

[2] الغثبر، خالد بن سليمان، بن هيشة، سليمان بن عبد العزيز. الاصطياد الإلكتروني: الأساليب والإجراءات المضادة. الرياض: مركز التميز لأمن المعلومات، 2009. ص 45.

[3] يوسف، خليل يوسف عبد الجبار. مدى فاعلية إجراءات الرقابة في توفير أمن المعلومات الإلكترونية في شركات الصناعية الأردنية. مذكرة ماجستير: محاسبو والتمويل ،جامعة الشرق الأوسط،الأردن،2013.ص 28.

3- مهام ومواصفات أمت المعلومات

3-1- أساليب مواجهة تهديدات أمن المعلومات:

- **تحليل المخاطر الناجمة عن الانتهاك :**

1. ينتج الانتهاك غير متعمد لأمن وسلامة البيانات غالبا عن إجراءات خاطئة وغير سليمة تتراوح بين اجراءات تجهيز وإدخال البيانات وحتى الأخطاء التشغيل التي تحدث أثناء المعالجة، مرور بالأخطاء ونقاط الضعف غير المنظورة في برامج التطبيقية نفسها.[1]

- **تحديد المستوى الحالي لظهور مخاطر الانتهاك :**

تساهم عدة عوامل في تعقيد إمكانية تحديد المستوى الحالي لظهور مخاطر الانتهاك وهي:

1. صعوبة تحديد القيمة الناجمة (الخسارة) عن مختلف الحوادث الانتهاك.

2. عدم إلمام مسئولي أمن المعلومات بطبيعة العمليات التي تتم بداخل النظم المعقدة أو في تحديد عدم كفاية الاجراءات الحالية.

3. صعوبة تقدير احتمالات وقوع أو نجاح بعض المحاولات الانتهاك بسبب عدم وجود توثيق شامل وجيد لحوادث الانتهاك داخل وخارج المؤسسة.

4. صعوبة التنبؤ بالعوامل الإنسانية وبالتالي عدم إمكانية إخضاعها للقياس

- **العقبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية**

2. نقص الأفراد المدربين والذين يبدون اهتماما بمشكلة أمن وسلامة البيانات.
3. نقص التمويل والوقت والمساعدة من جانب الإدارة والجهات المستفيدة من المعلومات.
4. سوء التقدير لمدى تعقد النظم والتطبيقات والاستعجال لبلوغ حالة التشغيل الأمر الذي يؤدي إلى قلة الاهتمام أو إغفال التدابير السلامة الضرورية [2]

2.3. الإجراءات والوسائل اللازمة لحماية أمن المعلومات:

3-2-1- الإجراءات اللازمة لحماية أمن المعلومات:

1. حماية المعلومات على المستوى الأنظمة والبرامج

لاشك أن برامج والأنظمة المستخدمة في أي منظمة دائما عرضة للتهديد من قبل أشخاص غير مصرح لهم لمحاولة تدمير أو تغيير ومحاولة الحصول على نسخ منها لذا فإنه يجب التركيز على حماية هذه البرامج والأنظمة وإبعاد أي خطر قد يهدد أمنها وسلامتها .

❖ **إجراءات حماية المعلومات على مستوى الأنظمة والبرامج:**

1) ضرورة تحديد الأشخاص المصرح لهم بالاطلاع على هذه البرامج والأنظمة داخل المنظمة.
2) الاحتفاظ بنسخة من الأنظمة والبرامج في مكان آمن خارج المنظمة.

[1] دلال، صادق ،الفتال، حميد ناصر. المرجع السابق. ص.18.19

[2] دلال، صادق ،الفتال، حميد ناصر. المرجع السابق. ص 20.

3) ضرورة تحديث بيانات بصفة دورية واختيار كلمات المرور مع تحديثها دوريا
4) ضرورة استفادة الإدارة المنظمة من التقدم التكنولوجي في مجال تخزين المعلومات.[1]

❖ **طرق الحماية على مستوى الأنظمة والبرامج:**

- **وضع كلمات السر أو المرور:**

هي آلية تعريف للمستخدم تعد من أهم وسائل حماية المعلومات فهي تعتبر القفل على الخزينة الإلكترونية لما تقوم به من حماية للمعلومات وأنظمة التشغيل الخاصة بالمستخدم كما تعتبر أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم وفاعليتها وتعتمد على درجة انضباط العنصر البشري في اختيارها والتعامل معها وفق أساليب صحيحة ،ومن مميزاتها أنها طويلة، معقدة، عملية سرية، غير شخصية، و سهلة الحفظ.[2]

- **نسخ وتخزين الاحتياطي:**

على الرغم من الاحتياطات الأمنية المتعددة التي قد تتبع لحماية البيانات إلا أنه من المحتمل وقوع أي نوع من التلف أو التحريف أو الفقدان للبيانات ،لذا كان لابد من تأمين طريقة يمكن من خلالها استعادة البيانات التالفة او المفقودة أو المحرفة لضمان مستوى أعلى من الحماية للنظام. ويحقق النسخ الاحتياطي للبيانات هذا المستوى من الحماية حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجة ويتم تحديثها بصورة منتظمة لضمان أقل قدر من الخسائر في حالة فقدان البيانات الأصلية. ولابد من تحديد ما ينبغي نسخها احتياطيا ومتى ينبغي نسخه ويعتمد هذا على درجة اهمية البيانات المختزنة على خادم الملفات.[3]

- **التحديث التلقائي للبرامج وأنظمة التشغيل :**

يعد من أهم النقاط حماية أمن المعلومات وذلك لأن عملية بناء هذه النظم هي غاية في التعقيد ولا تخلو من بعض الأخطاء التي تحدث في فترات البناء وتعمل الشركات على إيجاد التحسينات المستمرة لسد نقاط الضعف في هذه البرامج والأنظمة التي تمكن المخترقون من اختراق النظام وهذه التحسينات تتاح دائما فيما يعرف بالتحديثات ومن هنا تأتي أهمية قيام المستخدم بعمليات التحديث الدائم للبرامج والانظمة التي تتبناها في جهازه الشخصي على مستوى الفردي وعلى مستوى البرامج والأجهزة[4]

---

[1] الشريف، أشرف عبد المحسن. أمن وحماية المستندات الالكترونية على بوابة الحكومات العربية. مجلة الاتحاد العربي للمكتبات والمعلومات. ع 16، 2016 . ص 100.

[2] الغثبر، خالد بن سليمان، القحطاني، محمد بن عبد الله. أمن المعلومات بلغة ميسرة.، مركز التميز لأمن المعلومات.: الرياض، 2009. ص18

[3] عبد الهادي، محمد فتحي. الاتجاهات الحديثة في المكتبات والمعلومات، ع .18 ،2002. متاح على الرابط:
http://www.books.google.dz أطلع عليه يوم : 02 /2020/01.على الساعة : 12.09

[4] دخيل، أحمد نوري، سعد، عبد السلام. اختراقات أمن المعلومات وطرق تفاديها. المجلة الدولية المحكمة للعلوم الهندسية وتقنية معلومات. مج 2،ع 2،يونيو 2012،ص 06.

المستخدمة في شبكات المعلومات ونظرا لصعوبة مطالبة الشركات لمستخدمي هذه البرامج بتحديث البرامج بأنفسهم فإن معظم الشركات المصنعة لهذه البرامج قامت بإضافة خاصية التحديث الآلي والتلقائي لهذه البرامج ولكي تعمل هذه الخاصية يقو البرنامج المثبت في الشبكة بالاتصال تلقائيا وعلى فترات معينة بالشركة المنتجة له والقيام بالبحث عن أية تحديثات جديدة وتنزيلها تلقائيا.

- **طمس البيانات :**

أغلب المستخدمون يعتقدون بمجرد حذف الملف فإنه فقده نهائيا حتى لو كان قد حذفه من سلة المحذوفات وهذا غير صحيح فحذفه من وحدة التخزين يتم بحذف مؤشر الذي يدل عليه وليس الملف نفسه أي أن المحتويات الملف تظل في وحدة التخزين ،و لكن على هيئة مساحة فارغة وبناء عليه فإنه يمكن استرجاعه بواسطة برامج لاسترجاع متخصصة وهنالك ثلاث طرق لطمس البيانات وهي:

1) طمس الملف عند حذفه
2) طمس المساحة الفارغة في وحدة التخزين
3) ما يعرف بملف المبادلة.[1]

2. حماية المعلومات على مستوى الأفراد العاملين على النظام :

يشكل الأفراد العاملين على النظام الآلي في المنظمة أحد التهديدات القوية التي يمكن أن تؤثر على أمن وسلامة المعلومات فقد يرتكب الفرد خطأ عند استخدام النظام أو أثناء إعداد وتجهيز البرامج مما يقلل من فاعلية كما يجب عدم إغفال نقطة مهمة وهي أنه من المحتمل أن يكون أحد الأفراد العاملين على النظام ليس فوق مستوى الشبهات فيصبح من أكبر تهديدات على النظام وما يحتويه من برامج وبيانات

❖ **إجراءات الحماية على مستوى الأفراد العاملين على النظام:**

- الحرص على توظيف المؤهلين علميا وعمليا ما أمكن لتقليل احتمال الوقوع في الخطأ أثناء العمل.
- ضرورة إصدار النشرات المتعلقة بالجوانب الأمنية للقدرة على مواجهة أي تهديد لأمن المعلومات
- إخضاع المبرمجين وحللي النظم وبصفة مستمرة للمراقبة من قبل مشرف صاحب خبرة طويلة في هذا المجال وإشعارهم بأنهم خاضعون للرقابة الأمنية المستمرة من قبل إدارة المنظمة.
- إبعاد أي فرد من العاملين يمكن أن يهدد أمن المعلومات كما يجب أن تضع الإدارة عقوبات رادعة لهم.

[1] دخيل، أحمد نوري، سعد، عبد السلام. المرجع نفسه . ص 06.

- أخد تعهد على الموظف المنتهي خدماته في المنظمة بالمحافظة على أسرار العمل التي كان يطلع عليها .[1]
- تحديد كلمات مرور للعاملين على أن يراعي تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله وتكون قاصرة على نطاق عمله بالمؤسسة فقط وليست صلاحيات دون حدود.
- اختيار العاملين بعناية تامة مع ضرورة التأكد من أمانتهم وإخلاصهم ويظهر ذلك من خلال قيام الإدارة بمراقبة سلوكياتهم عن بعد للتأكد من ذلك.
- التأكد من إزالة بيانات العاملين المنتهية مدة خدمتهم في المؤسسة من قائمة مستخدمي النظام.[2]

2.2.3. الوسائل التقنية والمادية لحماية المعلومات:

1- **الوسائل التقنية:** تتمثل في نقاط التالية

- **الجدار الناري:**

هو تطبيق برمجي يقوم بمراقبة جميع البيانات والمعلومات التي تصل إلى الخادم عن طريق الفضاء السيبراني بهدف حماية البيانات والمعطيات الأصلية المخزنة على خادم الويب لحماية الملكية الفكرية أو أي خادم آخر متصل بالإنترنت فهو إذن بمثابة الحراسة الأمنية المشددة على بوابة المؤسسة أو الشركة التي تتفحص بشكل دقيق كل من بداخل وكشف أي محاولة عبثية وإجرامية تستهدف التخريب[3]

❖ **مزايا الجدار الناري:**

- منع دخول المستعملين غير مصرح لهم بالدخول للشبكة.
- حماية استعمال الخدمات المهمة عند دخول الشبكة ومغادرتها.
- توفير الحماية اللازمة للشبكة والمعلومات. بالإضافة إلى خدمات التشفير
- متابعة المستخدمين للشبكة ومن يحاول العبث بها، بالإضافة إلى توافقه مع جميع الشبكات المفتوحة

❖ **عيوب الجدار الناري:**

1. أنه لا يتعامل مع تنفيذ البرامج الداخلية التي تهاجم النظام.
2. لا يقدم حماية للنقل الاذاعي والتليفزيوني.[4]

---

[1] الشريف، أشرف عبد المحسن.. المرجع السابق، ص100.

[2] جبرا، كمال محمود. التأمين وإدارة المخاطر. القاهرة: الأكاديميون للنشر والتوزيع، 2015. ص 122.متاح على الرابط: http://www.google.books.dz أطلع علية يوم:2020/03/23.على الساعة:14.16.

[3] المصري، عبد الصبور عبد القوي علي. التنظيم القانوني للتجارة الالكترونية. الرياض: مكتبة القانون والاقتصاد، 2012. ص 338.

[4] وليام، ستولينج. أساسيات أمن الشبكات تطبيقات ومعايير،2011. ص 108.متاح على الرابط : http://www.books.google.dz أطلع علية يوم :2020/03/15. على الساعة 14.23.

- **برامج مكافحة الفيروسات:**

هي برامج يتم تركيبها على الجهاز ولهذه البرامج قواعد بيانات خاصة موجودة بها تواقيع وأو بصمة خاصة لكل فيروس بحيث تتم مقارنة أي برامج موجودة على الجهاز سواء في حالة طلب تشغيل البرامج أو أثناء عمل المسح على الجهاز مع قواعد البيانات وفي حالة العثور على تطابق في شلوك البرنامج مع قواعد البيانات فإنه سيصدر رسالة مشعرا المستخدم بوجود الفيروس أو برنامج التجسس.[1]

- **الكاشفات الالكترونية والبيولوجية:**

تعتبر من أفضل النظم المستخدمة للتحقق من شخصية المستخدم لأنها تعطي درجة عالية من الأمان مقارنة بالأساليب الأخرى بحيث لا يمكن نسيانها أو سرقتها كما هو الحال مع كلمات السر، لذا وجب استبدالها بالقياسات الحيوية واستخدامها لتحديد هوية الشخص والتعرف عليه، تسمح له بالوصول جسديا ،أو منطقيا إلى الحاسب الآلي أو قاعدة البيانات، فهي عبارة عن خصائص بيولوجية الموجودة في جسم الإنسان يمكن تقسيمها إلى قسمين:

1) **الخصائص الفسيولوجية**: تتمثل في بصمات الأصابع، هندسة اليد، قزحية العين، الوجه، الحمض

2) **الخصائص السلوكية**: وهي التعرف على الصوت، التعرف على التوقيع، إيقاع حركة اليد في استخدام المفاتيح.[2]

- **التشفير:**

هو إخفاء المعلومات السرية بطريقة يصبح من خلالها معناها غير مفهوم بالنسبة إلى أي شخص غير مصرح له بالاطلاع عليها عن طريق خوارزميات التشفير.[3]

تعتمد تكنولوجيا التشفير الحديثة على النظرية التالية بحيث يمتلك كل فرد مفتاحين للتشفير وفك التشفير البيانات المفتاح الاول هو مفتاح خاص ويكون بحوزة الجهة المطلوبة فقط والمفتاح الثاني وهو المفتاح العام ويتم نشره على الانترنت أو على شبكة الحكومة الالكترونية من أجل استخدامه من قبل الجهات الأخرى لتشفير الملفات والمعلومات المراد إيصالها إلى الطرف الآخر[4]

---

[1] حربي، خالد بن نواف. أمن والحماية في الانترنت. السعودية، متاح على الرابط :
http://www.Mudhesh.netpdf أطلع علية في: 2019/11/18.على الساعة 22.23.ص 8.

[2] دسوقي أحمد،فايزة. بصمة اليد والعين والقياسات الحيوية في امن المعلومات، تاريخ الصدور 2010/11/21.متاح على الرابط:
http://www.lahaonline.com أطلع علية يوم :2020/02/11. على الساعة 16.32.

[3] باييروشون ميرفي، فريد. تر. محمد سعد طنطاوي. علم التشفير. مؤسسة الهنداوي للتعلم والثقافة، 2016. ص. 16.

[4] ليتم، فتيحة. ليتم، نادية. الامن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، ع 12،ص 249.

الهدف من التشفير هو الزيادة إلى الحد الأقصى لعدم الترتيب لغرض إخفاء المعلومات لذلك فإن تقليص عدد الاختيارات الممكنة وذلك بمراقبة النماذج الثنائية الغير مقبولة نميل إلى امتلاك نوع من الترتيب.[1]

- **محاكاة أساليب الهجوم الإلكتروني:**

يسمى هذا الأسلوب في بعض الاحيان بالمناورات الامنية الإلكترونية وتعمل خلالها اجهزة الأمن الإلكتروني على القيام بهجوم تجريبي غير ضار على انظمة إدارات الدولة المختلفة لتحقيق من صلاحيتها ومقاومتها وقد يتم هذا الهجوم بدون سابق إنذار للتأكد من فعالية أجهزة الحماية ومستوى تطبيق الإدارات الحكومة لمعايير الامن الإلكتروني للمعلومات، من أجل توفير حماية أمنية للتأكد من عدم تجرؤ مختلف الأطراف على العبث والتخريب للمعلومات.[2]

- **أمن الشبكات:**

من الأساسيات في حقل أمن المعلومات حماية المعلومات الخاصة التي تنتقل عبر الشبكة الحاسوبية هذا الامر ما يتكفل به أمن الشبكات، وامن الشبكات هو مجموعة من الإجراءات المضادة التي تكفل إدخال المعلومات الرقمية الخاصة المشتركة المعدة للنقل في وضع الأمان عند مرورها عبر شبكة غير آمنة، وتتمثل مجموعة الإجراءات المضادة في حماية الشبكة نفسها وفي حماية المعلومات الخاصة التي تمر عبرها، وعموما يؤدي أمن الشبكات دوره لحماية المعلومات الخاصة في المحيط الإلكتروني فقط.[3]

❖ **إجراءات حماية أمن الشبكات:**

- **إجراءات الحماية غير مادية:** تتمثل في العناصر التالية

1. عنونة الشبكات بوضع عناوين لجميع الأجهزة المرتبطة بالشبكة لكي يمكن التعرف عليها عند تشغيلها.
2. متابعة جميع محاولات الدخول إلى النظام سواء المحاولات الصحيحة أو الفاشلة.
3. توفير آليات الحماية بعد الدخول إلى النظام كالتزام المستخدم بالخروج من النظام عند عدم استخدامه والخروج الآلي عند عدم استخدامه لفترة معينة وعند نهاية العمل به.
4. اتخاذ إجراءات مراجعة الشبكة بعد تشغيلها والإشراف عليها من قبل إداريين وفنيين بهدف اكتشاف وتحسين خدمتها باستمرار.[4]

---

[1] دهب، علي محمد. التشفير وأمن المعلومات. جامعة كردفان، كلية دراسات الحاسوب والإحصاء، سودان، 2016.ص 07.متاح على الرابط http://www.kutub.info.pdf أطلع عليه يوم: 2020/01/25.على الساعة:15.32

[2] الكافي، مصطفى يوسف. الحكومة الإلكترونية في ظل الثروة العلمية التكنولوجية المعاصرة. دمشق: دار ومؤسسة رسلان للنشر، 2009،ص 161.متاح على الرابط:. http://www.book.google.dz أطلع علية يوم : 2020/03/16.على الساعة:18.11.

[3] ساري، محمد خالد. اتجاهات في امن المعلومات وامانها. الرياض: العبيكان للنشر، 2017،ص 61.

[4] الشريف، أشرف عبد المحسن. مرجع سابق، ص 103.104.

▪إجراءات الحماية المادية:

1. يتضمن إجراءات التوصيلات والتمديدات بين الأجهزة بشكل آمن من خلال تمريرها عبر القنوات غير مكشوفة ويصعب الوصول إليها وعزل الكابلات داخل أنابيب بلاستيكية وعبر الجدران أو فوق الأسقف حتى لا تكون معرضة للوصول غير المرخص. مع وضع أجهزة استشعار لإطلاق إنذار عند الخطر.

2. تخصيص غرف مغلقة لحماية أجهزة خادم الشبكة المركزية للمؤسسة أي بعيدا عن غرف العاملين أو المستفيدين حتى لا يكون متاحا للجميع.

3. استخدام كابلات المغلقة وذلك لتقليل الإشعاع الثانوي المنبثق من خلال منع إمكانية إضافة أكثر من غلاف عليها لمنع هذا الإشعاع.

4. توفير وسائل مراقبة لموقع المؤسسة من الداخل والخارج مثل الدوائر التليفزيونية المغلقة.

5. تأمين الأبواب والنوافذ وذلك باستخدام أجهزة إنذار الآلية لتقوم بتشغيل أجراس التنبيه في حالة دخول في غير ساعات العمل.[1]

❖ **الأنواع للهجوم على أمن الشبكات:**

- **الانقطاع:**

هي عندما ترسل الرسالة من المرسل ولا تصل المستقبل وقد يكون السبب في المسير أو الموجه.[2]

- **التصدي:**

وهي عندما ترسل الرسالة من المرسل إلى المستقبل ولكن بطريقة غير شرعية يتصدى لها مستمع آخر بالتصنت واستراق السمع على المحادثة.

- **التعديل:**

وهي عندما ترسل الرسالة من المرسل إلى المستقبل ولكن تذهب أولا إلى مستمع ثالث يجري تعديل على الريالة ثم يكمل إرسالها معدلة.

- **الدبلجة:**

وهي عندما يقوم مرسل ثالث بفبركة الرسالة ثم يقوم بإرسالها بحيث ينظر إليها وكأنها من المصدر الشرعي.[3]

---

[1] الشريف،أشرف عبد المحسن. . مرجع نفسه،ص 103.104.

[2] فايز جمعة النجار،نظم المعلومات الإدارية منظور إداري: MANAGEMENT INFORMATION SYSTEMS –MANAGERIAL PERSPECTIVE. عمان: دار الحامد للنشر والتوزيع، 2009،ص 273.

[3] فايز جمعة النجار؛المرجع نفسه.ص 273

- **إخفاء IP الخاص بالحاسب الآلي:**

وذلك حتى تتجنب إخطار الهاكرز والمخترقين وتكون في أمان لطكن هذا الأمان لأجل منع اختراق الجهاز وليس الفيروسات، كما ان IPالا يختفي بالنسبة للشخص الذي قام بوضعه ولكن هذا الرقم يختفي لأي شخص مخترق آخر بمعنى الأفراد غير مصرح لهم بالوصول للمعلومات والمعطيات.[1]

- **التحكم في الوصول:**

توفر هذه الخدمة الحماية ضد الوصول إلى معطيات لكل ما له علاقة بعمليات التعديل والتنفيذ للبرامج وغيرها من العمليات، بحيث يتم اللجوء إليه لتحديد سماحيات وصول المستخدم إلى معطيات ومصادر المملوكة من قبل النظام مثل: السماحيات الممنوحة وفقا لكلمات السر أو الرموز السرية. [2]

2- **الوسائل المادية:** تتمثل في العناصر التالية

- **الحواجز الفيزيائية:**

ويتضمن استخدام المكونات المادية التي تساعد في الحفاظ على أمن المعلومات وتمنع الوصول إلى المنشأة المعلوماتية مثل:

وضع حواجز محيطة بالمنشأة وحواجز أمام مدخل مركز الأجهزة وإقفالها لمنع الوصول إليها[3].

- **الكاميرات ونظم المراقبة:**

وهي التي تكون بواسطة الكاميرات تلفيزيونيه مركبة على الحوائط والأسوار وبزوايا متعددة مرتبطة بلوحة تحكم شاشة وتسمى بالحارس المتحرك وهذا نظام يساعد على تأمين المنشأة من الداخل والخارج كما تساعد في المراقبة على رصد أي نشاط من جانب أفراد غير مصرح لهم بالتواجد في المكان الذي توجد فيه الأجهزة الحساسة. كما تعد دليلا في حال ارتكاب أي تهديدات على أمن المعلومات من ناحية المادية.

- **نظم الإنذار المبكر:**

تستخدم كنوع من التدابير اللازمة لحفظ أمن محيط المنشاة وحماية المواد التقنية والمادية الموجودة بها وتستخدم هذه النظم العديد من الأجهزة الحساسة الخاصة بالإنذار المبكر لرصد أعمال السرقة والحريق والعديد من الكوارث الطبيعية .

---

[1] خالد، محمد خالد. أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الإلكتروني. الإسكندرية: المركز العلمي لتبسيط العلوم للنشر، 2006،ص 28.

[2] الدوه حي، صلاح. مقدمة في التشفير. سورية: من منشورات الجامعة الافتراضية السورية، 2018،ص 09.08.

[3] عبد الحليم. مبادئ امن المعلومات،أسس،2017/04/14،متاح على الرابط : http://www.aodus.org/t/topi1971.
أطلع عليه يوم:2020/03/22.على الساعة:10.53

❖ **أنواع نظم الإنذار المبكر:**

- **أجهزة الإنذار للبوابات والمنافذ:**

تتم بواسطة بطاقات مقروءة ومشفرة لفتح الأبواب والخزائن وإبطال محاولات الاقتحام تعتمد على عناصر البطاقة المشفرة، قارئ للبطاقات المشفرة، نظام فتح الأبواب، نظام إنذار آلي.

- **أجهزة إنذار الأسوار:**

وهي أجهزة متعدد تتم إحاطة مبنى المنشأة بها لاكتشاف أي محاولة للاختراق إذ ما تم قطع الدارة الكهربائية فيدون ذلك في لوحة خاصة توضح مكان الاقتحام.

- **أجهزة إنذار الخزائن:**

تتصل بغرفة العمليات وتبين محاولات الاقتراب من الخزائن أو فتحها فتعطي إنذار إذ ما تم قطع الدارة الكهربائية.

- **أجهزة إنذار الحريق:**

تعطي إنذار إذا ارتفعت درجة حرارة المكان الموجود فيه جهاز إنذار بطريقة آلية وإلكترونية.[1]

3-وسائل التوعية:

كان يعتبر أمن المعلومات هو مسؤولية إدارة أمن المعلومات، وأن برامج وأنظمة الحماية كافية لصد الهجمات الإلكترونية هذا لم يعد مجديا هذه الأيام، ولا يكفي لضمان الحماية للأصول المعلوماتية الهامة. ولهذا السبب هناك توجه عالمي ومحلي لسدة الفجوة المعرفية لدى الموظفين في مختلف القطاعات من خلال تفعيل ما يسمى ببرامج "التوعية بأمن المعلومات". وهذه البرامج تستهدف جميع العاملين في المؤسسات والخاصة على مختلف المستويات الإدارية لرفع مستوى الوعي بأهمية أمن والتعرف على أخطر التهديدات، وطرق التعامل معها من خلال أساليب متنوعة إلكترونية ومطبوعة، تشكل في النهاية جملة من الوسائل التوعية م التي تتمثل في: المحاضرات، لإعلانات التوعية، المطبوعات. و شاشات التوقف. نشرات إلكترونية .[2]

بالإضافة إلى وجود مجموعة أخرى من الوسائل التي من شأنها أن تحقق الأمن المعلومات وهي:

- **مجموعة الوسائل الهادفة للحماية التكاملية:** (حماية المحتوى):

وهي الوسائل المناط منها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مسموح لها بذلك وتشمل من بين ما تشمل تقنيات الترميز والتوقيعات الإلكترونية وبرمجيات تحري الفيروسات.

---

[1] الليبدي، إبراهيم محمد. تامين المنشآت. مركز الإعلام الأمني. متاح على الرابط: http://www.policemc.gov.bh/msms-store/pdf .
أطلع عليه يوم:2020/03/21.على الساعة:15.30

[2] التوعية في أمن المعلومات. مركز التميز لأمن المعلومات. الرياض،2020. متاح على الرابط:
http://www.coeia.ksu.edu.sa . أطلع علية يوم: 2020/03/19 على الساعة 21.12

- **مجموعة الوسائل المتعلقة بمنع الإنكار:** (إنكار تصرف صادر عن شخص)

تهدف إلى ضمان عدم قدرة الشخص المستخدم من إنكار أنه هو الذي قام بالتصرف وهي الوسائل ذات أهمية بالغة في بيئة الأعمال الإلكترونية وترتكز هذه الوسائل في الوقت الحالي على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.

- **وسائل مراقبة الاستخدام وتتبع سجلات النفاذ أو الأداء:**

وهي تقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بعمل معين في وقت معين وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.[1]

4.3 **آليات تعزيز أمن المعلومات :**

نظرا لتعدد ومجالات اختراق أمن المعلومات فقد زاد الاهتمام بتعزيز أمن المعلومات من خلال الاعتماد على الآليات المناسبة التي تكفل تحقيق هذا الامن وتتمثل هذه الآليات فتمايلي

1.الإستراتجية الأمنية :

إن وجود استراتيجية الملائمة لأمن المعلومات يساعد على توفير المناخ السليم لتحقيق هذا الأمن وتعزيزه من خلال ما يلي:

1. .إعداد الحلول الأمنية التكتيكية في ضوء صلتها بأهداف المنظمة
2. تربيت أسبقيات المنظمة من انشطة وبرامج أمنية المعلومات
3. .تشخيص نقاط القوة والضعف في برامج الحالية لأمن المعلومات[2]
4. وضع سياسة محددة وموثوقة لأمن المعلومات
5. تحديد قائمة التهديدات المحتملة وقوعها وإجراءات الوقائية لها.
6. .توزيع المسؤوليات المتعلقة بأمن المعلومات.

2.التشريع والقانون :

عن طريق إصدار التشريعات والقوانين التي تحد من الخروق الأمنية بعد انتشارها وتعددها.

3.العاملون :

إن الأفراد المستخدمون للحاسوب هم العامل الاساسي في أمن المعلومات ولا قيمة لأي نظام أمني مهما كانت التكنولوجيا المستخدمة فيه متطورة في حال فشل مستخدمو هذا النظام في إتباع الإجراءات اللازمة لتنفيذه .إن الالتزام بنظام أمن المعلومات يشمل جميع العاملين بما فيهم الإدارة العليا.

[1] الجنبيهي، محمد منير، الجنبيهي؛ محمد ممدوح. المرجع السابق.ص64.65

[2] جبرا، كمال محمود؛المرجع السابق. ص122

4.التعامل مع اختراقات أمن المعلومات :

يتمثل هذا في إتباع الإجراءات الصحيحة في التعامل مع مجالات اختراق أمن المعلومات مثل الملفات الورقية وذلك من خلال تجاوز العيوب والثغرات التي تشكل الفرصة السامحة لاختراق أمن المعلومات.

5.وحدات أمن المعلومات :

ويتمثل هذا العنصر في ضرورة استحداث وحدات تنظيمية تتولى مسؤولية توفير أمن المعلومات مثل وحدة المعايير والسياسات التي تقوم بمراجعة وتقييم الوضع الأمني للمعلومات في المؤسسة.[1]

4.3 المعايير الدولية لأمن المعلومات:

1.معايير المنظمة الدولية للتوحيد القياسي :

أنشئت المنظمة الدولية للتوحيد القياسي عام 1947 وهي منظمة غير حكومية تتعاون مع كل من اللجنة الدولية الكهروتقنية والاتحاد الدولي للاتصالات. ومن أهم المعايير التي أصدرتها الإيزو مجموعة معايير أمن المعلومات والتي تسمى مواصفات نظم إدارة نظم المعلومات إيزو 27000 والتي تتكون من ستة معايير فرعية وهي 27001 الأسس والمفردات:

27002 قواعد الممارسة العملية لأنظمة إدارة المعلومات

27003 دليل تنفيذ إدارة امن المعلومات

27004 قياس فاعلية نظم إدارة أمن المعلومات

27005 إدارة مخاطر أمن المعلومات

27006 دليل لعملية المصادقة على نظام إدارة أمن المعلومات

ومن بين هذه المعايير الفرعية نجد إيزو 27002 هو الاهم لأمن المعلومات [2]

1.1. **معيار ايزو 27002 :**

هو أحد معايير سلسلة إيزو 27000 الصادرة عن المنظمة العالمية للتوحيد القياسي الذي يهدف إلى إنشاء نظام إدارة أمن المعلومات ويستخدم في المؤسسات لتحديد الأهداف والمطالب الأمنية وتحديد المسؤوليات والضوابط وإدارة أصول المؤسسة.

ملاحظة :سوف يتم التطرق لهذا المعيار بالتفصيل في الجانب التطبيقي من الدراسة

2.1. معيار إيزو 27016:

أصدر هذا المعيار في 2014 ويهدف إلى تقديم المبادئ التوجيهية القائمة على الممارسات الجيدة المقبولة عموما والتي يمكن استخدامها وفهمها من قبل أصحاب الخبرة في مجال أمن المعلومات

[1] ان سعيد، إبراهيم عبد الواحد.، المرجع السابق ،ص 19.

[2] العربي، أحمد عبادة. معيار المنظمة الدولية للتوحيد السياسي إيزو 27002 لسياسات أمن المعلومات. مجلة جامعة الطيبة للآداب والعلوم الإنسانية. ع7. سعودية،1436هـ،ص 678.679.

والمديرين لمناقشة الخطوات الإجرائية والبدائل المتاحة لبرنامج أمن المعلومات من حيث النتائج المالية المتوقعة، فإنه يهدف إلى تقديم مبادئ توجيهية بخصوص أمن المعلومات .

3.1. معيار ايزو 27038 :

أصدر هذا المعيار في مارس 2014 ويسمى أيضا بمعيار التنقيح ويعني إبعاد المعلومات الحساسة مثل أسماء ومواقع يجب أن تظل مجهولة ومختلف المعلومات الشخصية أو الملكية الأخرى التي يجب أن تبقى سرية للغاية من داخل الملفات الأصلية حتى لا يتم نشرها لأطراف الثالثة أو لعامة الناس ويهدف هذا المعيار إلى تحديد الخصائص التكنولوجية للقيام بعملية التنقيح الرقمي على المعلومات الرقمية كما يحدد متطلبات أدوات برامج للتنقيح وطرق الفحص والاختيار التي تمت على عمليات التنقيح الرقمي التي تم الانتهاء منها بشكل آمن.

2. معيار COBIT 5:

اختصار لكلمة The control objectives for information and related technology: (أهداف الرقابة على المعلومات والتكنولوجيا ذات الصلة)مجموعة من أفضل الممارسات لإدارة تكنولوجيا المعلومات التي تم إنشاءها بواسطة معهد حوكمة تكنولوجيا المعلومات ITGI وتطويرها بالتعاون مع جمعية الرقابة[1]

و المراجعة على انظمة المعلومات ISACA وبعد إصدار النسخة الخامسة من COBIT من قبل ISACA في عام 2012 والتي تعتبر أداة فعالة لإدارة المقاييس الأمنية والعمليات والمراقبة الأمنية والمؤشرات اللازمة لدعم برامج الحماية وتشمل النسخة الخامسة COBIT 5 على مجموعة من الإصدارات لتوفير توجيهات وإرشادات إضافية حول العوامل المساعدة ضمن إطار الCOBITو كيفية قيام المتخصصين بإستخدام COBIT في توصيل خدمات تكنولوجيا المعلومات Stroud 2012 وتنقسم تلك الإصدارات إلى مجموعتين هما:

1) **دليل المساعدة:** يحتوي على COBIT 5 لتمكين العمليات

2) **دليل المتخصصين:** و تحتوي هذه المجموعة على:

- CIBIY 5 للتطبيق، COBIY 5 لأمن المعلومات،COBIT 5 للتأكيد،COBIT 5 للمخاطر.

و يقوم COBIT باختيار سياسات الأمن ومعايير والعمليات والرقابة على موارد أمن المعلومات، وكما يوفر إطار شامل لإجراء تكامل بين الأمن والعمليات التجارية بالشركة (الأمن المادي)

3. معيار ITIL:

اختصار Information Technology Information Library يعتبر معيار ITIL (مكتبة البنية التحتية لتكنولوجيا المعلومات)من أكثر المناهج قبولا في العالم لإدارة خدمات تكنولوجيا المعلومات تم

[1] علي محمود مصطفى خليل، منى غربي محمد إبراهيم. الدور التأثيري لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبة الإلكترونية-دراسة ميدانية، جامعة بنها. ص 13.

وضعه من قبل مكتب التجارة الحكومي في المملكة المتحدة ،وهو عبارة عن مجموعة من الارشادات في مجال إدارة خدمات تكنولوجيا المعلومات فهو يصف العمليات والهياكل التي تعمل على تدعيم خدمات تكنولوجيا المعلومات ويعتبر أمن المعلومات واحد من العديد من العمليات التي يصفها معيار.[1]

[1] مصطفى، علي محمود خليل ،منى مغربي محمد إبراهيم المرجع نفسه. ص. 14.15

الفصل الثاني:
الأرشيف: المفهوم والأطر النظرية

تمهيد للفصل :

يمثل الأرشيف بالنسبة لكل أمة ذاكرتها الرسمية وتراثها التاريخي، لأنه شاهد على وجودها ودليل على سيادتها، باعتباره الموروث الثقافي وحضاري، فلا شك أن الاهتمام بهذا الموروث(الأرشيف) يجعل منه مصدرا أساسيا للمعلومات ووسيلة للبحوث كونه مرآة التي تعكس تاريخ الأمم ولهذا عملت الأمم ولازالت تعمل عبر العصور لتوفير الامن والحفاظ على مخزونها الوثائقي، من كل التهديدات التي يتعرض لها سواء التقليدية أو الإلكترونية مما يجعل الاهتمام به ضرورة ملحة. ولمعرفة كل هذا فقد عالج هذا الفصل بثلاث مباحث تحت كل مبحث اربع مطالب فكان المبحث الاول بعنوان ماهية الارشيف: فتطرقت إلى كل من: مفهوم الأرشيف ،مراحل تطوره ،خصائصه، مبادئه، أما المبحث الثاني فقد احتوى على: أنواع الأرشيف ،أعمار الأرشيف، الإضافة إلى الجمعيات والمعاهد العلمية الخاصة به وفي آخره بينت أهميته، وفيما يخص مبحث الثالث: فقد جاء حديث فيه عن تقنيات الحديثة في مجال الأرشيف، وتأثيرها عليه، ثم جاء الحديث عن أخطار التي يتعرض لها الأرشيف ،الإجراءات الوقائية لحمايته منها. ومن خلال هذه العناصر يمكن القول بأن الاهتمام وحماية الموروث التاريخي أمر ضروري يتطلب العمل به في كل المؤسسات من أجل الحفاظ على ذاكرة الأمم.

1- ماهية الأرشيف

1-1- مفهوم الأرشيف:

❖ **لغة:**

اتفقت مجمل التعاريف على أن أصل كلمة أرشيف يوناني الأرشيف كلمة مشتقة من الكلمة الإغريقية الأرخيون والأرشيون، تعني مكان إقامة القاضي أو المكان العام. وتعني السلطة .[1]
و قد اختلفت دلالاتها اللغوية بين مؤلف وآخر شاع استعمالها من اليونانية إلى لغات أخرى.[2]

اللغة	الكلمة باللاتيني	لفظها بالعربية
الفرنسية	Archives	أرشيف
الإنجليزية	Archives	أركايفز
الألمانية	Archiv	أرشيف
الإسبانية	Archivos	أرشيفوس(أرخيفوس)
الإيطالية	Archivi	أرشيفي

جدول رقم 01 يمثل لفظ لكمة ارشيف في اللغات الاجنبية

1. **اصطلاحا:**

- **عرفه قاموس أكسفورد:** الأرشيف على أنه:

1. المكان الذي تحفظ فيه الوثائق العامة والمستندات التاريخية الهامة.
2. تطلق الكلمة على المواد الوثائقية نفسها.
3. الهيئة أو الإدارة القائمة بعملية الإشراف على الأرشيف.

- **اما بالنسبة للجمعية الأمريكية الأرشيفية:**

عرفته بأنه الوثائق الغير الجارية المنظمة والتي أنتجتها مؤسسة أو منظمة وتم حفظها بسب قيمتها الدائمة ويتم الرجوع إليها وقت الحاجة.[3]

---

[1] دلهوم، انتصار، تسيير الأرشيف في المؤسسات والإدارات العمومية: دراسة ميدانية بولاية سوق أهراس، مذكرة ماجستير، جامعة منتوري،قسنطينة،2006،ص 64

[2] الغرابي احمد بن عبد الله. الأرشفة الإلكترونية في المملكة العربية السعودية: دراسة لواقع الوزارات والمؤسسات شبه الحكومية،الرياض:2008.ص 48

[3] محمد مصطفى محمد علي، الأرشيف الإلكتروني، ص 1،متاح على الرابط:
http://www.dspace.mahdi.edu.sd تاريخ الإطلاع:2020/03/29.على الساعة::12.40

تعريف الأرشيف في معجم السيفير لمصطلحات الأرشيف: 1964 هو الوثائق المستلمة أو الموجودة معا تحت رعاية فرد طبيعي (عادي)أو ذو اعتبار (القانون)عام أو خاص أرسلت لطبيعتها ثم حفظت لدى الشخص نفسه. [1]

1-1-1- تعريف الأرشيف في التشريع أو القانون:

إضافة إلى هذه التعاريف نجد بأن القانوني الجزائري أعطى تعريفا للأرشيف وفقا للقانون 09/88 المؤرخ في جمادى الثانية عام 1408 الموافق ل 26 يناير1988 اهتم بتعريف الوثائق الارشيفية كل على حدى وجاء فيها ما يلي:

المادة 01 :

الوثائق الأرشيفية بمقتضى هذا القانون عبارة عن وثائق تتضمن أخبار مهما كان تاريخها أو شكلها أو سندها المادي ،أنتجتها أو سلمها أي شخص طبيعيا كان أو معنويا أو أية مصلحة أو هيئة عمومية كانت أو خاصة أثناء ممارسة نشاطها.

المادة 02 :

يتكون الأرشيف بمقضى هذا القانون من مجموعة الوثائق المنتجة أو المستعملة من الحزب أو الجماعات المحلية أو الأشخاص الطبيعيين أو المعنويين سواء من القانون العام أو الخاص أثناء ممارسة نشاطها معروفة بقواعدها وقيمتها سواء كانت محفوظة من مالكها أو حائزها أو نقلت إلى مؤسسة الأرشيف المختصة[2].

1-2- التطور التاريخي لمفهوم الأرشيف:

1-2-1- في العصور القديمة:

يمكن القول بصورة عامة أن الأرشيفيات كانت موجودة ومعروفة في حضارات الشرق القديم وكذلك عند الإغريق والرومان، فمن المعروف أن بلاد ما بين النهرين كانت الموطن الأول للكتابة والتدوين، فقد اخترع العراقيون القدماء الكتابة الصورية، ومن العراق أخذت الكلمة المطبوعة طريقها إلى الشيوع والاستعمال في بقية أرجاء العالم القديم، أما الأرشيفات التي كانت معروفة عند القدامى العراقيين كالسومرين والآكاديين والبابليين والآشوريين والآكاديين والكلدانيين وكذلك عن المصريين القدماء والفرس والأمم الأخرى وما خلفوه القدماء الفرس والأمم من طين وألواح حجرية ومدونات أخرى، وكانت المواد الأرشيفية مواد طبيعية ومكتبية غالبا وتحفظ في مكان واحد سواء كان معبدا أو قصرا للملك أو غيرها وفي الأزمنة القديمة لم تميز الحضارات الأولى بين الكتب والوثائق وبعبارة أخرى لم يفرقوا ما بين المصادر وبين أنماط وأساليب التوثيق. [3]

---

[1] إليو، لودوليني، تر أحمد إبراهيم المهدوي، مبادئ وقضايا علم الأرشيف،بنغازي،2018،ص 142.متاح على الرابط: http://www.books.google.dz .. أطلع عليه يوم:2020/03/28.على الساعة:12.47

[2] خولي ،جمال، الوثائق الإدارية بين النظرية والتطبيق، القاهرة، الدار المصرية اللبنانية،1993،ص 58.

[3] سالم، عبود، الألوسي، مالك محمد محجوب. الأرشيف تاريخه، أصنافه، إدارته. بغداد : الحرية للنشر والطباعة،1979، ص .5.6

- **في عهد الإغريق:**

ليس هناك دليل على وجود أرشيفات عند الإغريق القدماء، فالكلمة الإغريقية BIBLIOTHEQUE التي تقابلها اللفظة اللاتينية BIBLIO TEC التي كانت عبارة عن مستودعات لحفظ الممتلكات والمواد التي نسميها بالمواد الأرشيفية كما ان الأرشيفات المنظمة الوحيدة كانت تحفظ فيها أصول القوانين،وكان أسسها القائد **ÉPHIALTES** في حدود **460 ق.م** ،ومن الخطأ الافتراضي أن المعابد أو الأماكن العامة التي كانت مخصصة لإيداع مثل هذه القضايا تعتبر من الأرشيفات.[1]

- **في العهد الروماني:**

أول أرشيف ظهر عند اليونان قد أسسه السياسي الروماني الشهير فاليريوس بوبلي وكولا وذلك في حدود عام 509 ق .م وكان موضعها في إيراريوم أو الخزانة داخل معبد الإله(زحل)وهو إله الزارعة عند الرومان وفي هذا الموضع كانت تحفظ القوانين والمراسيم وأنظمة في مجلس الشيوخ ومستندات المقاطعات ،أما الوثائق التي لها صلة بالدول الأجنبية . فكانت تحفظ في مبنى (الكابيتول)أما في عهد الإمبراطورية فقد تم إنشاء دار تعرف بـ (دار الوثائق القيصرية)أو أرشيف الإمبراطور الذي كانت تودع فيه ليس جميع الأوارق الشخصية العائدة للممتلكات الإمبراطورية فحسب،بل وكافة المستندات الرسمية ،وقد بقيت هذه الأرشيفات قائمة حتى وقت متأخر من عهود إمبراطورية، بالإضافة إلى الأرشيفات البلدية التي كانت تودع فيها القوانين والأنظمة الخاصة بالمجالس البلدية وكذلك القيود والسجلات المالية وشهادات الولادات وقضايا التبني والممتلكات.[2]

1-2-2- في العصور الوسطى:

تعددت السلطات وتنوعت الامتيازات وساد الاقطاع ،فكان لكل ناحية أرشيفها خاص بها الذي يشير الى ما تملكه من حقوق وامتيازات الذي كان يتمثل في وثائق الكنيسة ،اذ كانت الكنائس في تلك الفترة بعيدة عن تقلبات الحروب وبالأمن من السلب والنهب. وفي البلدان الغربية تؤلف أرشيفات الاساقفة والباباوات في الاديرة والكنائس المسيحية جسرا بربط الازمة القديمة بالعصور الوسطى وذلك من خلال استمرار ممارسة العمل الأرشيفي في الدولة البيزنطية حيث كانت الأحوال تتميز بشيء من الاستقرار، فكان هناك نوع من الاستمرارية فالتنظيمات الارشيفية الرومانية ويمكن القول أنه كان لملوك أوروبا نوعان من الأرشيفات كانت موجودة منذ القرن 12الارشيف الثابت، الارشيف المتنقل[3]

[1] السيد،محمد إبراهيم. مقدمة في تاريخ الأرشيف ووحداته. القاهرة: دار الثقافة للنشر والتوزيع، 1998، ص 15.

[2] مرابطي ،حسان الدين.الإطلاع على الأرشيف بين التشريع والواقع: دراسة ميدانية بأرشيف مديرية الموارد المائية بسكرة. مذكرة،ماستر:تخصص:إدارة مؤسسات وثائقية والمكتبات، جامعة محمد خيضر بسكرة،2019،ص 12.

[3] الألوسي،سلم عبود، محجوب، محمد مالك،الأرشيف تاريخه أصنافه وإدارته،المرجع السابق،ص12.

1-2-3- في العصور الحديثة:

- **كندا :**

تأسست دار الوثائق العامة منذ عام 1872 وألحقت بوزارة الزراعة في أول الأمر وتضم المذكورة مجموعات ضخمة جدا من الوثائق الاصلية ،و منذ منتصف القرن العشرين (20) أضيفت إليها مجموعات أخرى عن طريق وضع مناهج طويلة الأمد نظمت بموجبها عملية تصوير الوثائق المتصلة بالتاريخ الكندي مما هو محفوظ بدار الوثائق العامة بلندن وأماكن أخرى كالأرشيفات الفرنسية وفي عام 1873 م عين محافظ مسؤول عن الأرشيف في الأمانة العامة للدولة حيث نهض بمهمة تنظيم الوثائق الرسمية والتاريخية ،و بوجود عدد من الأرشيفات المهمة في مختلف الأقاليم.

- **الولايات المتحدة الامريكية :**

كان هربرت هوفر رئيس الولايات المتحدة الأمريكية قد وضع في 20 فيفري 1933 حجر الأساس لبناء دار الوثائق القومية وصدر القانون المنظم لها كمصلحة مستقلة في 19 جوان 1934 م، وكانت الوثائق محفوظة في مكتبة الكونغرس أول الأمر فنقلت الى البناية الجديدة للأرشيف كافة الوثائق الخاصة بإعلان الاستقلال والدستور والوثائق الخاصة بالمؤشرات الدولية والقارية وقد بلغ حجم هذه المجموعات من الوثائق 800 ألف قدم مكعب وبموجب القانون الصادر عام 1949 ،تم توسيع الصلاحيات التي تمارسها الادارات الارشيفية ،و على الاخص الصلاحيات التي نص عليها نظام الوثائق الفيديرالي الصادر عام 1950 والذي خول امناء الوثائق حقوق تفتيش دوائر الحكومة والدولة واجراء المسح الوثائقي فيها.

- **فرنسا:**

كانت الوثائق قبل الثورة الفرنسية بيد سلطات متعددة ،و قد بلغ عدد هذه الوثائق ما يزيد على 10 ألاف مركز فكان لباريس وحدها الى عام 1970 م ما يقارب 405 مركز وكان من عادة الملوك أن يحملوا وثائقهم معهم .و بناء على ذلك استنسخت الكثير من الوثائق ووضعت في صناديق خشبية وحفظت في اللوفر فكانت بمناسبة النواة الأولى لخزانة الوثائق ونشر الى نابليون اهتم كثيرا بالأرشيف الفرنسي ،بل أراد أن يجعل من الأرشيف القومي لفرنسا أرشيف لأوروبا عامة وضم بعض الوثائق من ألمانيا إيطاليا بلجيكا النمسا إسبانيا.[1]

[1] شاشو، ابراهيم، بن عطية، محمد عدة، واقع الأرشيف في ظل التطورات التكنولوجية الحديثة: مصلحة أرشيف ولاية وهران نموذجا. مذكرة ماستر، تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة ابن باديس،مستغانم2018.2019.،ص 28.29

3-1- مبادئ الأرشيف:

1. **مبدأ المنشأ الأصلي :**

ويعني المكان الذي أتت منه المواد الوثائقية الأرشيفية ويعني أن يكون مسجلا ولقد أسس من خلال الممارسة ليكون الطريق الأفضل لتحقيق التحكم في المواد الأرشيفية يجب الموافقة على مبدأ المنشأ الأصلي والاعتراف بصحته وإتباع الأسباب التالية:

- يمكن المبدأ من التعامل مع الوثائق مجمعة.
- يسهل المبدأ ترتيب الوثائق.

2- تطبيق احترام البنية الداخلية لرصيد أو السلسلة:

إن تطبيق هذا المبدأ تعترضه حالات على الأرشيفي معرفتها حتى يمكنه التعامل معها بكيفية مناسبة لما هو موجود

3- **مبدأ احترام الرصيد :**

هو مبدأ أساسي عالمي معترف به يمثل قاعدة على الأرشيف النظري والتطبيقي وهو يحفظ الأرشيف الصادر من نفس الجهة بالترتيب الداخلي المنجز من طرف الهيئة الأصلية له. .[1]

- **درجات احترام الرصيد :**

1. **درجة الأولى:**

يطبق المستوى الأول لمبدأ احترام الرصيد عندما نترك الوثائق مجمعة كما هي أو عند ما نقوم بعملية تجميعها إذا كانت متفرقة ،و التي نتجت أو صدرت لنفس الشخص أو المؤسسة في إطار نشاطاتهم اليومية، والبعد حقيقي لتطبيقه أساسا على مستوى القيمة الأولية لأرشيف(العمر الأول)و دون إهمال القيمة الثانوية (العمر الثاني).

2. **الدرجة الثانية :**

في هذه المرحلة يتطلب أن تكون كل الوثائق الرصيد الواحدة مجمعة في مكان معين والذي يجب أن يحترم ويعاد تشكيله إذا كان الترتيب الأولي أو الترتيب الأصلي تم تغييره لأسباب ما وعلى مستوى القيمة الأولية للوثائق الجارية والنصف الجارية هذا الاقتراح يكون ضروريا على أن يكون للوثائق ترتيبا أوليا واضحا.[2]

[1] بوطيبة بن قلاوز عبد الله،بن درف أسماء. التحولات التكنولوجية في إدارة العمليات الأرشيفية :دراسة ميدانية بمصلحة ارشيف ولاية مستغانم،2019.مذكرة ماستر: تخصص تكنولوجيا وهندسة المعلومات .مستغانم. ص 29.

[2] شاشو، ابراهيم، بن عطية، محمد عدة. .المرجع السابق، ص 39.

4. مبدأ توارث الدول :

وهو إحلال دولة محل دولة أخرى من حيث ممارسة السيادة في إطار تصفية الاستعمار وبموجبه تلتزم الدول المستعمرة تسليم الأرشيف الذي أنتجته إلى الدولة المستعمرة ،فمصي الأرشيف مرتبط بمصير الإقليم ،وعند ما يسترجع الإقليم يسترجع الأرشيف معه.[1]

5. مبدأ إقليم الأرشيف:

مفاده الأرشيف يبقى في الإقليم أو البلد الذي أنتج فيه،و يتحكم بذلك استرجاعه في حالة ترحيله وظهر هذا المبدأ في القرن الرابع عشر 1152 حيث قام ابن ملك فرنسا والكونت ديسافو تبادل الأرشيف عند ما تبادلا المقاطعات .حيث يتفق المبدأ الأول والثاني هو الأرشيف في المكان الذي أنتج فيه ويعبران على أحقية الشعوب في إنتاجها وتراثها الفكري والفني.

1-4- خصائص الأرشيف

1- **عدم التجزئة :**

أن الأرشيف يكون جزء من الإدارة التي أنتجته أو زودت بها فلا نستطيع أن نفهم أهميتها الإدارية إلا لكل ،ولا تستطيع هذه الوثائق أن تخبرنا بشيء آخر غير الصدق ،وذلك لأن الأرشيف هو الأوراق التي كتبت أو استعملت في أثناء إجراء إداري.

2- **الصحة :**

من خصائص الأرشيف الحصانة أو الوصاية المتميزة فالوثائق تحفظ لقيمة معلوماتها تحت وصاية الشخص أو الأشخاص المسؤولين من ذلك الإجراء وخلفائهم الشرعيين وهذا افتراض منطقي لأنه هو الذي يميز بين الوثيقة الأرشيفية والغير الأرشيفية.

3- **النشأة الطبيعية:**

فالأرشيف ليس وثائق جمعت بطريقة غير طبيعية مثل الأشياء التي توجد في المتحف ولكن كون من تراكمات طبيعية للوثائق في إدارات أو مؤسسات نتيجة أغراض إدارية.

4- **العلاقة المتبادلة :**

لأي أرشيف علاقات وثيقة محتملة مع الأرشيفات الأخرى داخل أو خارج المجموعات التي حفظ فيها وتعتمد أهمية الأرشيف على هذه العلاقات[2].

5- **التسلسل :**

تكوين الوثائق وتجمعها الطبيعي يكسبها نوعا من التسلسل داخل المجموعة الأرشيفية ولا يمكن للباحث أن يستعين بموضوع معين على الوثيقة بمفردها

[1] شاشو، ابراهيم، بن عطية، محمد عدة. :المرجع نفسه،ص.40.

[2] قاني مخطارية، دوار فاطمة. حفظ الوثائق الأرشيفية في المصالح الولائية: دراسة ميدانية مصلحة أرشيف ولاية مستغانم نموذجا،2015.2016.مذكرة ماستر: تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق:مستغانم.ص14.

6- **الندرة:**

الوثائق الأرشيفية فريدة من نوعها لا يمكن أن توجد مكرر في إدارات ودور أخرى وعلى هذا الأساس تبقى الوثيقة دليلا يميز الجهة المنتجة لها تحمل أفكارها نشاطاتها وتوقيعها الرسمي عكس الوثائق المطبوعة لا يمكن أن توجد وثيقة الأرشيفية في مناطق مختلفة بنفس الشكل ونفس المحتوى وبأعداد كبيرة فنجد فقط النسخ التي تنتجها الإدارة خلال قيامها بنشطاتها علما أن لكل هيئة خصائصها واختصاصاتها والمجال التي تغطيه وإذا كان هذا الاختلاف بين هيئة وأخرى فإنه داخل الهيئة الواحدة لكل مصلحة أو مكتب اختصاص أو جانب من النشاط هذه الهيئة ومن جهة أخرى فإن تاريخ الوثائق صفة أخرى تعرف بين ما أنتج في يوم وأخر.[1]

2- أشكال الأرشيف وجمعياته

2-1- أنواع الأرشيف: ينقسم إلى 03 أنواع وتتمثل في:

2-1-1. **من حيث المصدر:** يوجد نوعين هما

1. **الأرشيف العام** :

هي المجموعات الأرشيفية التي تمتلكها وتديرها الدولة او الوزارات أو الهيئات والمؤسسات العمومية تشمل كل إنتاج فكري تابع للإدارة بمعنى آخر كل الوثائق الصادرة عن السلطة العامة.

2. **الأرشيف الخاص:**

هو أرشيف صادر عن جهات غير رسمية، اي صدرت من أشخاص طبيعيين، فيضم أرشيف أشخاص، العائلات والمؤسسات الخاصة .وقد أصبحت تعطى عناية كبيرة بهذا الأرشيف مثل أرشيف الشخصيات السياسية، العلمية الفكرية، حيث يعتبر هذا الأرشيف ملكا خاص .حيث تخصص لها حيزا في الأرشيف.

إن أرشيف الوطني مكون 1988 ولقد نص قانون الأرشيف الجزائري من أن أرشيف عام وأرشيف خاص يكتسيان نفس القيمة ويعتبران ملكا عاما لايجوز بيعه أو إتلافه ويعاقب القانون على ذالك.[2]

2-1-2. **من حيث النشاط:** وتوجد العديد من الأنواع نذكر أهمها:

1. الأرشيف التاريخي :

يمثل الوثائق التاريخية لتاريخ الامم والشعوب بحيث يعتبر مصدر للبحوث والدراسات العالمية وكذا التاريخية من طرف الباحثين ويمكن الاستفادة منه بطرق قانونية .

[1] دلهوم، انتصار .تسيير الأرشيف في المؤسسات العمومية والإدارات العمومية دراسة ميدانية بولاية سوق أهراس، ص 76.

[2] بوسمغون، إبراهيم. تكنولوجيا المعلومات وتطبيقاتها في مجال الأرشيف: ولاية قسنطينة نموذجا. مذكرة مقدمة لنيل شهادة الماجستير في علم المكتبات.: تخصص: إعلام آلي وتقني. الجامعة منتوري قسنطينة،2009.ص 25.

2. أرشيف الآداب و الفنون :

يضم كافة الوثائق التي تتصل بالحركة الثقافية للجمعيات الثقافية ووثائق الشخصيات البارزة في ميادين الثقافة والشعر والأرشيف الفني فيحتوي على وثائق النوادي الفنية والموسيقى والفنون ،كفنون السينما،النشاطات الفنية تشكيلية كالرسم والنحت .

3. الأرشيف السياسي:

ويتضمن وثائق الاحزاب ،الجمعيات والهيئات السياسية و الوثائق السياسية لرجال السياسة المشهورين.

4. الأرشيف التجاري:

ويضم وثائق الوزارات والمؤسسات والدوائر الحكومية بأنواعها والجمعيات والمعاهد والهيئات المختلفة،وكذلك الشركات والمصالح التي تمارس أنشطة الإدارية.

5. الأرشيف السياسي:

ويضم وثائق الأحزاب والجمعيات والهيئات السياسية ،و الوثائق الشخصية للبارزين في النشاطات السياسية ،و يمكن أن يضم المعاهدات والاتفاقيات المعقودة مع الدول الأجنبية ومنه الاجتماعات السياسية المهمة.

6. الأرشيف ديني:

و يضم الوثائق الدينية الصادرة عن الوزارات والمؤسسات والجمعيات والهيئات الدينية لكافة الطوائف والمدارس الدينية.

7. الأرشيف القضائي:

و يضم وثائق وزارات العدل والمحاكم والهيئات التشريعية والقضائية وكذلك القوانين والانظمة والمحاكم الخاصة ما يتصل برجال القضاء وما إلى ذلك .

8. أرشيف العسكري:

ويضم وثائق وزارة الدفاع والطيران والبحرية والحروب، الأسلحة بأنواعها والاختراعات العسكرية الخطط العسكرية. وغير مما يدخل في هذا المجال ،ويتسم هذا الأرشيف بالسرية التامة.[1]

9. أرشيف المؤسسات :

يعتبر أرشيف المؤسسات أرشيف عمومي وفي نفس الوقت أرشيف خاص كما ورد في القوانين الدولية لأنه ينتج من طرف المؤسسات والهيئات والجماعات المحلية سواء عمومية أو خاصة، منذ العشرية الأخيرة أعطيت له أهمية كبيرة وبصفة محددة الأرشيف الاقتصادي في الحقيقة أن التوعية بأهميته وباستثناء هذا النوع من الأرشيف قديم قدم الزمان، أول من اهتم به هم الإيطاليون بالإضافة إلى

[1] بن دوف أسماء، بوطيبة بن قلاوز عبد الله، التحولات التكنولوجية في إدارة العمليات الأرشيفية: دراسة ميدانية بمصلحة أرشيف ولاية مستغانم، مذكرة لنيل شهادة ماستر في علم المكتبات: تخصص تكنولوجيا وهندسة المعلومات، جامعة عبد الحميد بن باديس،مستغانم.2019.ص 28.27.

الألمان ،أقدم الأرصدة التي كونت كانت ملك للمؤسسات والشركات الكبرى وخاصة البنوك ابتداء من القرن السابع عشر في إيطاليا ،وفي قرن ثامن عشر في ألمانيا وهولندا، أما فرنسا قد اهتمت بأرشيف المؤسسات في السنوات 1973 إلى 1990 في مصالح خاصة بالحفظ المؤقت وقد صدرت مجلة كدليل أرشيف مؤسسات سنة 1980 من طرف الأرشيفيون الفرنسيون.

إن المؤسسات مهما كان حجمها ونوعها فهي ملزمة بالاحتفاظ بأرشيفها لغرض استخدامه لإثبات حقوقها ،لذا اوجب تحديد سياسة لحفظ أرشيف المؤسسات .[1]

10. الأرشيف الإداري:

هو ذلك الأرشيف الذي يتناول مختلف الوثائق الإدارية كالوزارات المؤسساتية والدوائر الحكومية وكذا الجامعات والمعاهد والهيئات المختلفة وأيضا الشركات والمصالح التي مارست ولا تزال تمارس نشاطاتها الإدارية ،بمعنى هو كل الوثائق الناتجة عن الجهات الإدارية [2]

3-1-2. من ناحية شكل الوعاء:

يهتم هذا النوع من الأرشيف بنوع الوعاء حامل للمعلومة أرشيفية حيث يختلف من وعاء إلى آخر وتتمثل في الأنواع التالية:

1)الأشرطة السمعية البصرية:

تضم الأفلام بجميع أنواعها من أفلام السينما أفلام وثائقية، وتضم الميكروفيلم، الميكروفيش وأشرطة فيديو.

2) الصور الفوتوغرافية:

يضم كل الصور ذات أهمية كالبطاقات البريدية،الصور المأخوذة من الجو. [3]

3)وسائط التخزين الإلكترونية :

يضم كل الوثائق المحمولة على الوسائط الإلكترونية كالأقراص الضوئية (الديفيدي وألسيدي)القرص الصلب،الأقراص المرنة

---

[1] تاقة مليكة، مناجمنت أرشيف التأمينات الاجتماعية لوكالة وهران: إشكالية الإتلاف، مذكرة لنيل شهادة ماجستير في علم المكتبات والعلوم الوثائقية، جامعة ألسانيا،وهران.2012.ص 37.

[2] بحيح فاطمة الزهراء، بن عروس الجوهر، رقمنة أرشيف البنوك: التنمية المحلية(BDL)فرع مستغانم وحدة رقم 834 دراسة حالة، مذكرة لنيل شهادة الماستر في علم المكتبات :تخصص نظم المعلومات وتكنولوجيا الحديثة و. التوثيق. جامعة عبد الحميد بن باديس،مستغانم.2016.ص 25.

[3] حافظي، زهير. الأنظمة الآلية ودورها في تنمية الخدمات الأرشيفية: دراسة تطبيقية بأرشيف بلدية قسنطينة. مذكرة دكتورة، جامعة منتوري،قسنطينة،2008،ص 33.32.31.

4) **الوثائق المطبوعة:**

يقصد بالوثائق المطبوعة تلك الوثائق التي أنجزت عن طريق استخدام مختلف آلات أو عن طريق الحاسوب مثل الوثائق الإدارية،وأصبحت الوثائق المطبوعة مع مرور الوقت مصدرا أساسيا من المصادر التاريخية يعتمد عليها الباحثون في دراستهم.

5) **الوثائق السمعية البصرية:**

هي الوثائق السمعية البصرية هي فئات من أوعية المعلومات غير التقليدية تقوم على تسجيل الصوت أو الصورة المتحركة،أوكلاهما معا بإحدى الطرق التكنولوجية الحديثة الملائمة،بحيث يطلع عليها بالأرشيف الجديد.

6) **المصغرات الفيلمية:**

عبارة عن أسلوب تعامل تقني حديث مع مصادر المعلومات يعتمد على تسجيل العديد من مصادر المعلومات على أفلام خاصة بمساحة صغيرة جداً وحفظها في أماكن صغيرة واسترجاعها بسرعة عند الضرورة.

7)الوثيقة الإلكترونية:

تختلف بنية الوثيقة الإلكترونية إختلافاً جذريا عن بنية الوثيقة التقليدية وذلك أن مضمون الوثيقة التقليدية يسجل على وسط ورقي في أغلب الأحيان ويستخدم الموثق رموزاً معينة للدلالة على مضمون الوثيقة كالأحرف الأبجدية مما يسمح بقراءة ا بقراءة الوثيقة مباشرة دون وسيط،في حين أن مضمون الوثيقة الإلكترونية يتم تسجيله برموز إلكترونية مثل الأرقام الثنائية.[1]

الذي يتمثل في عنصرالأرشيف الإلكتروني الذي يتم التطرق عليه في جانب التقنيات الحديثة في مجال الأرشيف .

2-2- أعمار الأرشيف :

2-2-1. **أرشيف العمر الأول أو الحي:**

هي الوثائق المنتجة يوميا أو ذات الصياغة الحديثة العهد في مختلف الهيئات والمؤسسات فهي الوثائق التي لازالت مصالحها تستعملها وتحتاجها يوميا عند الحاجة على سبيل المثال هناك شؤون في طور البحث أو ملفات لم يتم دراستها وملفات تم تصنيفها على مستوى الموظفين حيث مازالت في إطار التحليل أو على مستوى الأمانة. تشكل هذه الوثائق ما يسمى الأرشيف الحي وتتأرجح مدة خفضها على مستوى المصالح المختصة لدراستها من سنتين حتى 10 سنوات (أحيانا أسابيع تكفي)وكما هو الحال بملفات الموظفين التي تبقى محفوظة لمدة 40 سنة ما يعادل مدة المسلك المهني كما تم الإشارة إلى ذلك

[1]. حافظي، زهير؛ المرجع نفسه. ص 34.35.36

في المنشور رقم 1 المؤرخ في 15 سبتمبر 1990 الذي ينظم تسيير الوثائق المشتركة المنتجة على مستوى الإدارات المركزية. لكن رغم قصر لمدة إبقاء الوثائق على مستوى المصالح التي تنتجها وتحفظها تشهد المرحلة الأولى لتكوين الأرشيف استعمالا وافرا، وفي هذه الفترة بالذات تتعرض الملفات للإهمال يترتب عنه انعكاس وخيم حيث يؤدي إلى عدم احترام قواعد التصنيف.

2-2-2. أرشيف العمر الثاني أو الوسيط:

يعد هذا النوع أكثر أهمية فهو يتألف من مجموعة من الوثائق المنتجة أو المستلمة من طرف مختلف قطاعات النشاط الوطني أو محفوظة لديهم منذ 1962 إلى السنوات الإثنين أو الثلاث الأخيرة وهي أكثر الوثائق حجما لذا يجعلها أكبر مصدر إنشغال للمسيرين لأنها تطرح مشكل الصيانة وعلاوة على مشاكل التصنيف والحفظ وبالفعل نلاحظ أن أرشيف الطور الأول يتعرض للتلف طفيف خلال ترحيلة يلبي التحويل الإداري لأن هذا النوع من الأرشيف مرتبطا إرتباطا مباشر بالمصالح التي تعمل به في حين توحي مثل هذه التحويلات على ضعف أرشيف الطور الثاني ليس لسبب الضياع الذي يتعرض إليه بل أيضا التلف الذي يكون ضحيته[1]

3-2-2. أرشيف العمر الثالث:

ويطلق عليه الأرشيف التاريخي يتكون من الوثائق التي تفوق مدة وجودها 15 سنة،والتي أصبحت غير ضرورية لسير شؤون المصالح ويتم دفعها إلزاميا إلى مصلحة الأرشيف الولائي أو الوطني ولا يحق حذف الوثائق المفتقرة إلى قيمة الأرشيف إلا بتسريح مكتوب صادر عن مؤسسة الأرشيف الوطني.تتميز هذه المرحلة بانتهاء القيمة الإدارية لبعض الوثائق فتصبح عديمة القيمة سواء كانت تاريخية،أو ثقافية،حيث يتم حذفها وذلك بإتباع طرق المستعملة للحذف أو الإقصاء وفي المقابل تظهر إرثا ثقافيا آخر.[2]

2-3- الجمعيات العلمية والمعاهد الأكاديمية المتخصصة في الأرشيف:

2-3-1. الجمعيات العلمية:

تكونت في دول كثيرة من العالم المتقدمة والنامية مجموعة من الجمعيات المختصة في مجال الأرشيف ،تعمل على ربط ذوي التخصص علميين والمهنيين لتعريفهم بالتطورات الحديثة فيه وتنظيمه وتبادل المعلومات والخبرات وطرق الممارسات المهنية وإلا أن بعضها لم تستمر خاصة في الدول النامية أما الدول المتقدمة أشهر جمعياتها :

- **جمعية الأرشيفيين الأمريكيين SAA:**

والتي تأسست سنة 1936 وتصدر مجلة الأرشيفيين الامريكيين منذ 1938.

[1] طويلي، محمد. منشور رقم 3 المؤرخ في 02 فبراير 1919 الخاص بتسيير وثائق الأرشيف، مديرية العامة للأرشيف الوطني، ص 27.28.

[2] مرابطي حسان، الاطلاع على الأرشيف بين التشريع والواقع دراسة ميدانية بأرشيف مديرية الموارد المائية بسكرة، مذكرة لنيل شهادة الماستر: تخصص إدارة المؤسسات الوثائقية والمكتبات. جامعة محمد خيضر،بسكرة.2019.ص 20

- **جمعية المحفوظات البريطانية SRS:**

تصدر مجلة الأرشيف منذ عام 1949.

- **جمعية الأرشيفيين البريطانية SBA:**

تأسست سنة 1954 وتصدر مجلة Society of Archivistsمنذ 1955.

2-3-2. المعاهد الأكاديمية:

هنالك معاهد منتشرة حول العالم ومدارس متخصصة في مجال الأرشيف تضطلع بهذه المهنة

- **مدرسة الوثائق بباريس:**

أنشأت سنة 1821 وكانت تابعة للأرشيف الوطني ومدة الدراسة بها سنتين وقد أغلقت سنة 1823 تم أعيد فتحها سنة 1829 ليصبح عدد السنوات بها ثلاث سنوات تم أصبحت فيما بعد معهدا مستقلا عن الأرشيف الوطني تقدم شهادة معترف بها تسمى Diplôma d archivist paliograph.

- **مدرسة المكتبات والأرشيف في لندن:**

مدة الدراسة بها وتمنح شهادة خاصة في تسيير وإدارة الأرشيف .

- **معهد تدريب الوثائقيين ببغداد:**

أنشئ وفقا لتوصيات الفرع العربي الإقليمي للوثائق.

- **الأقسام والمعاهد المتخصصة:**

وتدرس الأرشيف كمقياس وهي منتشرة عبر العالم.[1]

1.4. **أهمية الأرشيف:**

للأرشيف أهمية كبرى في حياة الأفراد والدول فهو يلعب دورا مهما على صعيد جميع المجالات العلمية والاقتصادية والثقافية ؛إذ به يمكن استشراف جميع الأمور الإدارية أو العلمية؛ فهو بذلك يشكل قيمة إثباتيه ،وعليه عملت كل القطاعات الإدارية على إعطاء أهمية كبرى للأرشيف الذي أصبحت تعتمد عليه في تسييرها الإداري ،باعتمادها على الوثائق

1) **أهمية رسمية قانونية:**

يعتبر كشهادة إثبات حق من الحقوق وهي نتيجة طبيعية وحتمية للممارسة الإدارية لدى المؤسسات المتنوعة والمختلفة النشاط وذلك خلال مراحل معينة وهو الكفيل بإثبات ما تحقق أثناء تلك المراحل فيعكس نشأتها ونموها.[2]

[1] دلهوم، إنتصار. تسيير الارشيف في المؤسسات والإدارات العمومية. المرجع السابق،ص 157.158.

[2] ينجح،خديجة. قصري، فطيمة. واقع إستخدام التسيير الإلكتروني للوثائق في ميدان الأرشيف: دراسة ميدانية لأرشيف وزارة العمل والتشغيل والضمان الاجتماعي. مذكرة ماستر في علم المكتبات .جامعة جيلالي بونعامة خميس مليانة،2016/2015.ص 41.

2) **الثقافية والبحث العلمي:**

تمثل وسيلة هامة لدراسة التطور السياسي والاجتماعي والاقتصادي لبلد ما وهو أيضا وسيلة لنقل تراث الماضي لما تحتويه من أفكار ومبادئ ،كانت أساس بناء الحكومات فالأرشيف يعتبر ثروة ثقافية كالكتب وخزائن المتاحف ،إلا أنها ولدت نتيجة نشاطات الحكومات والأفراد.[1]

- أما الأرشيف في ميدان البحث العلمي من بين المصادر التاريخية الأساسية إذ تشكل مادة حية لتاريخ الإنسانية فهو يعكس لنا الحيات اليومية للشعوب والأمم في شتى مظاهرها اجتماعيا اقتصاديا وسياسيا وثقافيا يعتمد عليها الباحث بالدرجة الأولى لأنها غير قابلة للتغيير.

3) **أهمية من الناحية الرسمية وعلى مستوى الحكومة:**

الأرشيف يمثل ذاكرة الأمم والحكومات فهو يحتوي على معلومات تزداد قيمتها حسب تطور هذه الدول وبإمكانه أيضا معالجة موضوعات ذات طابع اجتماعي فهو يسير طريقنا في الحاضر ويساعدنا على حل مشاكلنا في المستقبل.

4) **على مستوى الأفراد:**

يثبت الأرشيف حقوق الأفراد وملكياتهم وامتيازاتهم وتثمين الأرشيف وسيلة لإثبات الهوية ومن يمتلك المعلومة يمتلك الحكم ومن يمتلك الحكم يسيطر ويفرض نفسه، والوثيقة الأرشيفية هي لسان الماضي وجواب الحاضر.[2]

3- التكنولوجيا والأرشيف

3-1- التقنية الحديثة في مجال الأرشيف:

- **ظهور الحاسوب وأسباب انتشاره في مجال الأرشيف:**

يستخدم الحاسوب في مجال الأرشيف باعتبار هذا الأخير من بين نظم المعلومات، ويستخدم في عمليات استرجاع المعلومات الببليوغرافية عن الوثائق، ولقد أستخدم الحاسوب في العديد من الأرشيفات ودور الوثائق الوثائقية. إلا أن هذه الأرشيفات لا تزال بعيدة عن طرح فهارسها على الشبكة أو على الخط المباشر كما تفعل المكتبات الآن، ومع ذلك فإنها تسير الأن في نفس الاتجاه التي سارت فيه المكتبات الذي أكده هذا التوجه المدير العام للأرشيف الوطني. [3]

- **تأثير الإعلام الآلي على ميدان الأرشيف :**

دخل الإعلام الآلي قطاع الأرشيف كباقي القطاعات الأخرى لمعلومات، وقد أثر الإعلام الآلي على قطاع الأرشيف من عدة نواحي أهمها:

[1] الشريف، عبد المحسن. تقييم وثائق الأرشيف: معايير وإجراءات. القاهرة: دار الثقافة العلمية، 2001. ص 248

[2] قبسي، محمد. علم التوثيق في الوطن العربي. بيروت: دار الآفاق الجديدة، 1980. ص 125

[3] بودوشة، أحمد. التشريعات ودورها في دعم وتطوير الأرشيف الوطني. مجلة المكتبات والمعلومات. مج 02،ع 03،ديسمبر 2003 ،ص 109

- **أتمتة الجانب الإداري:**

وذلك بتسيير الموارد البشرية إصدار الوثائق المختلفة، تتبع المراسلات من البريد الصادر وذلك عن طريق حزمة أو قيس المحترفة.

- **أتمتة الجانب الفني:**

الذي جاء من الاستفادة من البرمجيات التي طورت وطوعت من النسخ التي استعملت في مجال المكتبات ومراكز المعلومات مثل: مايكرو ايزيس س يدي أس لليونسكو

3-2- **تأثير تكنولوجيا حديثة على قطاع الأرشيف:**

1. تأثير وسائط التخزين الحديثة:

أمام كثرة وتنوع الوسائط الإلكترونية وجب تحديد بدقة نوع الوسائط التي سوف تستخدم أمام ظاهرة التقادم السريع في تكنولوجيا المعلومات، وذلك بمعرفة خصوصياتها، كيفية حفظها أكبر وقت ممكن.

2. تأثير الخدمات:

بتزايد الطلب على الوثائق الأرشيفية ،تنوع مواضيعها ،تنوع المستفيدين وظهور الخدمات عن بعد بالإضافة إلى سرعة توفيرها بدقة في عصر يتسم بالسرعة وعدم الانتظار[1]

3. تأثير الانفجار الورقي:

الكم الهائل من الوثائق التي تصل إلى مرحلة الفوز النهائي والتي تفرض مجهودا في التقييم والمعالجة الفية في أسرع وقت ممن وهذا يفرض عددا كبيرا من الأرشيفيين ذوي كفاءات العلمية الفية والعلمية العالية لقيام بهذه الأعمال على أحسن وجه وإنجاحها، ومنه ضرورة تتبع الوثائق مذ نشأتها حتى مرحلة الأرشفة النهائية وهذا صعب التحقيق في النظم الكلاسيكية.

4. تأثير المعالجة الآلية:

أمام المعالجة الفنية عدد من الوثائق في تزايد مستمر في آجال قصيرة وبطريقة فنية جيدة لمحافظة عليها، تخزينها واتاحتها لمستفيدين عند الطلب، لذا استوجب إدخال المعالجة الآية في مراكز الأرشيف.[2]

5. الأرشيف الالكتروني:

1.5. مفهوم الأرشيف الإلكتروني:

يعتبر سلسلة من الرموز المسجلة على أوعية إلكترونية وهو الوحدة الأساسية للمعلومة في عالم المعلومات الإلكترونية ما يستلزم اللجوء إلى وسائل تكنولوجيا لقراءتها والاستفادة منها فهي تختلف عن الوثائق الورقية التي تحتوي معلومات قابلة للاستغلال فورا ودون تجهيزات خاصة، ويتميز هذا النوع من الوثائق (الوثائق الإلكترونية)بالعملية وسرعة الاستغلال والنسخ والتعديل والتبادل كما يقضي على الحيز المكاني نتيجة لطاقة الاستيعاب الهائلة لها، إلا أنها تتميز بالصعوبة والتعقد بالنسبة

[1] مكيلودي، زكية. إسهامات تكنولوجيا المعلومات في أمن الأرشيف: دراسة حالة أرشيف ولاية مستغانم نموذجا، مذكرة ماستر ،تخصص: نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة عبد الحميد بن باديس مستغانم،2016 /2017، ص40.

[2] مكيلودي، زكية؛ المرجع نفسه.ص.41.

للوصف الأرشيفي كما أن بعضها لا يتميز بعضها بالسرية في ظل عدم وجود نظام صارم للاطلاع عليها الأرشيف الإلكتروني أو الأرشفة الآلية أو الأرشفة الإلكترونية هي عبارة عن مجموعة من النظم لغدارة الوثائق بحيث نبدأ بتصوير وفهرسة الوثائق وتحويل بياناتها بحيث تكون متاحة للمستخدم يمكن الاطلاع عليها واستعمالها وتداولها إلكترونيا وبسهولة، ومن خلال نظام الأرشفة الإلكترونية يتم الاحتفاظ بالوثائق على شكل ملفات إلكترونية وبالتالي يتم استغلال الاماكن المخصصة لحفظ الوثائق الورقية، واستخدمها في نشاطات حيوية أخرى. .[1]

2.5. أنواع الأرشيف الإلكتروني:

- **الأرشيف الإلكتروني على الخط:**

يتبع فيه حفظ جميع الوثائق بصفة مستمرة على الخوادم بحيث يمكن استرجاعها من خلال الطرفيات الحاسوبية المتصلة بالشبكة، وهو الأرشيف الذي يؤدي فيه كل الأعمال بالحاسب الآلي ويعتمد بدرجة كبيرة على الأنترنت والاجهزة الإلكترونية الحديثة في توفير الخدمة لمن يطلبها .

- **الأرشيف شبه الإلكتروني :**

هو الأرشيف على الخط المباشر أي على الأقراص المدرجة وهي On line Archivinge on cds وهدا النوع يستخدم برامج أرشيف إلكترونية مثل Rx cd managare وهو أيضا الأرشيف التي يؤدى فيع الاعمال يدويا مع الاستعانة ببعض الآلات في الأجهزة الإلكترونية الحديثة، بمعنى هو عبارة عن مزج بين الأرشيف التقليدي والإلكتروني.[2]

2.6. خطوات الأرشيف الإلكتروني:

* وضع خطة مدروسة ومفصلة ومقسمة إلى فترات زمنية بحيث تشمل على كل متطلبات عمل أرشيف ومعاينته (تجهيزات مادية وكوادر بشرية)

* إعداد الكادر البشري المكلف بعمل الأرشيف وتأهيله

* تحديد الهدف من وجود الأرشيف غير تحديد الغاية من وجود الأرشيف وما ينتج وما يصنعه.

* وضع لكل فترة زمنية خطة عمل خاصة بها وتحديد الوثائق التي سوف تدخل في العمل

* أخذ نسخة إلكترونية من الوثائق عن طريق الأجهزة المخصصة لذلك

* تخزين الوثائق في نظام الأرشفة الإلكترونية الذي يتيح عملية الفهرسة من خلال كلمات مفتاحيه وتصانيف إلكترونية لكل وثيقة.

---

[1] بودويرة طاهر؛ تثمين رأس المال البشري في ميدان أرشيف بين التكوين وممارسة المهنة، مذكرة لنيل شهادة الماجستير في علم المكتبات :تخصص نظم المعلومات، جامعة منتوري،قسنطينة.2009.ص 56.55.

[2] محمد مصطفى محمد علي ،الأرشيف الإلكتروني ،ص 03.

* اختيار الوثائق التي سوف تجرى عليها عملية الأرشفة الإلكترونية ليس بالضرورة تحويل كل الأرشيف التقليدي إلى أرشيف إلكتروني

* تحديد المعوقات التنظيمية والتقنية.

* تأكيد الحماية القانونية للأرشيف.[1]

3.5. خصائص الأرشيف الإلكتروني:

* توفير الحيز المكاني واستغناء عن الأرشيف التقليدي وأكوام المعاملات والملفات.

* سهولة وسرعة نقل الرسائل والوثائق الإلكترونية بين فروع المؤسسة أو خارج نطاقها.

* سهولة الوصول إلى الوثائق الإلكترونية أي كان موقع مستفيد أو المستخدم لهذه الوثائق.

* مراقبة الوثائق وتحولاتها ومتابعتها وتطورها ومعرفة سير المعاملات داخل المؤسسة .

* تعدد نقاط الوصول للوثائق المحفوظة إلكترونيا مما يسهل استرجاع الوثائق.

* التقليل من أخطاء ومخالفة الأنظمة ومراجعة الدوائر الحكومية من قبل المستفيدين.

1.5. فوائد الأرشيف الإلكتروني :

* حفاظ على الوثائق النادرة من التلف دون الحجب للوصول إليها من قبل الراغبين في دراستها.

* سهولة الاسترجاع للوثائق من خلال الموضوع أو جهة المصدرة لها أو التسلسل الزمني.

* الاقتصاد في استعمال الورق واستهلاكه. سرعة في تقديم الخدمات للمستفيدين

* المرونة الفائقة في التعامل مع المعلومات والتحديث الدوري لها.

* ارتفاع مستوى السرية مقارنة مع بأنظمة حفظ الوثائق التقليدية.

* السرعة الفائقة في الإجابة على أسئلة الباحثين باعتبارات الإعلام الآلي بإمكانه تأدية عمليات بحث في نفس الوقت وجيز.[2]

5.5. أسباب التوجه إلى الأرشيف الإلكتروني:

1. المعطيات العلمية والعملية:

- التعامل المباشر مع الوثائق وما يترتب عنه من أخطار ويقلل من عمرها وربها يؤدي إلى ضياعها.

[1] لعيدي فاطمة، بن نونة فضيلة، ترتيب وتصنيف ارشيف المؤسسات الاقتصادية أرشيف مؤسسة سوناطراك بمصلحة GP1-Z أرزيو نموذجا، مذكرة لنيل شهادة ماستر في علم المكتبات والمعلومات تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة عبد الحميد بن باديس ،مستغانم. 2016.ص 68

[2] لعيدي فاطمة، بن نونة فضيلة؛ المرجع نفسة .ص 69

- حماية الوثائق من الأخطار التي تتعرض لها في المعالجة التقليدية(التلف، ضياع، سرقة...إلى غيره من المخاطر)
- توفير نسخة احتياطية من الوثائق[1]
- تعدد أنواع الوثائق واختلاف المعالجات في كل نوع من الأنواع، أما في الأرشفة الإلكترونية فنستطيع دمج كل هذه الأنواع في قاعدة ومكان واحد.
- التغيير في نوعية المواد التي تصنع منها الوثيقة، وكما أسلفنا القول بأن هناك مواد تمنح الوثيقة عمرا أطول، وهناك تمنح الوثيقة عمرا اقل.
- النمو المتزايد للوثائق في شتى المجالات.
- اتجاه النشر العالمي إلى النشر عن طريق الصورة الإلكترونية.
- إظهار تفاصيل لا يمكن رؤيتها مباشرة على الورق.
- النفاذ إلى المعلومة عن بعد مع الاطلاع على الوثيقة الأرشيفية نفسها من طرف أكثر من شخص في الوقت نفسه.
- المساعدة في الحفاظ على الوثائق النادرة وسريعة العطب

2. **المعطيات الاقتصادية والمالية:**

- التكاليف المادية العالية نتيجة لكثرة الوثائق الورقية.
- التكلفة الباهظة للأرشفة التقليدية، فالتعامل اليدوي مع الوثائق عملية مكلفة ومرهقة،
- توفير الحيز المكاني التي كانت يشغلها الأرشيف التقليدي.[2]

متطلبات الأرشيف الإلكتروني:

- **كوادر البشرية والفنية والمدربة:**

يجب أن تتوفر كوادر البشرية والفنية والمدربة على استخدام الحاسب الآلي والأجهزة الإلكترونية ووسائل الاتصالات الحديثة في مجال الوثائق و الأرشيف .

- **الاجهزة والمعدات الإلكترونية الحديثة:**

[1] - مولاي أمحمد؛ ختير فوزية. المتطلبات التقنية للأرصدة الأرشيفية: مشروعات رقمنة الأرشيف الجزائري نموذجا. المؤتمر الدولي العشرين للاتحاد العربي للمكتبات والمعلومات. ديسمبر 2009. المملكة المغربية: الدار البيضاء.

[2] - سامية عبد القادر محمد أحمد، سارة شمو شاع الدين. الأرشفة الإلكترونية وواقعها في دار الوثائق بالسودان. المؤتمر الدولي العشرين للاتحاد العربي للمكتبات والمعلومات. ديسمبر 2009. المملكة المغربية: الدار البيضاء.. ص 25

يحتاج الأرشيف الإلكتروني غلى العديد من الاجهزة الإلكترونية ووسائل الاتصال الحديثة لإنجاز وإعداد مهامه بجودة كبيرة وسرعة عالية ،و مثال هذه الاجهزة نجد الحاسب الآلي، الهاتف، الفاكس، الماسحات الضوئية.[1]

- **البرمجيات:**

تعمل أجهزة الحاسب الآلي والمعدات الإلكترونية الحديثة السابقة من خلال حزم برمجية عديدة كبرامج التشغيل والتطبيقات مثل حزمة مايكروسوفت والحزم الإحصائية، ومعالجات النصوص والصور، ومتصفحات الانترنت وقواعد البيانات، وخدمة نقل الملفات وغيرها من البرامج المختلفة.

- **التجهيزات والأثاث والبيئة المناسبة:**

لابد من توفر بيئة وظروف حفظ مناسبة للأرشيف الأرشيف من تهوية جيدة وإضاءة وأثاث وتجهيزات ومكاتب تساعد العاملين الجمهور من الوصول للأهداف المرجوة.[2]

3-3- **الأخطار التي يتعرض لها الأرشيف:**

ملاحظة: قبل الخوض في هذه النقطة يتم التنويه لأهميتها والهدف من ذكرها وذلك لأن الأرشيف الورقي هو الذي سوف يتم قمنته ويصبح أرشيف الإلكتروني وبالتالي عند الحافظة على هذا النوع من الأرشيف فنحن نحافظ على الأصل للأرشيف الإلكتروني.

وعليه فهناك عدة أخطار وكوارث يمكن أن يتعرض لها الأرشيف، منها ما هو ناتج عن عوامل طبيعية تحدث فجأة، كما أنه هناك عوامل بيولوجية، ومنها ما يحدث نتيجة لإهمال أو تهاون أو تكون غير مقصودة، إلا أنها تتسبب في تلف وضياع وثائق أرشيفية وتتمثل في:

1. **الفيضانات** :

وتعد من أكثر الأخطار التي تتسبب في مشاكل عظمى للوثائق، كونها ظاهرة من الظواهر الطبيعية والتي تسببها الامطار أو السيول أو الإهمال وعدم الالتزام بالضوابط والمعايير ولتفادي تعرض قاعات الأرشيف للفيضانات والتقليل من أضراره يجب مراعاة التالي:

- عدم وضع قاعات الأرشيف في قبو المبنى.
- مراعاة عدم وجود ثغرات تسمح بتسريب مياه الأمطار الى المبنى.
- تركيب نظام كشف تسرب المياه إلى القاعات
- عدم تمرير أنابيب المياه عبر قاعات الأرشيف.

[1] محمد مصطفى محمد علي ،الأرشيف الإلكتروني، ص07

[2] محمد خير، عزات كساب، متطلبات نجاح نظام إدارة الوثائق الإلكترونية في الهيئة العامة للتأمين و المعاشات –فلسطين-مذكرة لنيل شهادة الماجستير في إدارة الأعمال ،الجامعة الإسلامية،غزة.2008.ص 51.

●وضع خطة للطوارئ لمواجهة الفيضانات. .[1]

2. الحرائق:

وهي ثاني عامل خطير يأتي بعد الفيضانات، حيث يتسبب في تلف الوثائق بسرعة كبيرة جدا، كما لا يمكن التحكم في صيانة الوثائق المحروقة كما هو الحال بالنسبة للفيضانات كومها تحدث إما بسبب الإهمال وعدم الالتزام بضوابط ومعايير الأمن والسلامة أو عمدا بفعل فاعل.[2]

3. الزلازل:

من الظواهر الطبيعية فمنها الهزات البسيطة التي قد لا يشعر بها الإنسان ولكن تقوم برصدها أجهزة الاستشعار الدقيقة ومنها الهزات الأرضية الشديدة وهذه قد تؤدي إلى هدم مراكز الأرشيف وهذا ما يسبب ضياع الوثائق الأرشيفية المهمة ،وما يهمنا هنا هو الآثار التي يمكن أن تنجم عن الزلزال داخل مراكز الأرشيف من خسائر مادية وبشرية بالإضافة إلى إتلاف كل محتويات المركز من مستندات ووثائق وملفات، ومن الحقائق المؤكدة[3]

4. العوامل البيولوجية :

وتتمثل بصفة خاصة في القوارض والحشرات التي تتسبب في تلف الوثائق الأرشيفية وهي:

- **الحشرات والكائنات الحية الدقيقة :**

يتزايد وجود الحشرات والكائنات الحية الدقيقة في الأوساط الدافئة الرطبة،المظلمة والتي تعاني من سوء التهوية،وتنمو كذلك في الأماكن التي تهمل فيها أعمال التنظيف يظهر تلف الوثائق الأرشيفية الورقية الناتج عن الحشرات كالصراصير بسرعة وللعين المجردة مباشرة بعد إصابتها بينما يظهر تأثير الإصابة بالكائنات الحية الدقيقة (الفطر والبكتريا)ببطء مع مرور الزمن .كما تكون الوثائق الأرشيفية الورقية أكثر عرضة للإصابة بالكائنات الحية الدقيقة،والتي تتسبب في تكسير الألياف السلولوزية بفعل الإنزيمات التي تفرزها لتصبح غذاء لها.

- **القوارض:**

تدخل الفئران والجرذان إلى المخازن بفضل الثقوب الموجودة في الجدران والأسقف لتلتهم الورق بسرعة. فضلا على أنها تتلف ما تبقى منها بإفارازتها القذرة.[4]

5. العوامل البشرية:

هو التصرف النابع عن الإنسان والذي يؤدي إلى إحداث الإضرار البالغة من بينها الحرائق المتعمدة، الإتلاف العمدي أو الإتلاف عن جهل، بالإضافة إلى السرقة التي تعتبر من أخطر المخاطر التي تتعرض لها الوثائق الأرشيفية داخل مراكز الأرشيف، بالإضافة إلى قيامة بالعديد من الأمور وتتمثل في :

---

[1] دليل حفظ الأرشيف، وزارة شؤون الرئاسة، المركز الوطني للوثائق والبحوث. ابو ظبي، الإمارات العربية المتحدة.

[2] دليل حفظ الأرشيف، وزارة شؤون الرئاسة، المركز الوطني للوثائق والبحوث. ابو ظبي، الإمارات العربية المتحدة.

[3] مصطفى أمينة، صادق. إدارة الأزمات والكوارث في المكتبات. القاهرة : الدار المصرية اللبنانية، 2002.ص 44.

[4] عزون زهية، الحفظ الوقائي للوثائق الأرشيفية ،مجلة علم المكتبات،ع06،ص 62.63

- التدخين داخل قاعات الأرشيف مما يتسبب في إحداث حرائق غير متوقعة.
- ترك صنابير المياه مفتوحة، بالإضافة إلا لحرق والتخريب المتعمد والاضطرابات المدنية.[1]

3-4- لإجراءات الوقائية لحماية الأرشيف:

انطلاقا من كل ما سبق ذكره من أخطار وكوارث تهدد الأرشيف ،وجب إتباع خطوات معينة من أجل الحد منها والحفاظ على الأرشيف وحمايته، وبالتالي الحفاظ على ذاكرة الأمة، وهذا في حد ذاته مطلب تسعى كل الدول نحو تحقيقه ولا يمكن ان نحقق الأمن للأرشيف الإلكتروني بدون توفير الحماية للأرشيف التقليدي الذي يعتبر هو الأصل في وجود الأرشيف الإلكتروني فهما وجهان لعملة واحدة من بين هذه الإجراءات نجد:

3-4-1- الحماية من الماء:

- يمنع مرور أنابيب الماء عبر مخازن الأرشيف أو فوقها
- استخدام أجهزة إنذار بالماء لإعلان وجود أي سائل نتيجة انكسار الأنابيب أو حدوث أي تسرب
- يجب أن تكون الأرضية منيعة لمنع أي تسرب للماء أو انتشاره في البناية ويمكن رفع عتبة الأبواب لسد الطريق أما الماء إذا اقتضى الامر.
- عدم تخصيص مكاتب ومصالح الأرشيف في الطوابق الأرضية لتفادي تسرب المياه، و بصفة خاصة مياه الأمطار والفيضانات
- ومن أهم ما يمكن إتباعه، هو بناء مراكز الأرشيف حسب المعايير الدولية ووفق تعليمات الأرشيفي الذي يجب أن يكون حاضرا مع المهندس، لتفادي عدة أخطار كالفيضانات، خطر الانهيار. ...

3-4-2- الحماية من الحرائق:

اعتمادا على شبكة الإنذار المبكر للحريق_يهدف هذا النظام إلى الإنذار المبكر للحريق وهي:[2]

- **كاشف الدخان**: ينطلق عند ظهور الإشارات الأولى للدخان، حتى في حالة التدخين من قبل أعوان غير منضبطين؛ كما يعتبر الأفضل لأنه ينطلق تلقائيا في اللحظات الأولى من الحريق

[1] الوقاية من الكوارث والخطط الأستعجالية، دليل إيفلا،2006.ص.12.

[2] بجاجة عبد الكريم، المبادئ التوجيهية من الكوارث ومراقبتها، دراسة رقم 11.الإمارات:المجلس الدولي للأرشيف، فبراير 2008.ص 16- 18

- **كاشف الحرارة:** لم ينطلق الإنذار إلا إذ تغيرت درجة الحرارة داخل قاعات الأرشيف بازدياد حراري يفوق 15 أو 20 درجة، و في هذه الحالة يمكن أن ينتشر الحريق قبل انطلاق الإنذار.
- **كاشف اللهب:** يترقب الجهاز ظهور اللهب قبل أن يأمر بالإنذار.
- وضع مطافئ يدوية مائية بمقياس لتر في مساحة 200 متر مربع ولا ينصح باستخدام مطافئ الرغوة أو المسحوق بسبب الأضرار التي تلحقها بالوثائق.
- يجب وضع مطفأتين في كل مكان حساس الأولى مائية والثانية من نوع ثاني أكسيد الكربون يستخدم لإطفاء الحريق من مصدر كهربائي أو من أي حريق آخر للتقليل الأضرار في المجموعات .
- تركيب الأبواب وانظمة الحماية المضادة للحرائق قدر الإمكان لعزل الحرائق وإبطاء مفعولها.
- تفكير في تركيب دارة كهربائية خاصة بكل غرفة .

2.1. الحماية من الموارد البشرية:

- التحقق من عدم تدخيل العمال داخل قاعات الأرشيف.
- التحقق من تطبيق الإجراءات الأمنية على موظفي المؤسسة أيضا
- فرض عقوبات صارمة على المخالفين للإجراءات الامنية.
- يجب وضع إشارات إنذار ضد التدخلات الطفيلية.
- توعية الموظفين بضرورة الترقب والحذر في الدور الذي يقومون به بالانطلاق المبكر لإشارة الإنذار.
- يجب تنظيم حلقات تدريبية دوريا للموظفين لإعلامهم وتوعيتهم بما ينتظرهم في حالة الطوارئ.
- تذكير العمال بالأخطار مهما كانت الإجراءات الوقائية.
- القيام بتكوين الموظفين وخاصة الأرشيفين تكوينا اساسيا يؤهلهم لاستعمال التجهيزات لمكافحة الأخطار التي يتعرض لها الأرشيف.[1]
- أما فيما يخص لحماية الأرشيف الإلكتروني من الأخطار فقد تم التطرق إليها في الجانب الخاص خاص بأمن المعلومات في الفصل الأول.

[1] بجاجة عبد الكريم. المرجع السابق .ص 20.21 .19

الفصل التطبيقي : أمن المعلومات بمصلحة أرشيف الصندوق الوطني للتقاعد

تمهيد :

بعد أن تمت الإحاطة بكل ما هو نظري لموضوع دراستنا سوف يتم الانتقال الآن إلى الجانب التطبيقي للدراسة الذي كانت على مستوى مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد و الذي سوف يتم التطرق فيه إلى :

1. التعريف بمؤسسة الصندوق الوطني للتقاعد و مصلحة الارشيف بها
2. دراسة تحليلية للمعيار إيزو 27002 لأمن المعلومات
3. تحليل المقابلة و فق المحاور الكبرى للدراسة و مقارنة المعطيات بمعيار إيزو 27002

1- تقديم مصلحة أرشيف وكالة الصندوق الوطني للتقاعد لولاية تيسمسيلت محل الدراسة

1-1- نبذة تاريخية عن صناديق التقاعد ونظمها:

تم إنشاءه بموجب المرسوم رقم : 223/85 في 20 أوت 1985 المتعلق بالنظام القانوني لصناديق الضمان الاجتماعي والهياكل الإدارية. كما تجدر الإشارة إلى أنه قبل 1983 كانت هناك عدة صناديق للضمان الاجتماعي وهي:

- الصندوق الوطني للمتقاعدين من النظام العام.CAAV
- الصندوق الوطني لتقاعد الموظفين.CGRA
- الصندوق الوطني لتقاعد عمال المناجم.CASOMINE
- الصندوق الوطني لتقاعد الفلاحين. CRMA
- الصندوق الوطني لتقاعد العمال غير الأجراء.CASNOS
- الصندوق الوطني لتقاعد عمال سونلغاز .CAMPS

وبعد صدور قانون 1983 أصبح نظام التقاعد في الجزائر موحد تحت اسم الصندوق الوطني للتقاعد. يتميز الصندوق الوطني للتقاعد بلامركزية عالية يتكون من مصالح ووكالات محلية، ومراكز جهوية للإعلام الآلي والأرشيف. كما خضع لعدة تعديلات في إطار المهام المخولة للصندوق بموجب القوانين والقرارات فإنه يتضمن مديرية عامة مقرها الجزائر العاصمة.

1-2- نظم التقاعد Systems de Retreater :

نظام التقاعد في الجزائر منذ جانفي 1984 يعمل على تطبيق وتوحيد نظم التقاعد على جميع المتقاعدين والمتعلقة بتقدير الحقوق والاستفادة بالإضافة إلى توحيد النظام المالي. و أهم هذه القواعد هي:

- النسبة المئوية القصوى تمثل 80 % أي مدة 32 سنة من الأجر وذلك بنسبة 2.5 % في السنة، أما فيما يخص فئة المجاهدين والمشاركين في حرب التحرير بنسبة 3.5 % في السنة أي بنسبة 100%
- لحساب معاش التقاعد يتم الحساب بناء على 5 سنوات الأخيرة من العمل.
- النسبة القصوى للتقاعد المنقول هي نسبة 90 % من تقاعد معاش المتوفى.
- يتم مراجعة معاشات ومنح التقاعد سنويا خلال شهر مايو.
- لتأمين المتقاعدين عن المرض وعن الوفاة يتم خصم 2% من أجر التقاعد شهريا وهذا طبقا لقانون رقم 83/01 المؤرخ في 02 جويلية 1983.

- في حالة وجود عمل مأجور وعمل غير مأجور أو عمل خارج حدود الوطن يدخل معاش التقاعد في إطار عمل تنسيقي بين الصندوقين لتأمين المتقاعدين عن المرض وعن الوفاة يتم خصم 2% من أجر التقاعد شهريا وهذا طبقا لقانون رقم 83/01 المؤرخ في 02 جويلية 1983.
- يمكن التحصل على التقاعد ابتداء من سن 55سنة لحالات محددة ،حسب الشروط المعلن عنها في المادة 07 المعدلة من القانون 83/12 التي تتعلق بالعمال ذوو المناصب الخاصة التي تتعرض للمخاطر والضرر منها عمال أعماق المناجم وعمال المصالح النشطة في سلك الشرطة الوطنية .

(أنظر الملحق رقم01)

- **الضريبة عن المعاش(I.R.G):**

المعاشات التي تقل عن 20 000,00 دج شهريا تعفى من الضريبة كما تخفض الضريبة بنسب متفاوتة حسب قيمة كل معاش وهذا طبقا للتعليمة رقم 2010/11 من قانون المالية المؤرخ في 2010/08/26.

- **لجنة الطعون المسبقة الولائية Commission locale de recourse breakables :** هي لجنة تحكيم مستقلة وذات سيادة، تكون قراراتها ملزمة للطرفين فهي ترقي بحكم دورها وتشكيلها لأن تكون إجراء طعن أو مرحلة وسطية قبل كل تظلم أو ادعاء أمام اللجنة الوطنية أو الجهات القضائية.

إن مهمة اللجنة المحلية للطعن المسبق حسب المادتين 07/06 من القانون رقم 08/08 الصادر في 23 فيفري 2008 البث في الطعون المقدمة من طرف المؤمن عليهم اجتماعيا ضد القرارات الصادرة عن الوكالات المحلية. وعليه فإنها قابلة للتظلم ضد القرارات الصادرة عن اللجنة المحلية للطعن المسبق تخضع لشروط الآجال المحددة في المواد 13 و15 من نفس القانون والتي يبدأ سريانها من تاريخ التبليغ. يتم تعيين أعضاء اللجنة تطبيقا لأحكام المادة 02 من المرسوم التنفيذي رقم : 415/08 المؤرخ في ديسمبر سنة 2008 حيث الأعضاء كالتالي:

- عنوان ممثلي العمال الأجراء (عضو دائم وعضو إضافي)
- بعنوان ممثل الصندوق (عضو دائم وعضو إضافي)
- عنوان ممثلي أصحاب العمل (عضو دائم وعضو إضافي)
- بعنوان طبيب مقترح من طرف مدير الصحة والسكان.

1-3- التعريف بالوكالة المحلية للصندوق الوطني للتقاعد لولاية تيسمسيلت :

تم إنشاء مقر الوكالة سنة 1987 بحي عين البرج مؤقتا ليتم بناء مقر جديد بوسط المدينة بشارع العفري جمال مقابل حي 320 سكن تيسمسيلت ،كما عرف المقر توسع بداية من سنة 2012 حيث تم الانتهاء منها في 2017 . ويبلغ عدد عمال الوكالة 50عامل، كما يوجد ملحقات تابعة للوكالة ببعض بلديات الولاية وهي:

- الملحقة الأولى : متواجدة في منطقة برج بونعامة.
- الملحقة الثانية : متواجدة في منطقة ثنية الحد.

- الملحقة الثالثة : متواجدة في منطقة برج الأمير عبد القادر.
- الملحقة الرابعة : متواجدة في منطقة لرجام.

يشرف على هذه الملاحق موظفون يقومون باستقبال وتوجيه المؤمنين والمتقاعدين بصفة يومية وذلك من اجل تقريب الإدارة من المواطنين في بلديات سكناهم.

يتكون مقر الوكالة الولائية من طابق ارضي وطابقين علويين يحتويان على عدة مصالح

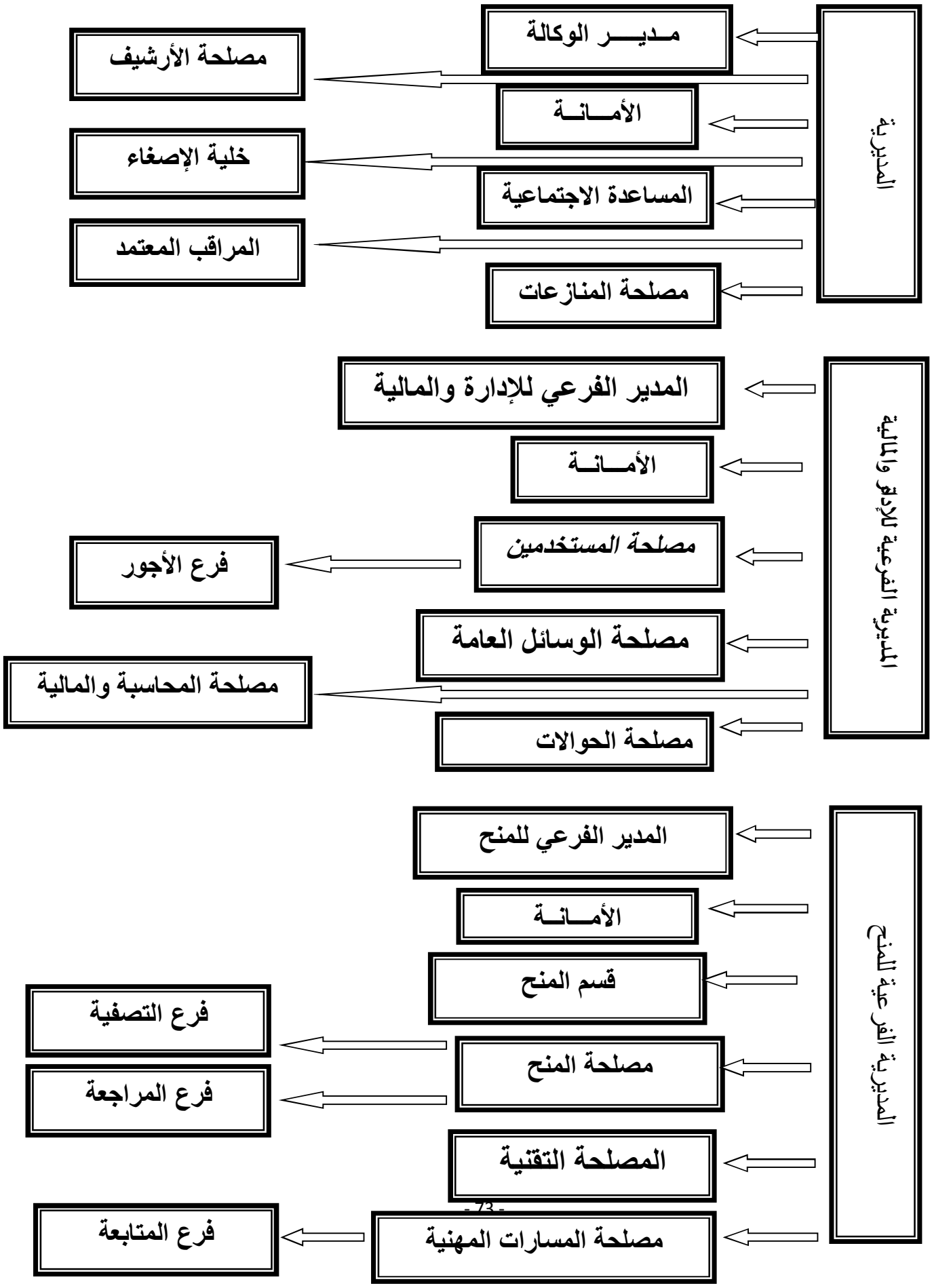
إذ يحتوي الطابق الأرضي على شباك موحد يتم من خلاله استقبال المؤمنين وتوجيهم وكذا الرد على جميع التساؤلات التي قد تشوب ملف التقاعد كما يحتوي أيضا على المصلحة التقنية التي تهتم هي الأخرى باستلام ملفات التقاعد وتتأكد من توافر جميع الشروط القانونية في ملف التقاعد لتقوم بتحويل الملف إلى مكتب المعالجة الالكترونية للمعطيات وهنا يتم تدوين جميع المعلومات الخاصة بالمتقاعد في التطبيقية STAR.

4-1- الهيكل التنظيمي للوكالة:

يتكون الهيكل التنظيمي للوكالة من المديرية ومديريتين فرعيتين هما: **المديرية الفرعية للإدارة والمالية والمديرية الفرعية للمنح** :

ويتحكم في هذا التقسيم عدد المتقاعدين في كل وكالة والملاحظ هو الدمج بين مديريتين فرعيتين في مديرية واحدة وهي الإدارة والمالية وسيتم فصلهما عن بعضهما ببلوغ عدد المتقاعدين في الوكالة أكثر من 20 ألف متقاعد ،كما يوجد في كل مديرية فرعية مصالح.

الهيكل التنظيمي للمؤسسة :



1-5- مهام صندوق التقاعد الوطني:

هو هيئة ذات طابع إداري تحت وصاية وزارة العمل، التشغيل والضمان الاجتماعي حيث يتولى هذا الصندوق المهام التالية:

- تسيير معاشات ومنح التقاعد ومنح ذوي الحقوق.
- ضمان عملية التحصيل والمراقبة وتحصيل الاشتراكات المخصصة لتمويل أداءات التقاعد.
- تطبيق الأحكام المتعلقة بالتقاعد والمنصوص عليها في الاتفاقيات في مجال الضمان الاجتماعي بين الجزائر وكل من تونس المغرب ليبيا بلجيكا وفرنسا.
- القيام بعملية إعلام المستفيدين والمستخدمين .

إضافة إلى مهام أخرى نذكر منها:

بالنسبة لخلية الإصغاء والاتصال الاجتماعي على مستوى كل وكالة، الهدف منها تحسين نوعية الأداء وتحسين العلاقة مع المواطن ورفع من ثقته في الإدارات العمومية.

مهامها تتمحور في:

- الاستقبال والإصغاء.
- التكفل بالشكاوي الشفهية والكتابية المطروحة من طرف المتقاعد
- إعلام المواطنين بحقوقهم وواجباتهم
- متابعة الإجراءات على مستوى وكالة الصندوق.

المساعدة في محل السكن:

هي عملية اجتماعية تتم شهريا لمساعدة المتقاعدين وذوي الحقوق في محلهم السكني ،تخص فئة المتقاعدين المعوقين والعجزة الذي يزيد سنهم فوق 70 سنة ،والساكنين في معزل وتتمثل المساعدة في:

- تقديم وسائل تقنية وسائل صحية مثل: كرسي متحرك.....الخ.
- بطاقة الشفاء. مساعدات طبية في محل السكن
- استخراج الوثائق الإدارية.

2-المركز الجهوي للأرشيف الصندوق الوطني للتقاعد :

نظرا للكم الهائل للأرشيف كان لزاما على الصندوق الوطني للتقاعد على إيجاد حل لمشكلة تخزين الوثائق وبعد التشاور مع الأرشيف الوطني تم الاتفاق على إنشاء مراكز جهوية لدفع أرشيف

العمر الثالث ومنه أنشأت ثلاثة مراكز الأول بغرب البلاد الموجود بعين تموشنت والذي يستقبل الدفعات من قبل 15 ولاية ، الثاني موجود بشرق البلاد بولاية أم البواقي والذي يستقبل بدوره الدفعات من 15 ولاية أيضا و الأخير موجود بجنوب البلاد بغرداية تحديدا والذي هو بدوره يستقبل الدفعات من 18 ولاية .

المركز الجهوي بعين تموشنت :

تم إطلاق المشروع سنة 2007 على إن يتم الانتهاء من الأشغال بعد 24 شهرا بقيمة إجمالية قدرت ب 74.512.294.03 دج ليتم افتتاحه سنة 2009 يقع بجانب مقر ولاية عين تموشنت وهو يستقبل الأرشيف من 15 ولاية من الغرب الجزائري وهي كالتالي :

عين الدفلى ،الشلف ،وهران ،مستغانم ،تيسمسيلت ،تيارت ،معسكر ،عين تموشنت ،سعيدة ،تلمسان، سيدي بلعباس ،غليزان ،البيض ،النعامة وأخيرا بشار.

مساحة تخزين الأرشيف تقدر ب 1561.92 م^2 ما يعادل تخزين مليون ملف وتتمثل مهمته الرئيسية في امتصاص الضغط على قاعات الأرشيف داخل الوكالات المحلية والأرشيف الوطني تطبق فيه كل معايير الأرشفة المتعامل بها تحت وصاية المديرية العامة للصندوق الوطني للتقاعد.

يعمل بالمركز 06 أرشيفيين متخصصين حاملين لشهادة ليسانس في الاختصاص ،مهندس في الإعلام الآلي و04 أعوان ترتيب ،عون استقبال وأعوان الأمن بالإضافة إلى رئيسة المركز.(**أنظر الملحق رقم 03)**

و بعد التقديم لمؤسسة الصندوق الوطني للتقاعد و مصلحة الأرشيف سوف تطرقنا إلى المعيار الذي سوف يتم معرفة تطبيقه من عدمه داخلها .

2- عرض تحليلي لمعيار إيزو 27002 لأمن المعلومات

نظرا لصعوبة الحصول على المعايير التي أغلبها يكون بمقابل مادي ونظرا لعدم تمكننا من العثور عليه في شبكة الإنترنيت وكذا عدم تمكننا من التوجه إلى المعهد الوطني للتقييس الكائن بالعاصمة للإستفسار والحصول على المعيار المطلوب فقد إعتمدنا على دراسة احمد طارش

وفيما يلي عرض تحليلي لمعيار ايزو 27002

حيث يتكون من 12 فصلا وتشمل على 40 معيار رئيسي و135 معيار فرعي كل معيار من معايير إيزو 27002 الرئيسية يتكون من 04 عناصر رئيسية وهي:

2. أهداف المعيار (داخل المؤسسة)

3. الضوابط التي تحقق أهداف المعيار.
4. توجيهات التطبيق (معلومات مفصلة تدعم تطبيق ضوابط)
5. معلومات أخرى (مثلا معلومات القانونية أو الإحالة إلى معايير أخرى ذات الصلة).[1]

الفصل الأول تقييم المخاطر ومعالجتها

جاء في هذا الفصل مقدمة عن تقييم المخاطر الامنية ،من حيث كيفية تقدير حجم المخاطر وتحديد أثرها.

هدفه:

تقييم المخاطر الأمنية بشكل دوري لمعالجة الثغرات في المتطلبات الامنية.

أهم ضوابطه:

1) تطبيق ضوابط لتقليص المخاطر
2) التوافق مع اللوائح والقوانين المحلية والدولية
3) ضوابط التشغيل

الفصل الثاني: السياسة الامنية

يتكون هذا الفصل من معيار رئيسي واحد هو" سياسة امن المعلومات"

هدفه:

توجيه إدارة المؤسسة ودعمها في طريقة تعاملها مع امن المعلومات والتوافق مع القوانين واللوائح ذات الصلة ينقسم هذا المعيار إلى قسمين رئيسين هما

- وثيقة عامة لسياسة أمن المعلومات.
- المراجعة لسياسة أمن المعلومات

الفصل الثالث: تنظيم أمن المعلومات

يتكون هذا الفصل من معياريين أساسين هما

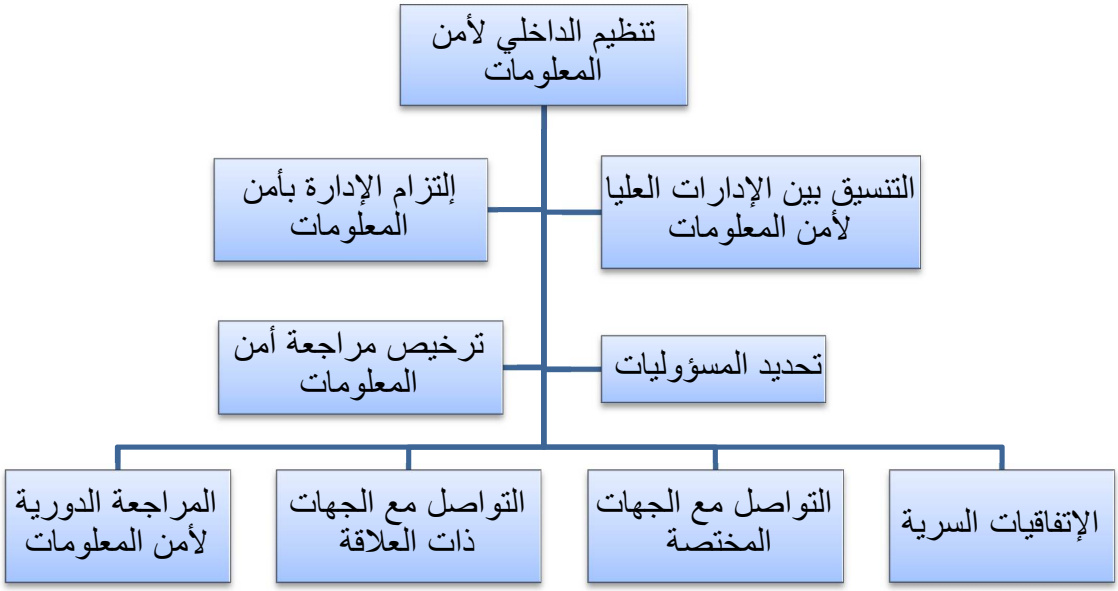
1) التنظيم الداخلي لأمن المعلومات : بدوره هذا المعيار يتكون من 08 معايير فرعية
2) الأطراف الخارجية :بدورة يتكون من 03 معايير فرعية

يهدف هذا الفصل إلى:

- الحفاظ على أمن المعلومات بالمنظمة وعلى مرافق معالجة المعلومات التي يمكن الوصول إليها أو تلك التي تعالج أو تدار من أطراف خارجية والتحكم

[1] الشريف أشرف عبد المحسن، ،المرجع السابق ،ص 94.

- السيطرة على دخول أطراف الخارجية وأخذ الاحتياطات الامنية اللازمة لإتاحة المعلومات ومرافقتها للأطراف الخارجية.[1]



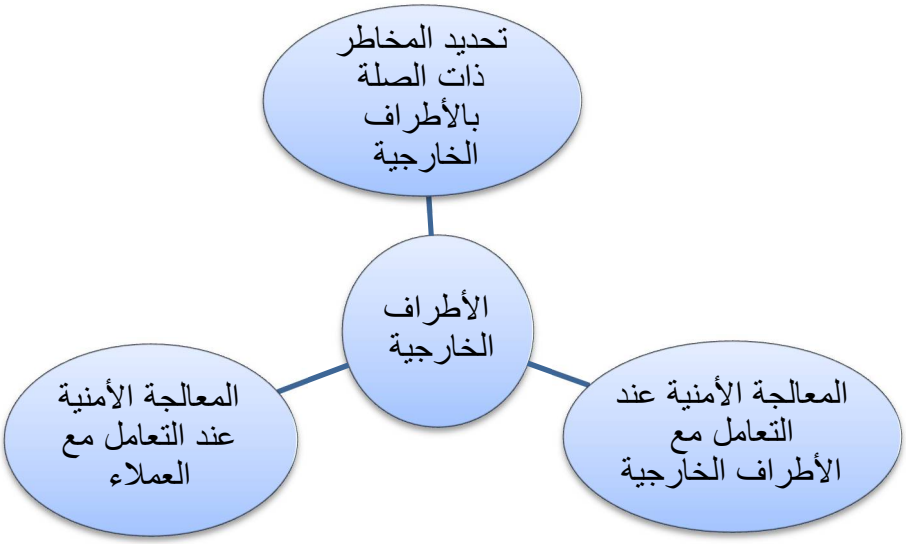
الشكل رقم 02 يمثل المعايير الفرعية لمعيار التنظيم الداخلي لأمن المعلومات

أهم توجهات التي خرج بها معيار تنظيم الداخلي لأمن المعلومات والتطبيق داخل المنظمة وتتمثل في النقاط التالي:

- توفير الموارد المادية والبشرية اللازمة لتحقيق أمن المعلومات
- تحديد المسؤوليات والمهام في جميع وحدات المنظمة
- تحديد الجهات المختصة ذات العلاقة بأمن المعلومات المؤسسة مثل وحدات الإطفاء والإسعاف
- فحص الأجهزة والبرمجيات للتأكد من أنها متوافقة تشغيليا مع مكونات النظم الأخرى
- وضع ضوابط لاستخدام الحاسبات المحمولة عند اتصالها بشبكة المؤسسة ،لعدم التسبب في إحداث ثغرات أمنية [2]

[1] عبادة أحمد العربي، المعايير الدولية لسياست أمن المعلومات دراسة تحليلة لمعايير المنظمة الدولية للتوحيد القياسي إيزو 27002 ومدى تطبيقها في الجامعات العربية ،مجلة مكتبة الملك فهد الوطنية، مج 19،ع 02 .أكتوبر 2013.ص 168.167

[2] عبادة أحمد العربي ،المرجع نفسة .ص 169.170

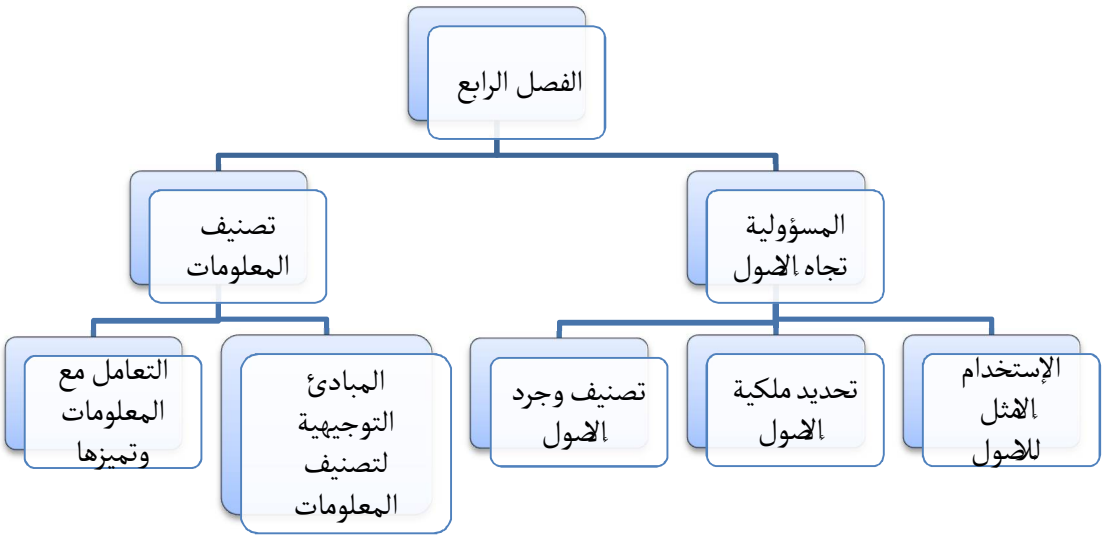


الشكل رقم 03 يمثل معايير الفرعية لمعيار الأطراف الخارجية

الفصل الرابع: إدارة الأصول

يتكون هذا الفصل من معيارين يشتملان على خمسة معايير فرعية، يحيث يهدف إلى:

تحقيق الحماية المناسبة لأصول المنظمة وتصنيفها من حيث القيمة والمتطلبات القانونية والحساسة شكل رقم (03)يوضح ذلك



الشكل رقم (04)معايير أساسية وفرعية للفصل الرابع لمعيار إيزو 27002 لأمن المعلومات

الفصل الخامس: أمن الموارد البشرية:

يهدف هذا الفصل إلى ضمان أن كل من الموظفين والمتعاقدين والأطراف الخارجية قد حددت مسؤولياتهم وأنهم مناسبون للأدوار المنوطة بهم ،و أنهم على علم بقضايا ومهددات أمن المعلومات

وتوفير قدر مناسب من الوعي والتدريب والتعليم في إجراءات الأمن، و في الاستخدام السليم لمرافق معالجة المعلومات لكافة العاملين .يتكون هذا الفصل من ثلاث معايير رئيسة كما في الشكل التالي [1]

الشكل رقم (05) يمثل المعايير الفرعية لمعيار امن الموارد البشرية

الفصل السادس :الأمن المادي والبيئي

يهدف هذا الفصل إلى وضع ضوابط لمنع الوصول المادي غير المرخص به وتفادي أية أضرار قد تحدث لمباني ومرافق المنظمة ويتكون من معيارين أساسيين هما بدورهما يشملان على 13.معيار فرعيا

[1] عبادة أحمد العربي، المرجع نفسه. ص 172

الشكل رقم (06) يوضح معايير الفرعية للأمن المادي والبيئي لمعيار إيزو 27002

الفصل السابع: إدارة العمليات /الاتصالات

يهدف هذا الفصل إلى وضع إجراءات تشغيلية لجميع مرافق تجهيز ومعالجة المعلومات ،ووضع ضوابط لرصد وتوثيق خدمات المعلومات المقدمة من منظمات خارجية والحماية من البرامج الخبيثة، بالإضافة إلى وضع سياسات تحظر استخدام البرامج الخبيثة والبرامج غير المصرح بها، و العمل على امتلاك نسخ احتياطا من المعلومات والبرامج ووضع ضوابط لحماية أمن الشبكة المعلومات بالمنظمة، ومعايير للتعامل مع وسائل الإعلام وكيفية وضع اتفاقيات لتبادل المعلومات والبرمجيات مع منظمات أخرى وحماية خدمات التجارية الإلكترونية، و توثيق أحداث أمن المعلومات. ويعتبر هذا الفصل من أكثر الفصول اشتمالا على المعايير الرئيسية والفرعية، حيث يتكون من عشرة معايير رئيسية هي:[1]

[1] عبادة أحمد العربي، المرجع نفسه. ص 176.175

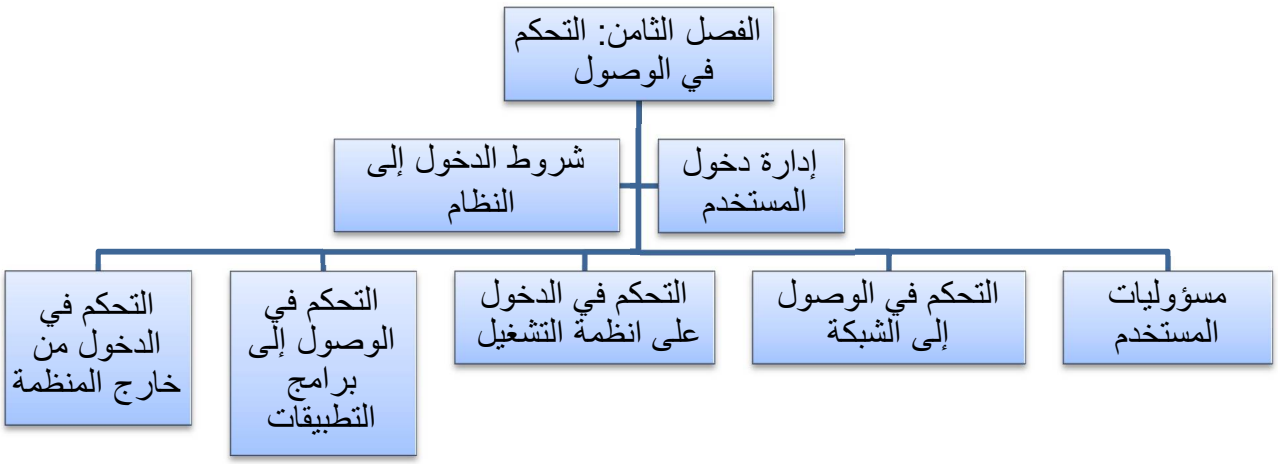
المعيار الرئيسي	المعايير الفرعية
الإجراءات التنفيذية	توثيق العمليات التشغيلية إدارة التغيير تحديد الصلاحيات الفصل بين مرافق التشغيل
إدارة تقديم الخدمات لأطراف خارجية	إيصال الخدمة مراقبة ومراجعة خدمات الطرف الثالث إدارة التغييرات في خدمات الطرف الثالث
تخطيط وإعداء الأنظمة	إدارة بناء القدرات نظام القبول
الحماية من البرامج الخبيثة	ضبط البرامج الخبيثة ضبط مكونات البرامج
النسخ الاحتياط	النسخ الاحتياط للمعلومات
إدارة تأمين الشبكات	الضوابط الأمنية للشبكات تأمين خدمات الشبكات
التعامل مع وسائط التخزين	إدارة وسائط التخرين القابلة للإزالة إجراءات التعامل مع المعلومات التخلص من وسائط التخزين حماية وثائق المنظمة
تبادل المعلومات	سياسات وإجراءات تبادل المعلومات اتفاقات التبادل الوسائط المادية في حالة النقل المراسلة الإلكترونية أنظمة المعلومات التجارية
خدمات التجارة الإلكترونية	التجارة الإلكترونية التحويلات المباشرة المعلومات المتاحة للجمهور

المراقبة والتوثيق	مراجعة التسجيلات مراقبة استخدام الأنظمة حماية سجل المعلومات سجلات المديرين والمشغلين تدوين الاخطاء مزامنة الوقت

جدول رقم (02) يمثل معايير الفرعية لمعيار إدارة العمليات / الاتصالات

الفصل الثامن: التحكم في الوصول

يهدف هذا الفصل إلى وضع سياسات لضبط الوصول إلى المعلومات ومرافقها وضمان وصول الأفراد المصرح لهم فقط وإتباع إجراءات رسمية لتسجيل المستخدمين ولإلغاء التسجيل وإتباع طرق آمنة لإختبار واستخدام كلمات المرور والحفاظ على أفراد تم اختبارهم وفقا لطبيعة وظائفهم ،يتكون هذا الفصل من 07 معايير فرعية وتتمثل فيما يلي:



الشكل رقم (07) المعايير الفرعية لمعيار التحكم في الوصول

1. شروط الدخول إلى النظام

- يهدف هنا المعيار إلى وضع سياسة لضبط الوصول وإلى المعلومات تتوافق مع السياسات الأمنية للنظام وأن توثق هذه السياسات وتراجع وتقيم باستمرار، وورد ت تحت مجموعة من توجيهات التطبيق أهمها -:
- وضع سياسة للتحكم في الوصول تلبي الاحتياجات الأمنية للمنظمة
- وضع قواعد للدخول مبنية عل مبدأ(كل شيء ممنوع ما لم يسمح ب صراحة.)
- إن قواعد التحكم في الوصول ينبغي أن تدعم بواسطة إجراءات رسمية ومسؤوليات محدد ة وواضحة[1].

2. إد ارة دخول المستخدم

يهدف هنا المعيار إلى ضمان وصول المستخدم المصرح له إلى نظام المعلومات، ووضع إجراء ات رسمية لضبط عملية الحصول عل حقوق الوصول إلى نظم المعلومات والخدمات.
ويتكون هنا المعيار من أربعة معايير:

- تسجيل المستخدم
- إدارة امتيازات المستخدم
- إدارة كلمة المرور.
- مراجعة وصول المستخدم للنظام.

3) مسؤوليات المستخدم :

يهدف هنا المعيار إلى التأكيد عل التزام المستخدمين بالحفاظ على سرية كلمات المرور وتأمين الأجهزة الرسمية والشخصية ضد الاستخدام غير المرخص في فترة عدم الاستخدام: يندرج تحته ثلاث معايير فرعية وتتمثل في

1) استخدام كلمة السر
2) تامين الأجهزة في غياب المستخدمين
3) خلو سطح المكتب والشاشة

4) التحكم في الوصول إلى الشبكة:

يهدف هنا المعيار إلى من الوصول غير المصرح لخدمات الشبكة وتطبيق طرق مناسبة لتوثيق المستخدمين والأجهزة ووضع ضوابط تحكم وصول المستخدمين لخدمات المعلومات.

[1] عبادة احمد العربي، المرجع نفسه. ص 181.182.

5) التحكم في الوصول إلى نظم التشغيل

يهدف هنا المعيار إلى من الوصول غير المصرح به إلى نظم التشغيل واستخدام أقصى درجات الأمن لقصر الوصول إلى نظم التشغيل على المستخدمين المصرح لهم، وتوثيق وتسجي المستخدمين ومحاولات الدخول الناجحة والفاشلة وصلاحيات النظام.

و يتكون هذا المعيار من ست معايير فرعية وهي

- الدخول الآمن للمستخدمين
- تعريف المستخدمين
- إ دارة كلمة المرور.
- انتهاء زمن جلسة العمل.
- استخدام الأدوات المساعدة[1].
- تحديد زمن الاتصال.

6) التحكم في الوصول إلى برامج والتطبيقات:

يهدف هذا المعيار إلى منع المستخدمين غير المصرح لهم من الوصول إلى المعلومات الي تحملها تطبيقات النظام ووضع سياسة للتحكم وتحديد الأشخاص المخول لهم للوصول إلى هذه البرامج.

ويتكون هنا المعيار من معيارين فقط هما:

- تقييد الوصول إلى التطبيقات.
- عزل الأنظمة الحساسة.

7) التحكم في دخول الحاسبات المتنقلة:

يهدف هذا المعيار إلى أخذ كل التدابير الأمنية عند استخدام الحاسبات المتنقلة ووضع وتطبيق إجراء ات وخطط تشغيل عند السماح بالدخول لأنظمة المعلومات عن بعد. ويتكون هنا المعيار من معيارين فرعين هما:

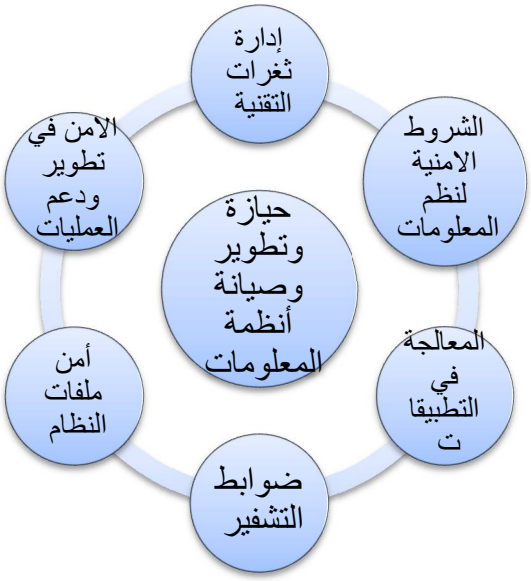
- العمل والاتصال عن بعد.
- مراقبة العمل عن بعد

الفصل التاسع : حيازة وتطوير وصيانة انظمة المعلومات

يهدف هذا الفصل إلى اعتبار أمن نظام المعلومات جزء ا مهما من نظم المعلومات، ومنع الأخطاء والخسائر وإساءة استخدام المعلومات وحماية سرية وصحة المعلومات من خلال برامج التشفير، ضمان أمن ملفات النظام والحد من وجود ثغرات أمنية ومراقبة نقاط الضعف التقني. ويشمل هنا الفصل ستة معايير رئيسية هي :[2]

[1] عبادة احمد العربي، المرجع نفسه. ص 183.184.

[2] عبادة احمد العربي، المرجع نفسه. ص 185.186.

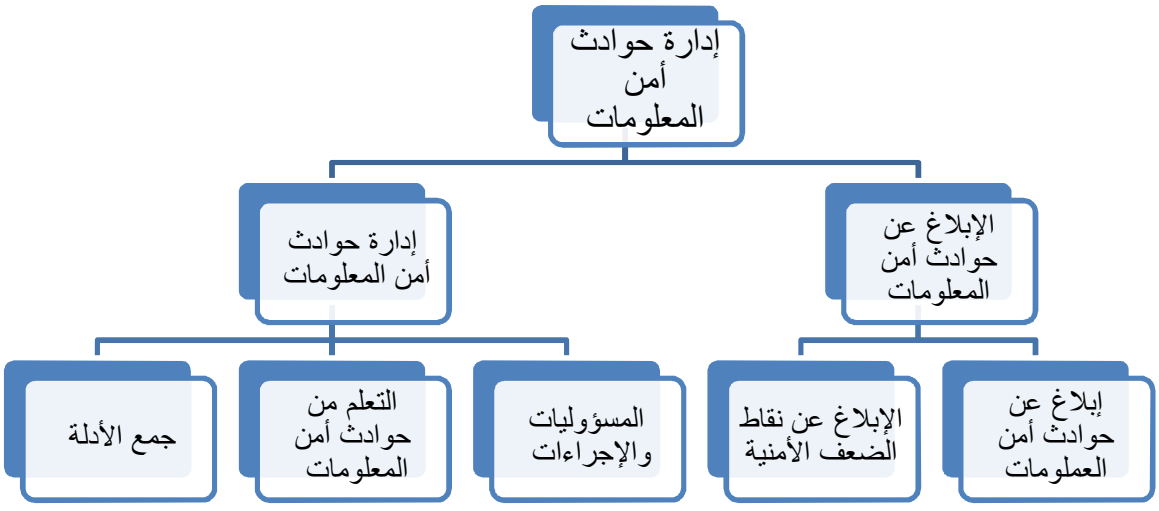


الشكل رقم (08) يمثل المعايير الفرعية لمعيار حيازة وتطوير وصيانة أنظمة المعلومات

الفصل العاشر: إدارة حوادث أمن المعلومات

يهدف هذا الفصل إلى التأكيد عل أمن المعلومات، والتبليغ عن مواطن الضعف في أنظمة المعلومات والتعامل معها، ومراجعتها في أقرب وقت ممكن وتحديد الإجراءات والمسؤوليات والإدارات المنوط بها التعامل مع حوادث أمن المعلومات، والإفادة من المعلومات المكتسبة من حوادث أمن المعلومات في المستقبل ،والتأكيد على تدخل الجهات الأمنية المنوط بها التحقيق في الوقت المناسب قبل الطمس المتعمد للحقائق .

ويتكون هنا الفصل من معيارين رئيسية ويوجد خمس معايير فرعية تحت هذين المعيارين وهي تتمثل في الشكل الموضح أسفل

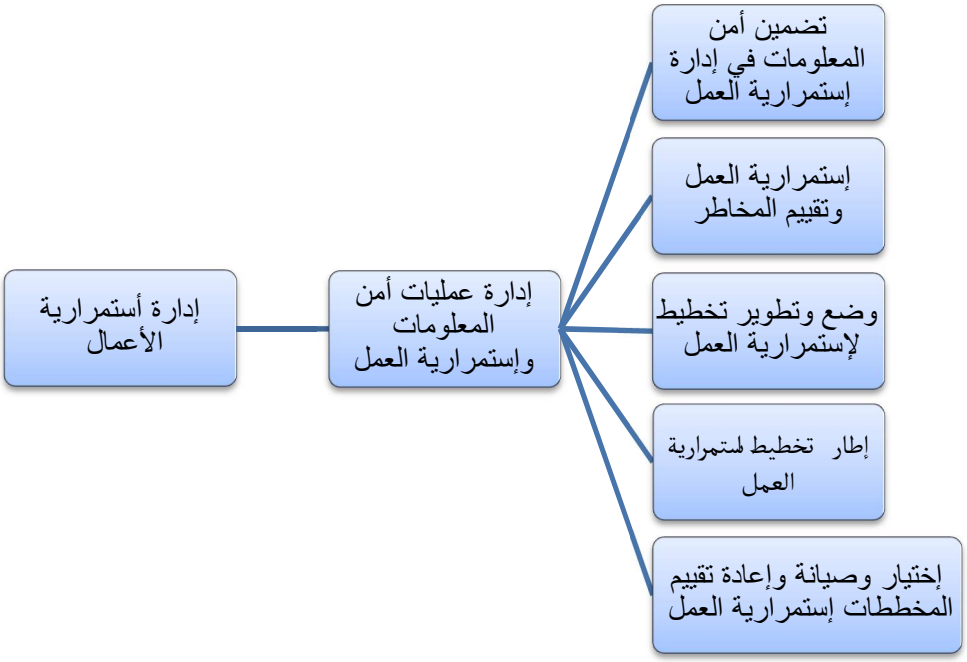


الشكل رقم (09) يمثل المعايير الرئيسية والفرعية لمعيار إدارة حوادث أمن المعلومات

الفصل الحادي عشر :إدارة استمرارية الاعمال

يهدف هنا الفصل إلى الحد من كل الأنشطة الي تحاول إعاقة سير العمل في المنظمة والعمل على حماية نظم المعلومات من لأعطال الرئيسية أو الكوارث وضمان إعادة تشغيل النظام في الوقت المناسب.

يتكون هنا الفصل من معيار واحد رئيسي ويندرج تحته خمسة معايير فرعية موضحة في الشكل التالي:[1]



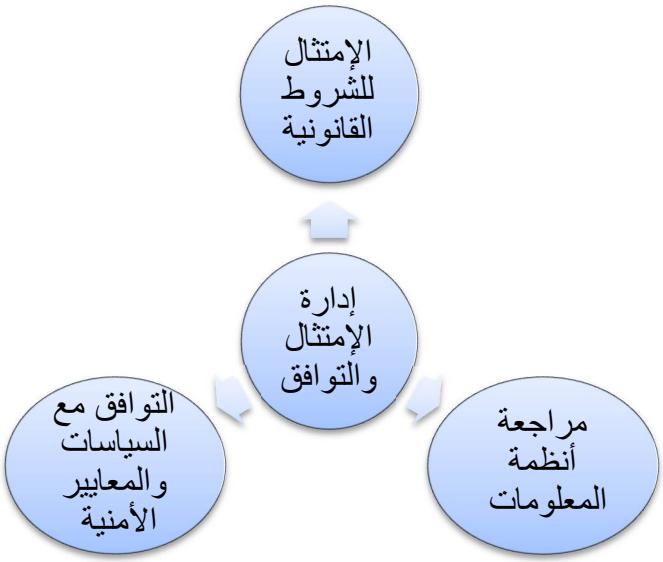
الشكل رقم (10) يمثل معايير الفرعية لمعيار إدارة عمليات أمن المعلومات واستمرارية العمل

الفصل الثاني عشر: إدارة الامتثال والتوافق

يهدف هذا الفصل إلى تجنب اختراق للقوانين والأنظمة والالتزامات التعاقدية، وتحديد وتوثيق هذه القوانين والأنظمة وتحديثها كلما لزم الأمر ومنع إساءة استخدام المعلومات ومرافقها وحماية خصوصية البيانات والمعلومات الشخصية ويتكون هنا الفصل من ثلاثة معايير رئيسية وهي [2]

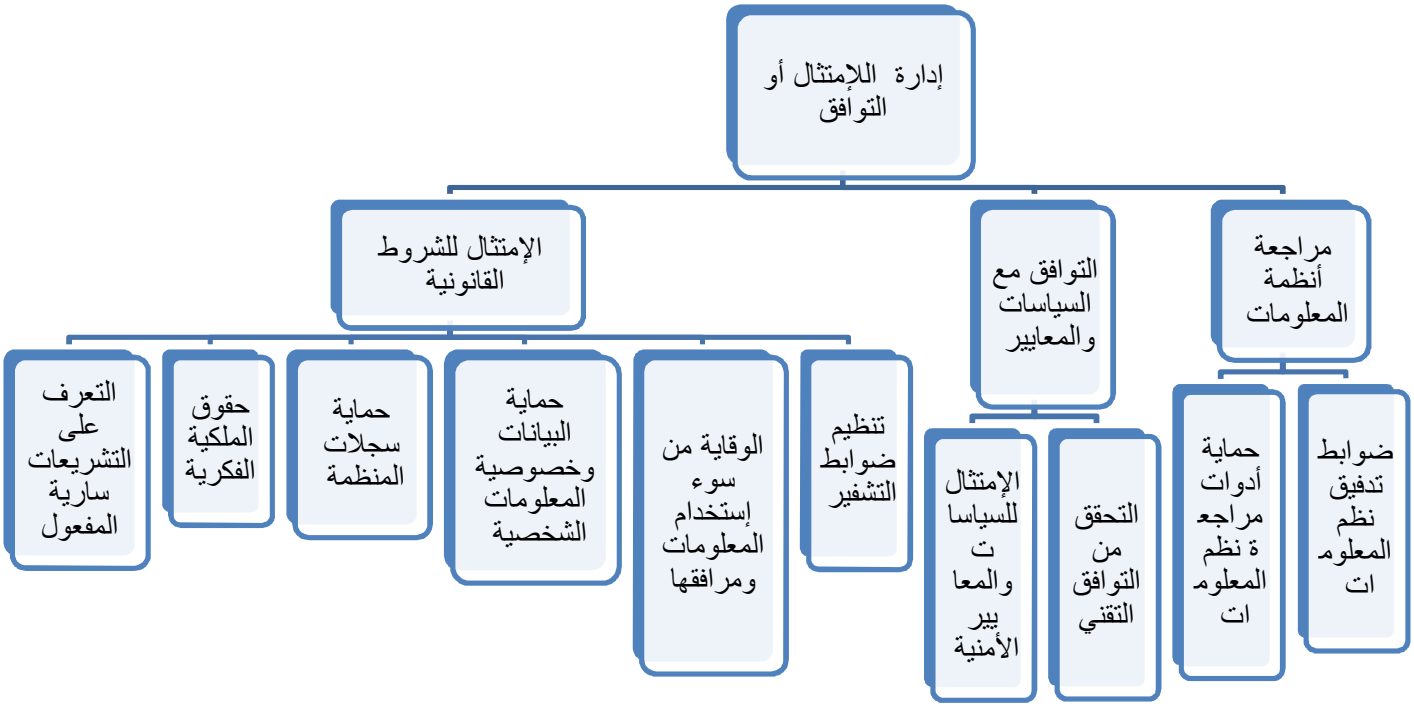
[1] عبادة أحمد العربي. المرجع نفسه. ص 187.188.

[2] عبادة احمد العربي. المرجع نفسه. ص



شكل رقم 11 يمثل معايير الرئيسية لمعيار إدارة الامتثال والتوافق

كما يندرج تحت هذه المعايير الرئيسية الثلاث عشرة معايير فرعية يمكن توضيحها في الشكل التالية



الشكل رقم (12) يمثل المعايير الفرعية لفصل إدارة الامتثال أو التوافق

بعد هذا العرض ننتقل إلى تحليل المقابلة وفقا لمحاور الدراسة و مقارنة المعطيات بمعيار إيزو 27002 لأمن المعلومات وفقا لمحاور المعتمدة في المقابلة

3- الإمكانيات المادية والكفاءات البشرية المتوفرة في مصلحة الارشيف صندوق الوطني للتقاعد لتحقيق أمن معلوماتها :

3-1- الميزانية:

3-1-1- مصادر تمويل المؤسسة:

يعود مصدر تمويل المؤسسة إلى الوزارة الوصية على ذلك المتمثلة في وزارة العمل والتشغيل والضمان الاجتماعي بحيث تتكفل هذه الأخيرة بكل الموارد المالية للمؤسسة ولا توجد أي جهة أخرى يمكن أن تقوم بتمويلها ماليا لأن مركز الوطني للتقاعد تابع لهذه الوزارة. وعلى هذا فإنها المسؤولة عنها في كل ما يخص الميزانية التي تحتاجها المؤسسة لتسيير أعمالها وإتمام وظائفها اليومية وبهذا فيمكن القول بأن وزارة العمل والتشغيل والضمان الاجتماعي هي الممول الوحيد لمؤسسة الصندوق الوطني للتقاعد. بحيث يتم تقديم هذه الميزانية عن طريق تمويل مركزي وذلك بعد دراسة احتياجات كل وكالة وتنقسم إلى قسمين ميزانية التسيير وميزانية التجهيز.

3-1-2- تخصيص حصة ثابتة من الميزانية بأمن المعلومات داخل مركز الوطني للتقاعد

فقد كانت إجابة المسؤول حول هذا الامر بأنه لا يتم تخصيص ميزانية خاصة بأمن المعلومات في المركز بحيث يتم تخصيص مبلغ معين من الميزانية العامة للمركز في حال ما إذا تطلب الامر لذلك مثلا شراء برامج الحماية أو ضرورة الحصول على بعض الاجهزة التي من شانها أن تساهم في تحقيق الامن داخل المؤسسة. بالرغم من عدم تخصيص ميزانية خاصة بأمن المعلومات داخل المؤسسة إلا أنه إذا تطلب الامر لذلك فإن المبلغ المخصص من الميزانية غالبا ما يفي بالغرض وهذا ما يبعث راحة وطمأنينة حول موضوع امن المعلومات داخل المؤسسة .

3-1- الموارد البشرية:

3-1-1- المؤهلات البشرية ومدى كافيتها في لتحقيق الأمن داخل المؤسسة الصندوق الوطني للتقاعد:

الموظفين	المؤهلات العلمية	العدد	طبيعة التوظيف
مسير المؤسسة	**ليسانس**	**01**	**تعيين مركزي**
إطارات مؤسسة	مستوى جامعي	19	التدرج في المناصب
الأرشيفي	ليسانس علم المكتبات والعلوم الوثائقية	01	على أساس الشهادة
أعوان المكاتب	ليسانس سنة 03 ثانوي	20	على أساس الشهادة المقابلة

	متوسط ابتدائي بدون مؤهل		الانتقاء
أعوان الأمن	الرابعة متوسط+ ديبلوم عون أمن ووقاية	06	على اساس الشهادة والانتقاء
عون النظافة	بدون مستوى	02	انتقاء
عدد الإجمالي		49	

جدول رقم 03 يمثل المؤهلات البشرية في مؤسسة الصندوق الوطني للتقاعد

3-2-2- الموظفين ومؤهلاتهم ومدى كفايته داخل مصلحة الارشيف المركز الوطني للتقاعد:

الموظفين	عددهم	مؤهلاتهم
الأرشيفي	01	ليسانس علم المكتبات والعلوم الوثائقية
عون مساعد الأرشيفي	01	سنة 03 ثانوي+ تكوين مهني في الأرشيف
أعوان مكتب التسيير الإكتروني	02	سنة 03 ثانوي

جدول رقم 04 يمثل المؤهلات البشرية في مصلحة الأرشيف

حسب الجدولين المبينن اعلاه يتضح لنا أنه فيما يخص المؤهلات البشرية للموظفين ككل فإن المؤهلات البشرية في الجدول رقم 3 0 غير كافية وذلك راجع إلى مستويات ومؤهلات العلمية التي يمتلكها الموظفون تعتبر غير كافية لتحقيق الامن اللازم بالإضافة إلى عدم الإحساس بالمسؤولية وقلة الوعي بأهمية المعلومات داخل المؤسسة وللدور الذي تلعبه في تحقيق الريادة والمستوى المطلوب من العمل بالإضافة إلى سمعة الجيدة التي تتحصل عليها المؤسسة في حال ما تحقق الامن داخلها .و عليه فإن مؤشر التوظيف لأفصل الخامس لمعيار إيزو 27002 من المعيار الرئيسي خاص بإجراءات سابقة للتوظيف غير محقق في مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد أما فيما يخص المؤهلات البشرية وعدد الموظفين الخاصة بمصلحة الأرشيف فيبين الجدول رقم 04 فإن عدد الموظفين غير كافي وذلك تطابقا مع ضغط العمل الذي يقوم به العمال داخل المؤسسة لأنها من بين المؤسسات التي تنشط يوميا ،بالتالي فإن العمل في تزايد كل يوم وخصوصا على مستوى مصلحة التسيير الإلكتروني التي تحتاج إلى أكثر من 3 موظفين على الاقل ،كما يعمل على مستوى مصلحة الأرشيف و مكتب التسيير الإلكتروني و قاعة الأرشيف 04 موظفين من أساس 49 موظف فهو غير كافي و هذا النقص في عدد الموظفين يرجع إلى قلة وانعدام التوظيف على مستوى المؤسسة لعدم تقديم طلب بزيادة عدد الموظفين من طرف مدير المؤسسة و كنتيجة حتمية لهذا الامر هي تراكم العمل عليهم خصوصا في مرحلة التي كان الموظفون يقومون بعملية الرقمنة للرصيد الوثائقي فهذا يستدعي إلى ضرورة زيادة عدد الموظفين للتخفيف من الضغوطات التي تتراكم على الموظفين وكما جاء في الفصل

الثالث خاص بتنظيم أمن المعلومات من معيار إيزو 27002 الخاص بأمن المعلومات الذي أدى إلى توفير الموارد البشرية اللازمة لتحقيق أمن المعلومات وعليه فهذا البند غير محقق داخل مصلحة الأرشيف بالمؤسسة.

غير أن مؤهلاتهم كافية لتحقيق الأمن المعلوماتي داخل مصلحة الأرشيف وذلك راجع إلى كون أن شهادتهم العليمة تتطابق مع وظائفهم المنسوبة إليهم داخل المؤسسة .

3-2-3- مستوى التكوين الذي يتحصل عليه الموظف في مركز الصندوق الوطني للتقاعد:

هو مستوى متوسط وذلك راجع إلى تلقي الموظف تكوين عن طريق تقديم و تبادل الخبرات بين الموظفين و تكوين في بعض الأحيان يكون بجلب أخصائيين و هذا ما تم بالفعل في الوقت الذي تحصل فيه المركز على الماسحات الضوئية فقد تلقى الارشيفي تكوين حول كيفية استعمالها والعمل بها من أجل القيام بعملية رقمنه الرصيد الوثائقي بالإضافة إلى انه يكون تكوين ،حسب ما هو مطلوب من التكوين حسب الصلاحيات الممنوحة له بالإضافة إلى الامور التي تكون جديدة على المؤسسة بمعنى في حال ما كان الموظف لا يعرف كيفية التعامل مع الماسحات الضوئية فإنه يتحصل على تكوين فيما يخص هذا المجال فقط كما إذن فإن مؤشر الخاص بتحديد المسؤوليات من المعيار الرئيسي المتمثل في الإجراءات التنفيذية للفصل السابع من معيار إيزو 27002 محقق جزئيا في مصلحة الأرشيف للمركز الوطني للتقاعد.

من هاتين النقطتين و بالإعتماد على معيار إيزو الذي يدعو إلى ضرورة التكوين وهذا ما أكدته دراسة أحمد بن علي عبد الله طارش و التي أفادت أن غياب التكوين والتدريب للعمال على احدث التقنيات يأثر في مستوى تحقيق أمن المعلومات

3-2-4- امتلاك الموظفين تقنيات التعامل مع الأجهزة الإلكترونية الحديثة المعتمدة داخل مصلحة الأرشيف بالمؤسسة:

كانت الإجابة حول هذا التساؤل بأن الموظفين يمتلكون تقنيات التعامل مع الاجهزة الإلكترونية ويتجسد ذلك من خلال تعاملهم اليومي مع الأجهزة الإلكترونية المتوفرة داخلها بالإضافة إلى مواكبتهم للتطورات التكنولوجية الحاصلة في مجال الأجهزة الإلكترونية،وذلك كون ان المجتمع أصبح معلوماتي ولابد من معرفة كيفية التعامل معها .بالإضافة إلى إتقانهم العمليات الحاسوبية لا سيما كيفية التعامل مع التطبيقات والبرامج الخاصة بالوكالة وهذا ما يتوافق ما مؤشر الفرعي للفصل الرابع من معيار إيزو 27002 الخاص بأمن المعلومات الذي يدعو إلى الاستخدام الأمثل للأصول في المعيار الرئيسي المسؤولية إتجاه الأصول

صورة رقم 01 تبين التعامل مع الأجهزة الإلكترونية داخل مصلحة الأرشيف

3-2-5- دورات تكوينية للموظفين في مجال التقنيات الحديثة المستعملة في أمن المعلومات

أشار المسؤول حول هذه النقطة بأنه لا يوجد دورات تكوينية خارج المؤسسة وهي في رأيه غير ضرورية سبب يعود إلى التركيز على إتباع كل القوانين و التعليمات خاصة بمركز التقاعد و كذا قيام كل الموظف بما يوكل إلية من مهام و هذا ما يضمن توفير و تحقيق الأمن المعلوماتي للمؤسسة . وهذا ما يتنافى مع ما هو موجود في معيار إيزو 27002 للفصل الخامس المتمثل في أمن الموارد البشرية في المعيار الرئيسي الثاني المتعلق بإجراءات أثناء أداء الوظيفة الذي يستدعي وجود التدريب والتكوين على أمن المعلومات وعليه فهو غير محقق في مصلحة الأرشيف.

3-2-6- مدى امتلاك الموظفين وعي بأهمية أمن المعلومات :

فقد تضمنت الإجابة علية بأنه هناك نوعين من الموظفين على مستوى المؤسسة فهناك من يمتلكون الوعي الكافي بأهمية المعلومات و يتجسد من خلال حس المسؤولية و وعي في حين هناك من لا يمتلكون وعي كافي بأمن المعلومات ويتجسد ذلك من خلال سوء استخدام لكلمات السر الخاصة بالأجهزة الآلية بالإضافة إلى عدم معرفتهم كيفية تحديث البيانات إلكترونيا فإن كل هذه الامور تجعل المعلومات في عرضة دائما إلى خطر الوصول غير مصرح للأشخاص وذلك لعدم امتلاك الموظف لوعي بضرورة أهمية أمن المعلومات وإلزامية الحفاظ عليها فهذا يؤدي إلى عدم مصداقية المعلومات وتشكك في صحتها دائما داخل المؤسسة، كما ان عنصر الوعي يمثل أحد اهداف الفصل الخامس معيار إيزو 27002 الخاص بأمن الموارد البشرية هو توفير القدر المناسب من الوعي للموظفين والأطراف الخارجية والمتعاقدين وذلك بتلقي تدريب حول اهمية امن المعلومات داخل المنظمة والتحديثات التي تدخل على السياسة الأمنية وعليه فإن مؤشر الخاص بالوعي الموظفين غير محقق داخل مؤسسة الصندوق الوطني للتقاعد

و هذا أيضا من بين أهم نتائج دراسة بغداد محمد التي وضحت ان العنصر البشري أحد أهم الموارد وفي نفس الوقت تعتبر اول مهدد وخطر على امن المعلومات

3-2- **الإمكانيات المادية**

3-3-1- موقع مركز الحاسبات والتصميم الهندسي في البناية ومدى مناسبته للحفاظ على أمن المعلومات:

صورة رقم 02 تمثل مركز الحاسبات في مؤسسة الصندوق الوطني للتقاعد

جاءت إجابة المسؤول حول هذه النقطة بأن موقع الحاسبات و التصميم الهندسي مناسب داخل البناية و ذلك كون تصميمها يوافق معايير البناء الضرورية التي تسمح بتوفير الأمن للمعلومات إضافة إلى وجود كل الوسائل اللازمة لتأمينها و لهذا يمكن القول انه هناك حماية" للحاسبات "لأنها بمثابة النواة الأساسية للمعلومات الإلكترونية التي تم رقمنتها ،وهذا ما يتوافق مع معيار إيزو 27002 للمعيار الرئيسي الاول المتمثل في تأمين المناطق للفصل السادس الخاص بأمن المادي والبيئي في المؤشر الأول منه المتمثل في أمن محيط الخارجي الذي دعى إلى ضرورة تأمين المحيط الداخلي للمؤسسة .

3-3-2- وسائل الراحة التي تتوفر عليها مصلحة الأرشيف بمركز الصندوق الوطني للتقاعد:

أفادة الإجابة المقدمة بوجود وتوفر كل وسائل الراحة (إنارة، تهوية، تدفئة)سواء الطبيعية ام الاصطناعية داخل المؤسسة عامة و مصلحة الأرشيف خاصة و ذلك لضمان سيرورة العمل بأحسن حالاته فمثلا الإنارة فإن المصلحة تحتوي على نوافذ ذات حجم كبير يمكن أن يدخل من خلالها ضوء الشمس بصورة و فيما يخص الإنارة الاصطناعية فهي تتوفر على اضواء لا تضر بعين الموظف في حال استعمالها خاصة في فصل الشتاء يكون ضوء الشمس يكون قليل و بالإضافة إلى وجود الرفوف المتحركة التي تتطلب العمل بالإنارة الإصطناعية، ونفس الأمر يتكرر مع وسائل الراحة الاخرى من تدفئة وتهوية التي تتوفر في كل قاعة ، وكل هذه الامور تجعل من عمل الموظفين بشكل سهل وتوفر لهم الراحة التامة خلال تأدية اعمالهم اليومية داخل مصلحة الأرشيف وبهذا يكون مستوى العمل عالي وبكفاءة وعلى اكمل وجه. وهذا ما يزيد من نسبة تحقيق أمن المعلومات بها ،و ن توفير هذه الوسائل تساعد على العمل في محيط آمن، بالإضافة إلى أن الفصل السادس من معيار إيزو 27002 في مؤشر

الخاص بتثبيت المعدات وحمايتها يدعو إلى ضرورة وجود مثل هذه الوسائل وتأمينها وعليه فإن هذا المؤشر محقق في مصلحة الأرشيف لمركز الصندوق الوطني للتقاعد

3-3-3- التجهيزات والاثاث المتواجد داخل مصلحة الأرشيف ومدى كفايتها في تحقيق الأمن المعلوماتي في مؤسسة الصندوق الوطني للتقاعد:

	التجهيزات	عددها	كافي	غير كافي
الأثاث	الكراسي	08	√	
	الخزانات	04	√	
	مكاتب الموظفين	06	√	
التجهيزات	الحاسبات الإلكترونية	04	√	
	مخزنات الطاقة	04	√	
	الماسحات الضوئية	03	√	
	الطابعات	01	√	×
	آلات النسخ	00	×	×
	الكاشفات البيولوجية	00	×	×
	كاميرات المراقبة	02	√	
	وسائط الإلكترونية	02	√	
	أجهزة إنذار الحرائق	07	√	
تجهيزات إضافية	مطافئ الحرائق اليدوية	04	√	

جدول 05 رقم يبين التجهيزات و الاثاث المتواجدة في مصلحة الأرشيف

حسب الجدول الموضح أعلاه يتضح بأن كل من التجهيزات والأثاث ضرورية داخل مصلحة الأرشيف لأي مؤسسة ولهذا فإن وجود معظم والأثاث كافية داخل مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد مثل كراسي وخزائن و مكاتب و توفرها بأعداد كافية للموظفين العاملين بمصلحة الارشيف و مكتب التسيير الإلكتروني و قاعة الأرشيف حيث ان الأثاث المتواجد يفوق عدد الموظفين المتواجدين و يجعل عملهم بأريحية عند تنقل من مصلحة إلى أخرى

أما فيما يخص التجهيزات نجد ان كل من الحاسبات الإلكترونية وماسحات الضوئية ....إلى غير ذلك من التجهيزات غير انه هنالك نقص في بعض التجهيزات الاخرى من بينها نذكر الطابعات التي تتوفر واحدة فقط وفيما يخص آلات النسخ والكاشفات الإلكترونية فهي منعدمة داخلها ،عموما يمكن القول بأن المصلحة تحتوي على كل التجهيزات الضرورية للعمل وبإعداد لا بأس بها ة تكفي للعمل بها

من طرف الموظفين ولكن لا يمكن غض النظر على النواقص من التجهيزات والعمل على توفيرها في أقرب وقت ممكن من أجل تسهيل العمل ورفع الكفاءة.

3-3-4- الرصيد الوثائقي داخل مصلحة الأرشيف ومدى تأمينه :

لا يمكن الحديث عن أمر أمن المعلومات بدون الحديث عن الرصيد الوثائقي وكيفية تكوين و طريقة ترتيبه داخل مصلحة الارشيف ،إذ كان لابد من التطرق لهذه النقطة من أجل معرفة كيفية توفير الحماية على مستواها.

حيث أفادنا المسؤول بما يلي ان الرصيد الوثائقي يتكون طبيعيا الرصيد الوثائقي من خلال عملية الدفع من مختلف المصالح للمؤسسة (مصلحة المنح، مصلحة المالية، مصلحة الحوالات ...) حيث تكون عملية الدفع بعد انقضاء مدة من الزمن على الوثائق لدى المصالح (و قد حدد مدة انتهاءها غاليا ب خمس سنوات) على الوثائق لدى المصالح ليأتي دورها وتسليمها إلى الأرشيف لتأخذ مكانا داخل قاعة الأرشيف ،ليتم الرجوع إليها نادرا وقت الحاجة .التي تقتضي تحويل الملفات والوثائق من المصالح المنتجة إلى مصلحة الأرشيف للحفاظ على هذه الوثائق وحمايتها ويتم تحويل الوثائق بحسب جدول زمني موضوع من طرف مديرية المسارات المهنية والأرشيف بالمديرية العامة ماعدا ملفات المتقاعدين والتي يتم تحويلها مباشرة إلى مصلحة الأرشيف نظرا لكمها الهائل الذي يتعذر حفظها في المصلحة و التي أنها تعتبر أرشيف العمر الأول .كما تتم عملية الدفع بالطريقة التالية: بعد تطبيق الجدول الزمني يتم الدفع عن طريق جدول دفع الأرشيف ويستخرج جدول الدفع عن طريق التطبيقية المستعملة لهذا الغرض تسمى (WIN POSيسهل هذا البرنامج عملية استخراج جدول الدفع وربح الوقت

تأمين الرصيد الوثائقي . فيكون وفق ما يلي :

3-3-5- إجراءات الوقائية لحماية الوثائق الأرشيفية من الأخطار داخل المؤسسة

انطلاقا من مقولة "الوقاية خير من العلاج "فقد قامت الوكالة بوضع مخطط شامل لمصلحة الأرشيف تم تطبيقه في أرض الواقع مع التوسعة التي مست الوكالة وتم الانتهاء منها بسنة 2017 نذكر منها:

- **المراقبة اليومية :** يتم مراقبة قاعة الأرشيف يوميا من طرف المشرفين على قاعة ومنع دخول الأشخاص إليها من دون ترخيص كما يقوم أعوان الأمن بمراقبة القاعة خارج دوام العمل مع مراقبة حنفيات المياه والتسربات التي قد تقع داخل دورات المياه حتى لا يصل الماء إلى قاعة الأرشيف

- **وسائل إطفاء الحريق :**

وتتمثل في المطافئ (Les Extincteurs)حيث يوجد نوعين من المطافئ في قاعة لأرشيف وهما: مطافئ معبأة بثاني أكسيد الكربون (CO2)و مطافئ معبأة بمسحوق ثاني فحمات الصودا وهو المفضل في حال حريق الأرشيف (Extincteur à prouder bicarbonate de soda) ويشمل عدة أصناف الحريق مبينة في الشريط اللاصق في المطفأة بالحروف(A-B-C-D)كما يوضح الشركة التي عبأت المسحوق مع تاريخ نهاية الصلاحية

صورة رقم(03) تمثل مطفأة الحرائق

صورة رقم (04) تمثل أصناف الحرائق

أصناف الحرائق :

A- الصلب

B- السائل.

C- الغاز.

D- الكهرباء (1000 VOLT -)

- **عازلات الشمس :**

تم وضع عازلات للشمس في كل النوافذ لمنع دخولها حتى لا يتضرر الأرشيف وتركيب شبكة إنارة خاصة لإعطاء الإنارة المناسبة في القاعة وتم طلب ترمومتر لقياس حرارة القاعة ولم يركب إلى يومنا هذا .

- **تطهير قاعة الأرشيف :(La Disinfection de la Salle d'Archives)**

تتم عملية تطهير قاعة الأرشيف كل ثلاثة أشهر أي أربع مرات في السنة من طرف شركة متخصصة في ذلك وبمواد مخصصة للقضاء على التعفن الذي قد تسببه الرطوبة أو الحشرات الصغيرة بالإضافة إلى مادة خاصة بالقوارض توضع فوق سقف القاعة لطردها نهائيا من السقف ،من خلال وثيقة رسمية موقعة من الطرفين . **(أنظر الملحق رقم 04)**

صورة رقم (05)تمثل عملية التعقيم داخل قاعة الارشيف

6-3-3- ترتيب وتصنيف الرصيد الوثائقي داخل مصلحة الأرشيف بالمؤسسة :

بعد القيام بعملية الفرز و معالجة للرصيد الوثائقي يتم ترتيبه وفق المعايير المعمول بها عالميا و حفظه مبدئيا و التي يعتمد في ذلك على ترتيب وفق المصالح بوضعها داخل العلب ذات مقاييس معمول بها في الأرشيف (35 سم طول، 10 سم عرض و25 سم ارتفاع) و التي تحفظ على نمطين من الرفوف في ذلك :

- **الرفوف المدمجة المتحركة :** (Les Rayon ages mobiles) :تتكون من 07 خزانات حديدية متحركة الثابتة يتم فتح الممر المستخدم فتتضاعف المساحة المخصصة للتخزين ،كما تحتوي الرفوف على نظام تحريك قوي وعجلات التوجيه تنقل الأحمال الثقيلة بجهد أقل. واجهة الرفوف مغلقة بأبواب كل باب له المفتاح الخاص به، كما تحتوي على نظام إغلاق محكم بحيث لا يمكن الاطلاع على

محتوى من طرف المشرفين على المصلحة. فيتم ترتب فيها ملفات المتقاعدين لوحدها وذلك حسب رقم كل ملف (رقم منحة التقاعد) الموضوع على الغلاف الخارجي للملف

صورة رقم 06 تمثل الرفوف المدمجة المتحركة في قاعة الأرشيف

عدد الخزانات المتحركة	الواجهة	عدد الصفوف في الخزانة	عدد الرفوف في الصف	عدد علب الأرشيف في الرف	عدد علب الأرشيف في الواجهة الواحدة للخزانة
07	02	08	06	09 / 11	252
المجموع	14	56	336	//	3528

جدول رقم 06 يمثل سعة تخزين الملفات في رفوف الخزانة المتحركة المدمجة بقاعة الأرشيف

- **الرفوف الثابتة**

يرتب أرشيف المالية، أرشيف مصلحة المسارات المهنية، ملفات المنح العائلية بالإضافة إلى ملفات التقاعد المرفوضة حسب الترتيب التالي:

- **أرشيف المالية** :يرتب أرشيف المالية ترتيب رئيسي حسب الموضوع ويتكون من ثلاثة مواضيع : المدفوعات، الإيرادات وعمليات مختلفة ونجد ترتيب ثانوي وهو ترتيب زمني حسب السنة المالية
- **أرشيف مصلحة المسارات المهنية** :يتكون من التصريحات السنوية للأجور مرتبة ترتيبا رقميا حسب رقم المستخدم (N° D'EMPLOIEUR) .
- **ملفات التقاعد المرفوضة:** ترتيب رقمي : ترتب حسب رقم ما قبل التصفية .
- **ملفات المنح العائلية :** ترتيب رقمي :ترتب حسب رقم المنحة.

صورة رقم 07 تمثل الرفوف الثابتة في قاعة الأرشيف

عدد الرفوف	الواجهة	عدد الصفوف في الرف	عدد الرفوف في الصف	عدد علب الأرشيف في الرف	عدد علب الأرشيف في الرف
02	01/02	03/04	06	09 / 12	360/270
المجموع	03	10	60	//	630

جدول رقم 07 يمثل السعة التخزينية للرفوف الثابتة داخل قاعة الأرشيف

و عليه فإن معيار الخاص بتصنيف المعلومات للفصل الرابع من معيار إيزو 27002 الذي يدعو إلى تصنيف المعلومات حسب وحساسيتها وتتلقى مستوى مناسب من الحماية محقق في مصلحة الأرشيف .

4-3-رقمنة الرصيد الوثائقي:

إن الرصيد الوثائقي قد تم رقمنته كليا وبطريقة منتظمة بإتباع الاولوية في عملية الرقمنة وذلك برقمنة الملفات القديمة اولا وصولا إلى الملفات الجديدة و بذالك نكون قد تم تحويل الوثائق الورقية إلى وثائق إلكترونيا التي تمت على مستوى مكتب مصلحة التسيير الإلكتروني للوثائق[1]: المجهز ب 03 حواسيب و 02 ماسحات ضوئية واحد مسطح والآخر تلقائي و التي تستعمل في عملية الرقمنة و قد إستغرقت مدة زمنية طويلة لإتمامها فاصبح الرجوع والاطلاع على أي ملف يكون إلكترونيا،إلى في حالات نادرة جدا يتم الرجوع إلى الأصل الورقي . وعليه فإن رقمنة الرصيد الوثائقي سهلت من عملية

[1] مكتب التسيير الإلكتروني مؤسسة الصندوق الوطني للتقاعد: يبلغ مساحته 25.5 م^2 ،يحتوي المكتب على هاتف ثابت 03 مكاتب خشبية ،طاولتين 04 كراسي، وخزانة بالإضافة إلى مدفأتين ومكيف هوائي ،كما تتواجد به 03 نوافذ كي تساعد على الإضاءة والتهوية الجيدة للقاعة مجهز بإنذار الحرائق

الإطلاع على الملفات والرجوع إليها في وقت وجيز وبدون عناء أو جهد يذكر غير انه لا هذا لا يعني إهمال الارشيف الورقي لأنة المصدر الاولي للرصيد المرقمن

3-5-توفر المؤسسة على شبكة الانترنت:

أفادنا المبحوث بعدم وجود شبكة الانترنت داخل المؤسسة و تعويضها بإستخدام الشبكة المحلية وذلك راجع إلى أهمية الوثائق المتوفرة داخل المؤسسة لأنها تعبر عن قيمة مالية مع الأخذ بمبدأ الحيطة والحذر للمعلومات والتأكد من سرية المعلومات والذي يهدف إلى أن تكون هذه المعلومات في معزل عن تدخل أي شخص غير مصرح له بالاطلاع عليها سواء كان من داخل الهيئة أو من خارجها التأكد وبصفة مستمرة من ان المعلومات متوفرة وبعيدة عن أي تهديد يعرضها للتلف أو التعديل أو السرقة. وبالابتعاد عن أي مصدر تهديد من الخارج وفي حال وجود الشبكة تصبح هذه الوثائق أكثره عرضة للأخطار والاختراقات المتعلقة بالشبكة ووصول الأشخاص الغير مخول لهم بذلك إلى هذه المعلومات الخاصة والمتعلقة بالمتقاعدين بالإضافة إلى ضعف القوانين والإجراءات المتعلقة بالجريمة الإلكترونية والحماية على مستوى شبكة الانترنت في الجزائر ،وبهذا يمكن تحقيق الأمن المعلوماتي داخل المؤسسة بالتحكم في المعلومات دون استعمال شبكة الانترنت لكنه لا يمكن اعتبار عدم وجود الشبكة أمر إيجابي 100% لأنها ضرورية في بعض الاحيان في العمل.

3-6- **وجود الحماية على مستوى الانظمة والبرامج داخل المؤسسة :**

تتم الحماية الانظمة و البرامج داخل مؤسسة الصندوق الوطني للتقاعد عن طريق استخدام الكلمات السر والمرور تعد من أهم وسائل حماية المعلومات فهي تعتبر القفل على الخزينة الإلكترونية لما تقوم به من حماية للمعلومات وأنظمة التشغيل الخاصة بالمستخدم كما تعتبر أحد مكونات منظومة حماية المعلومات فهي تساعد على التحقق من هوية المستخدم وفاعليتها وتعتمد على درجة انضباط العنصر البشري في اختيارها والتعامل معها وفق أساليب صحيحة بحيث تختلف كلمات المرور من موظف لآخر لزيادة مستوى الحماية للأنظمة والبرامج ولا يمكن الوصول إلى المعلومات سوى للشخص المصرح له بذلك بالإضافة إلى تحمل كل موظف للخسائر الناجمة عن أي خطا يمكن ان يحدث على مستواه لأنه الوحيد الذي يمتلك كلمة المرور ،بهذا تزيد درجة الحماية والامن للمعلومات. وبالرجوع إلى معيار إيزو 27002 لأمن المعلومات فهذا يتطابق مع ما جاء فيه حول التحكم في الوصول إلى البرامج والتطبيقات في الفصل الثامن الخاص بالتحكم بالوصول. من خلال مؤشر التأكد من تأمين الأنظمة والبرامج الخاصة بالمنظمة عند استخدامها .

3-7-**نظم الإنذار التي تساعد في اكتشاف الاخطار المتوقعة داخل مصلحة الارشيف:**

يوجود نوع من نظم الإنذار التي تساعد في إكتشاف الأخطار المتوقعة و المتمثل في شبكة الإنذار المبكر للحرائق: يهدف هذا النظام إلى الإنذار المبكر للحريق عند اندلاعه لكي يتمكن أعوان الأمن من التدخل الفوري فهي بمثابة المرشد لأعوان الأمن بإعطاء إنذار إذا ارتفعت درجة حرارة المكان الموجود

فيه جهاز إنذار عن الدرجة المكان المعتادة دائما بطريقة آلية وإلكترونية فهذا النظام يساعد في معرفة والتنبؤ بوجود امر غير طبيعي يستدعي التأكد من الامر بالإضافة إلى إخبار الموظف بوجود حريق في بدايته فهو يساعد على تفاديه والتقليل من الخسائر الناجمة عنه داخل المؤسسة عامة وقاعة الأرشيف خاص لأنها تحتوي على ملفات ضخمة وذات اهمية كبيرة للمتقاعدين و مكتب التسيير الإلكتروني بوجود الحاسبات فيها إضافة إلى الشكل.

الكتروني للرصيد الوثائقي في مكتب التسيير الإلكتروني.

صورة رقم 08 تمثل نظام الإنذار لشبكة الإنذار المبكر للحرائق

وتتكون الشبكة الإنذار المبكر للحرائق من :

نظام الإنذار: نظام خاص يرشد أعوان الأمن في أي طابق تم كشف دخان الحريق من طرف كاشفات الدخان

كاشف الدخان: ينطلق عند ظهور الإشارات الأولي للدخ حتى في حالة التدخين من قبل أي شخص

مصباح الإنذار :يوجد فوق كل باب من أبوب المكاتب يتوهج مصباح الإنذار عند الكشف عن دخان الحريق من طرف كاشف الدخان للدلالة على المكتب الموجود به الحريق.

صورة رقم 09 تمثل كاشف الدخان شبكة إنذار الحرائق

صورة رقم 10 تمثل مصابيح الإنذار لشبكة الإنذار المبكر

فهذه النظم تزيد من الامن المعلوماتي داخل المؤسسة وتمكن من الحفاظ على هذه المعلومات المتواجدة على مستوى المؤسسة. كما تساعد على معرفة حوادث المتعلقة بأمن المعلومات وبالتالي معرفة إدارتها وتفعيل الإجراءات اللازمة لضمان سرعة في تفادي وقوع مثل هذه الحوادث الامنية داخل المؤسسة وهذا ما نص علية الفصل العاشر من معيار إيزو 27002 الخاص بإدارة حوادث أمن المعلومات . ويتوافق معه. بالإضافة إلى تطبيق جزئي لمعيار تأمين المعدات الخاص بفصل الأمن المادي والبيئي لمعيار إيزو 27002.و ذلك بعدم وجود أجهزة رصد الرطوبة داخل المؤسسة .

3-8- إعتماد المؤسسة على كاشفات إلكترونية البيولوجية كوسائل للحماية وتحقيق الأمن المعلوماتي داخلها :

إن المؤسسة الصندوق لا تعتمد على هذا النوع فهي لا تعتمد على هذا النوع من الوسائل ولا تتوفر على مستواها وذلك راجع إلى وجود وسائل أخرى التي من شانها تحقيق الامن للمؤسسة ككاميرات المراقبة مركبة على الحوائط والأسوار وبزوايا متعددة مرتبطة بلوحة تحكم شاشة التي يمكن أن تساعد على تأمين المنشأة من الداخل والخارج ،بالإضافة إلى الثمن الباهظ لهذه الوسائل مع غياب ميزانية خاصة بأمن المعلومات داخل المؤسسة ،لكن تعتبر هذه الكاشفات من بيم الامور التي تسعى المؤسسة إلى توفيرها في أقرب وقت ممكن وذلك للدور الذي تلعبه في تحقيق الامن المعلوماتي للمؤسسة الذي يعتبر مطلب أساسي تسعى المؤسسة إلى الوصول إلية بأعلى درجاته دائما.

3-9- وسائط التخزين المستعملة لحفظ البيانات والمعلومات داخل مصلحة الأرشيف:

فحسب إجابة المسؤول عن وسائط التخزين المستعملة فقد صرح بوجود الخادم serveur كوسيط تخزين وذلك راجع لوجود الكم الهائل للمعلومات داخل المصلحة بحيث يقوم بحفظ لكل الملفات على مستواه لضخامة القدرة الاستيعابية التي يمتلكها ولا يمكن لأي وسيط آخر ان يحفظ بنفس سعته، بالإضافة إلى كونه وسيط معلوماتي آمن و لا يسمح سوى للمخولين الاطلاع على الوثائق الموجودة وفيه ،وهذا مع يتوافق على ما جاء بيه الفصل التاسع المتعلق بإدارة العمليات / الاتصالات في معيار الفرعي 07 خاص بالتعامل مع وسائط التخزين،لمعيار إيزو 27002،الذي ينص على ضرورة تخزين الوثائق في مكان آمن يسمح فقط للأشخاص المخولين بالاطلاع عليها. أما فيما يخص كيفية اقتناءه فذلك فقد تم ذلك عن طريق الموردين من خلال المناقصات ،غير أن وجود وسيط تخزين واحد داخل مصلحة الأرشيف أمر غير كافي وهذا للكم الهائل للوثائق المتواجدة فيها بالإضافة إلى ضرورة وجود نسخ من هذه الملفات في حال تعرضها للتلف على مستوى الخادم يتم الرجوع إليها وقتها. اما فيما يخص طريقة معالجة هذه الوسائط المعتمدة داخل المؤسسة بما ان الرصيد الوثائقي مرقمن كليا هذا الامر يدعي وجود طريقة إلكترونية لأن التعامل مع الوثائق أصبح إلكترونيا وتتمثل هذه الطريقة بوجود عملية المسح عن طريق مضادات الفيروسات على هذه الوسائط بالإضافة إلى وجود عملية تحديث للمعطيات الآلية المخزنة عليها التلقائيا .

3-10 البرامج و الأنظمة المعمول بها داخل مصلحة الأرشيف التي من شأنها تحقيق الامن المعلوماتي :

فقد صرح المسؤول بوجود برنامج Network الذي يعتبر برنامج مسح أمني يستخدم لفحص المنافذ واستكشاف الشبكات بالإضافة إلى انه يستخدم في المراقبة فهذا البرنامج يعتبر من أولى البرامج المعمول بها في المصلحة حيث يتم اقتناء برامج التشغيل واستغلال شبكة المعلومات في ذلك ،فقد أضاف هذا البرنامج الكثير لأمن المعلومات داخل مصلحة الأرشيف للمزايا التي يمتلكها من فحص

للمنافذ ومنع دخول أي أمر مشكوك فيه بالإضافة إلى مراقبة المعلومات المدرجة على مستواه ،كما انه يفي بغرض توفير امن المعلومات داخل المصلحة مما يعطي للمعلومات مصداقية وأكثر خصوصية .و عليه يتوافق هذا مع الفصل الثالث لمعيار إيزو 27002 في مؤشر الخاص تحديد المخاطر ذات الصلة بأطراف الخارجية

3-11- كيفية حماية المعلومات على مستوى الأنظمة والبرامج داخل المؤسسة:

إن الحماية على مستوى الانظمة و البرامج في مؤسسة الصندوق الوطني للتقاعد تتم باختيار كلمات مرور وتحديثها دوريا كون أن كلمات المرور تعتبر أحد مكونات منظومة حماية المعلومات من الاختراق والوصول غير مسموح به للأشخاص الغير مصرح لهم بالوصول بسهولة بالإضافة إلى إعطاء المعلومات خاصية الوصول والاطلاع عليها ،غير أنه لا يمكن اعتبار كلمات المرور طريقة مثلى لحماية المعلومات ولا تجنب الوصول إليها من طرف أشخاص غير مرغوب بهم فهي سهلت الاختراق مقارنة مع طرق أخرى وإجراءات أخرى .غير أن مطلب الحماية للأنظمة والبرامج التشغيل أمر ضروري مهما كانت الطريقة في ذلك وهذا ما نص عليه الفصل الثامن من معيار إيزو 27002 المتمثل في التحكم في الوصول في المعيار الفرعي الخامس الخاص بالتحكم في الوصول إلى أنظمة التشغيل الذي يهدف إلى منع الوصول غير المصرح به إلى نظم التشغيل واستخدام أقصى درجات الأمن وذلك بفرض استخدام كلمات المرور قوية وتحديثها بعد كل دخول

صورة رقم 11 تمثل الوسائل و التجهيزات المتوفرة في مصلحة الأرشيف

الإمكانيات المتاحة (مادية، مالية، تقنية) ومدى كفايتها في مصلحة الارشيف :

افاد المبحوث حول هذه فهي كافية للموظفين لتأدية أعمالهم داخل المؤسسة فهي توفر لهم الوقت والجهد في إتمام أعمالهم ووظائفهم اليومية التي يقومون بها على مستوى المؤسسة، ولكن بالرغم من نقض بعض التجهيزات و المعدات التي من شانها ان تقدم المزيد للمؤسسة مثل الإلكترونية البيولوجية وغياب ميزانية خاصة بأمن المعلومات الامر الذي من شأنه أن يعطي الموظف راحة اكثر في تأدية عملة في ظروف جيدة ،إلا ان الإمكانيات المتوفرة تفي بالغرض ولا يمكن تغاضي النظر على ما تقدمة من مساعدات وإضافات للموظفين داخل المؤسسة ،لهذا فهي تمثل عنصر

أساسي وضروري داخل المؤسسة لتمكين الموظفين من إنجاز

اعمالهم في ظروف جيدة وبمصداقية. غير أنه لا التوافق مع ما هو موجود في معيار إيزو 27002 فإن توفر الإمكانيات المادية ضروري و أمر هام جدا من أجل تحقيق امن المعلومات داخل المنظمة .

أفاد المبحوث حول هذه النقطة بكفاية الإمكانيات المتاحة كافية على الرغم من بعض النقائص،لكن ما نراه و على ما تم مقارنته بالمعايير نرى بان الإمكانيات ناقصة في حال وجود خطر على المعلومات ،

4- معايير أمن المعلومات المتبعة داخل مصلحة الأرشيف بمؤسسة الصندوق الوطني للتقاعد

4-1- اولويات ترتيب مكونات أمن المعلومات:

إن أمن الوثائق في مراكز الحاسبات يحتل الصدارة حيث يجب حفظها في مواقع خاصة وتحقيق السرية العالية لها داخل المؤسسة كما أن تصنيفها من حيث أهميتها وسريتها يعتبر من الوسائل المساعدة للوصول إلى هذه الوثائق لان العمل داخل المؤسسة أصبح رقمي لهذا اوجب تأمين الوثائق في مراكز الحاسبات بالدرجة الاولى، وبعد ذلك تأمين أنظمة التشغيل والبرمجيات التي تمكن من الوصول إلى هذه الوثائق وذلك باتخاذ الإجراءات الامنية لضمان سلامة أنظمة التشغيل والبرمجيات وذلك بوضع حواجز تعرقل الوصول إليها والدخول لها من خلال وضع كلمات المرور وبهذا نكون قد حمينا المعلومات من محاولات التدخل الغير مشروع ،وبعد تحقيق الامن للمراكز الحاسبات وأنظمة التشغيل يأتي الدور على تأمين أجهزة الحاسبات وذلك بتوفير الامن للأجهزة وملحقاتها المادية مثل الطابعات وأخيرا توفير الأمن للأفراد والإدارة وهذا الترتيب حسب مؤسسة الصندوق الوطني للتقاعد حسب الأولوية التي يراها المسؤول والتي تخدم المؤسسة .و بهذا يمكن القول بأن هناك وجود سياسة امنية لكن بدون وثيقة عامة لسياسة أمن المعلومات و هذا لا يتوافق مع المؤشر الخاص بوجود وثيقة عامة لأمن المعلومات لمعيار إيزو 27002 لأمن المعلومات ولكن يمكن القول بإن هذا المؤشر مطبقا جزئيا و ذلك بغياب الوثيقة في حين وجود سياسة .

4-2- اعتماد مصلحة الأرشيف على معايير عالمية ودولية لأمن المعلومات:

أن مصلحة أرشيف لا تعتمد على المعايير الدولية في تحقيق أمن المعلومات حسب إجابة المسؤول فيما يتعلق بهذه النقطة حيث برأيه أن تحقيق أمن المعلومات بدرجات عالية يتوجب وجود معايير متفق عليها دوليا ولكن هذا لا يمنع من وجود قوانين صارمة يمكن أن تحقق الأمن المعلوماتي داخلها وهذا ما يتم إتباعه من طرف المصلحة الأرشيف في عملية التسيير بوجود قانون داخلي لأمن المعلومات وذلك بالاعتماد على تخصيص عدة مواد قانونية(لم نستطيع الحصول على هذه المواد من طرف المسؤوول) في النظام الداخلي المعمول به لأجل حماية الأجهزة المعلوماتية وكذلك المعطيات الخاصة بالمتقاعدين الذين أودعوا ملفاتهم داخل مصلحة الأرشيف بالمؤسسة فهذا القانون الداخلي يعطي نوعا من الأمن للمعلومات كما أنه يضمن سريتها وحمايتها إلا انه حبذا لو كان العمل و التوافق مع السياسات و المعايير العالمية التي سوف يكون لها أثر واضحو أكثر دقة في حال العمل بها في تحقيق أمن المعلومات داخل المؤسسة. وهذا ما نص عليه الفصل الثاني عشر من معيار إيزو 27002 في المعيار الثاني الذي يدعو إلى التأكد من الإجراءات الامنية المتبعة وتوافقها مع السياسات والمعايير

الأمنية العالمية ،وعلية فإن هذا المطلب من المعيار غير محقق على مستوى مؤسسة الصندوق الوطني للتقاعد.

و فيما يخص مدى تحقيق الأمن للمعلومات من خلال الاعتماد على القانون الداخلي فقد أكدا لمبحوث انه يحققه نوعا ما لأنه من وضع المدير وبعض رؤساء المصالح فهم ليسوا على دراية كافية بكل مستجدات التي تحصل في مجال أمن المعلومات ولهذا يمكن القول ان القانون الداخلي لا يوفر امن المعلومات بشكل عام ويشمل جميع الامور داخل المؤسسة كونه يفتقر إلى أساسيات الامن التي تقرها المعايير الدولية التي تقرها المعايير الدولية لامن المعلومات لذلك وجب على المؤسسة أن تسعى إلى العمل بمعايير عالمية لأمن المعلومات من أجل حماية المعلومات من كل أنواع الأخطار والمهددات التي يمكن أن تتعرض لها داخل المؤسسة .و عليه فإن مؤشر المراجعة لسياسة امن المعلومات الخاصة بالفصل الثاني من معيار إيزو 27002 غير محقق

4-3- رأي المسؤول حول غياب المعايير العالمية وتأثيرها في تحقيق الأمن المعلوماتي في المؤسسة:

حسب تصريح المسؤول حول غياب المعايير فقد كانت إنه طبعا سوف يؤثر غيابها على تحقيق الأمن المناسب و الفعال للمعلومات داخل المؤسسة ويتمثل هذا التأثير في تحقيق منظومة معلومات بمقاييس عالمية على سبيل المثال بالإضافة إلى أن نظام المعلومات داخل مؤسسة الأرشيف سيكون بطيئا ومعرضا لأخطاء،ولا يمكن الثقة فيه لأنه سيجعل المؤسسة في خطر من الحفاظ على سلامة المعلومة وحفظها وإتاحتها أيضا للمستفيدين. وافتقار عملية الحفظ والتنظيم والتسيير إلى مرجع عالمي صحيح.

4-4- رأي المسؤول حول ما الذي سوف تضيفه المعايير في حال اعتمادها داخل المؤسسة:

فقد صرح بأنها سوف تحقق الكثير من حماية أمن المعلومات للمؤسسة فقد ذكر أن تلك الحماية تحمي النظام ككل ومكوناته والتأكد من عدم تعرضها للمخاطر وإتاحتها للأشخاص غير المعنيين،بالإضافة إلى أن اتباع المعايير يبعد المؤسسة عن الافلاس وخطر فقد المعلومات القيمة كون المعلومة رأسمال استراتيجي. بالإضافة إلى تقديم العديد من الأمور التي تفتقر لها المؤسسة مثل أنها سوف تقدم مبادئ توجيهية بخصوص أمن المعلومات يجب إتباعها لتحقيه في المؤسسة بدرجة عالية وأكثر دقة ،توفير معايير وأسس الرقابة الجيدة على موارد أمن المعلومات بالإضافة إلى أنها تحدد كل المتطلبات الواجب توفرها لتحقيقه داخل المؤسسة بغض النظر على الدرجة العالية من الأمن التي توفرها للمعلومات داخل المؤسسة والانضباط. بالإضافة إلى كون هذه المعايير تكون عبارة عن سياسة واضحة تسيير عليها المؤسسة فإن المؤشر الأول المتمثل في وجود وثيقة لسياسة امن المعلومات الخاص بالفصل الثاني من معيار إيزو 27002 للمعيار الرئيسي السياسة الامنية غير محقق

5- مهددات ومعيقات أمن المعلومات وطرق الحماية منها داخل المؤسسة

1.5. نوع المخاطر و التهديدات التي تتعرض لها المعلومات داخل مصلحة الأرشيف؟

يتضح من خلال الاجابة في المقابلة أن أكبر خطأ متخوف منه هو الخطأ التقني والفني الذي مصدره النظام بحد ذاته،فحسب رأي السيد منصور قد يتناقض النظام مع ما هو مطلوب وبذلك يشل المؤسسة لفترة قد تكون غير معلومة،والوقت مهم في مجال العمل لأن الاستمرارية مهمة والبقاء ضمن العمل لتحقيق الأهداف أيضا مهم. فيجب أن يكون النظام منيعا ضد الأخطاء التقنية والفنية. فمن أمثلة المخاطر التقنية نجد الفيضانات والرطوبة اما فيما يخص المخاطر الفنية نجد سوء الترتيب وعدم احترام التسلسل في الترتيب والإهمال .و حسب ما جاء في الفصل التاسع من معيار إيزو 27002 الخاص بحيازة وتطوير وصيانة انظمة المعلومات في المعيار إدارة ثغرات التقنية في المؤشر الخاص به يدعو إلى وجوب وضرورة التحكم في الثغرات التقنية وعليه فإن هذا المؤشر غير محقق في مصلحة الأرشيف .

2-5- نسبة الخسائر التي تسببها التهديدات لأمن المعلومات داخل مؤسسة الصندوق الوطني للتقاعد:

تعتبر قيمة الخسائر التي تسببها التهديدات الأمنية المعلوماتية الحالية منخفضة،لأنه المؤسسة لم تتعرض المؤسسة إلى تهديدات خارجية خطيرة بل فقط أخطاء تم اصلاحها داخليا لذا وهي ليست بالأضرار البالغة التكلفة،حسب ما تم التصريح به .وهذا راجع إلى وجود ضوابط منع الوصول غير المرخص به وهذا ما يعتبر محققا وفق لمؤشر الحماية من التهديدات الخارجية من الفصل السادس الخاص بتامين المادي والبيئي لمعيار إيزو 27002 وعليه فإن هذا المؤشر محقق في مؤسسة الصندوق الوطني للتقاعد.

3-5- نظام أمن المعلومات بالصندوق الوطني للتقاعد و القرصنة :

إن مؤسسة الصندوق الوطني للتقاعد لم تعترض لقرصنة النظام المعمول به داخل مؤسسة الصندوق الوطني للتقاعد وذلك حسب رأي السيد منصور فإن الموظفين حريصون تمام الحرص على إتباع اجراءات السلامة ومتابعة النظام ومراقبته ومع الصرامة وبرامج الحماية المتوفرة بالإضافة إلى التحكم في الوصول إلى الانظمة فإنه من الصعب اختراق نظام المؤسسة بسهولة. وهذا ما يتوافق مع المؤشرات التي تخص الفصل الثامن من معيار إيزو 27002 التي تخص التحكم في الوصول إلى أنظمة التشغيل بالإضافة إلى التحكم في الدخول من خارج المنظمة ومراجعة وصول المستخدم إلى النظام عن طريق إدارة كلمات المرور .و عليه فإن معيار التحكم في الوصول للفصل الثامن من معيار إيزو 27002 محقق في المؤسسة

4-5- دوافع المقرصنون في اختراق نظام امن المعلومات الخاص بالمؤسسة:

حسب رأي المتحدث فإن الدافع يكون الربح المادي،وفي الحقيقة لا يمكن التنبؤ بأفعال المقرصن والهدف من أفعاله التخريبية ولكن في الغالب يطالب المقرصنون لقاء سرقتهم للمعلومات مبالغ مالية طائلة،كما هو حال شيوع فيروس الفدية الجديد،حيث تقرصن المعلومات وتحجز بصيغ لا يمكن فك تشفيرها ويطلب من المؤسسة أو الضحية(موظف بالمؤسسة) مبالغ مالية طائلة لفتح الملفات واستعادتها. لذلك تتم حماية أنظمة المعلومات بكل الأساليب الممكنة والمتاحة مهما بلغت تكلفة حمايتها.

5-5- الإجراءات المتبعة لمواجهة القرصنة داخل مؤسسة الصندوق الوطني للتقاعد:

إتضح من خلال هذه النقطة المسؤول بأنه يتم إتباع اجراءات جيدة في مواجهة القرصنة،يجب اعتماد شبكة محلية خاصة بالمؤسسة وتكون معزولة عن الانترنيت لأنها أكبر مصدر للتهديدات الأمنية والقرصنة،بالإضافة إلى وضع برامج لتغيير كلمات السر للموظفين بشكل دوري،كما ورد سابقا ،وأيضا وتوعيتهم بمخاطر التهديدات الأمنية وقيمة المعلومة لدى المؤسسة وخاصة المصلحة الأرشيفية،فكثيرا ما يتم الاستثمار في الأرشيف وفي بحثه عن الوثائق النادرة والحفاظ عليها. مع عدم استعمال وسائط تخزين المعلومات كفلاش ديسك وذلك كإجراءات للتعامل مع المعلومات وتوفير الامن لها على مستوى المؤسسة بشكل عام ومصلحة الأرشيف بشكل خاص، إذن فإن مؤشر تطبيق إجراءات التعامل مع المعلومات للمعيار الرئيسي التعامل مع وسائط التخزين من الفصل السابع لمعيار إيزو 27002. محقق.

5-6- **الأجهزة الإلكترونية لمؤسسة الصندوق الوطني للتقاعد و الإختراق :**

إن مؤسسة الصندوق الوطني للتقاعد لم يسبق لها و ان تعرضت للاختراق الخارجي وفقا ما أجاب به المبحوث سواء خلال فترة عمله او إطلاعه على حياة المؤسسة ، على ذلك لأنها غير مربوطة بالشبكة العالمية، وتكتفي في كثير من المعاملات بالطرق التقليدية والإجراءات المادية،فهذه الطريقة تزيد من الأمان ولكن بها عيوبها من التكلفة الزمنية والمكانية على مستوى المكاتب. أما على المستوى الداخلي فالموظفون منضبطون في عملهم ويشعرون بأهمية المعلومات بالمؤسسة،ولا يسمحون بأي شخص بالعبث بالنظام. عن طريق وجود أساسيات للدخول إلى الأجهزة وعليه فإن مؤشر تامين الوصول إلى الأجهزة من معيار مسؤوليات المستخدم للفصل الثامن من معيار إيزو 27002 محقق.

5-7- الإجراءات المعتمد لمواجهة الإختراق في مؤسسة الصندوق الوطني للتقاعد :

البقاء خارج شبكة الانترنيت هو أحسن وسيلة للبقاء خارج التهديدات فهو يعتبر إجراء أمني للابتعاد عن مهددات أمن المعلومات وحماية نظم المعلومات ،سواء نظام المؤسسة أو أي نظام، فهذا هو ما اقترحه المسؤول لأنها أول وسيلة تخفف من خطر التهديدات على النظام، ومن البديهي أن تكون شبكة الأنترنت مصدر تهديد خاصة من جهة الويب الخفي والذي يحتمل أن تكون فيه مصادر غير معروفة، والنظام الآمن حسب تعبيره هو النظام البعيد عن المشاكل. ويضمن توفير أمن المعلومات واستمرارية العمل الأمر الذي وافق ما جاء به فصل إدارة استمرارية الأعمال من معيار إيزو 27002 الذي يهدف إلى

حماية نظم المعلومات من الأعطال الرئيسية والكوارث وضمان إعادة تشغيل النظام في الوقت المناسب.

5-8- أنظمة و برامج مؤسسة الصندوق الوطني للتقاعد و تعرضها لخطر الفيروسات

يذكر السيد منصور في اجابته أن المؤسسة لم تتعرض لخطر الفيروسات، والفضل يعود إلى تحكم العاملين في الحواسيب وعدم إدخال الأقلام المليزرة (فلاش ديسك) أو أي أداة تخزين خارجية إلى الحواسيب بالإضافة إلى توفر واستخدام أنظمة الحماية من الفيروسات والبرامج الخبيثة في كل حاسوب، فهذه الاجراءات وان كانت عادية إلا أنها مفيدة ووقائية، فبالنسبة للعمال فالوقاية خير من العلاج. إذن فإن هذا الإجراء يتوافق مع ما جاء به معيار إيزو 27002 في فصل خاص بإدارة العمليات والاتصالات في عنصر الحماية من البرامج الخبيثة .

5-9- الإجراءات الوقائية لمواجهة خطر الفيروسات داخل مصلحة الأرشيف:

تتبع اجراءات عديدة في مصلحة الأرشيف للوقاية من خطر الفيروسات فتستخدم برامج حماية من الفيروسات التي تتمثل في kaspersky وAVIRA وAVG، وهذا ما يوافق ما جاء في مؤشر حماية البيانات النظم في المعيار أمن ملفات النظام الخاص بالفصل التاسع لمعيار إيزو 27002 كما أنهم يقومون بتحميل دوري في كل شهر بنسخ من الملفات والمجلدات الموجودة على الحواسيب والخوادم، ونقلها في خزان صلب ومعزول لحمايتها كذلك من وصول الفيروسات لها. هذا الاجراء يساهم في وضع نسخة احتياطية للنظام حتى وان تعطل دون فيروسات أو تهديدات. وعلية فإن المؤسسة بإتباعها وتطبيقها لمثل هذه البرامج لمواجهة خطر الفيروسات فهي تكون تساهم في تحقيق الامن المعلوماتي للمؤسسة وإعطاء المعلومات نوع من المصداقية

5-10- أساليب مواجهة تهديدات أمن المعلومات أكثر استخداما داخل مصلحة الأرشيف:

يعتبر موظفو مصلحة الأرشيف أن تحديد العقبات أولا أهم خطوة لتوفير مستوى مناسب لتدابير الحماية الأمنية، فإذا ما تم تحديد التهديد وفهمه كانت خطوة مهمة للسيطرة عليه،ثم تتخذ التدابير المناسبة. فكل تهديد له شكله الخاص لذا يجب التعامل معه ،على هذا الأساس. و من أجل تفادي أي خطر يجب معرفته وتحديد الامور التي تحول دون توفير المستوى المطلوب من أمن المعلومات داخل المؤسسة لتسهيل الأمر و تفادي وقوع المهدد و حتى في حال وقوعه فلم تكن هناك خسائر كبيرة. وهذه النقطة تدرج ضمن الإبلاغ عن حوادث أمن المعلومات داخل المؤسسة وهذا ما هو موجود في للفصل العاشر من معيار إيزو 27002 في مؤشر الخاص بإبلاغ عن نقاط الضعف الامنية إذن المؤشر محقق

5-11- الطرق المتبعة للحماية الأمنية للمعلومات من أجل تحقيق الأمن المعلوماتي في المؤسسة:

يعتبر المسؤول أنه لتحقيق الأمن المعلوماتي في المؤسسة يجب دائما تحديث الجدار الناري كونه يمنع المتطفلين وغير المصرح لهم بالولوج للنظام، ويضاف له برنامج مكافحة الفيروسات مما يتيح لهم ضبط البرامج الخبيثة وبالتالي مكافحتها حيث يبقي النظام مراقبا ونظيفا من التهديدات، بالإضافة

إلى نظم المراقبة والكاميرات الالكترونية التي تزيد من الحماية من خلال مراجعة كل سجلات المراقبة والتحقيق في أي مشكل قد يقع. و من هنا يمكن القول بأن المعايير الخاص بالحماية من البرامج الخبيثة للفصل السابع من معيار إيزو 27002 محقق

5-12- إجراءات الحماية لأمن المعلومات عبر الشبكة في المؤسسة الصندوق الوطني للتقاعد

لأن مؤسسة الصندوق الوطني لا تتصل بالإنترنيت، وعليه لا توجد اجراءات حماية عبر الشبكة ولكن اجراءات الحماية كلها محلية وداخل النظام في المؤسسة. لأنه حاليا لا توجد رغبة في وضع معلومات المؤسسة على النت مخافة التسلل للنظام واختراقه إلى حين توفير نظم وإجراءات مناسبة. في حال اعتبار عدم وجود حماية للشبكة فهذا يتنافى مع معيار إدارة أمن الشبكة للفصل السابع من معيار إيزو 27002 الذي ينص على ضرورة ضمان حماية المعلومات في الشبكات، وذلك عن طريق ضوابط الامنية للشبكات غير أن عدم وجود التعامل بالشبكة فهذا في حد ذاته أمر لا يدعو إلى وجود حماية على مستواها

5-13- الإجراءات المتخذة لحماية أمن المعلومات من خطر الأشخاص غير مخول لهم من الوصول إلى المعلومات:

تتم إتباع إجراءات عديدة منها: يتم تحديد الشخص غير مخول له، يتم مساءلته عن الهدف من دخوله إلى نظام المعلومات دون اذن، في حالة ما اذا اشتبه فيه يتم الاتصال بالأمن والمصالح المختصة بذلك، مع معرفة من المتسبب في الثغرة وتنبيهه للأمر والمخاطر الناجمة عن ذلك. وعلية يمكن اعتبار هذا الإجراء فعلي ومتوافق مع ما جاء به معيار إيزو 27002 في فصل التحكم في الوصول للمعيار الفرعي الخاص بإدارة دخول المستخدم الذي ينص على ضرورة وضع إجراءات للتحقق من هوية المستخدم قبل منحه اسم المستخدم وكلمة المرور وبالتالي في حال عدم توافق هذه الأمور يتم السيطرة على خطر الأشخاص الغير مخول لهم بالوصول إلى المعلومات وبالتالي يمكن تحقيق الامن للمعلومات داخل المؤسسة.

5-13- تحديث نظم حماية المعلومات و النظم الامنية في مؤسسة الصندوق الوطني للتقاعد:

من الضروري أن يتم تحديث نظم حماية المعلومات والنظم الأمنية في كل مرة، ففي العصر الحديث دائما ما تتطور التهديدات وتتطور وسائل الحماية منها، لذلك يجب التكيف مع العصر ومواكبة التطورات لسد الفجوة التقنية بين نظم الحماية الخاصة بنا ونظم الحماية الحديثة وكذلك التهديدات. وكل هذا لمواكبة التطورات التكنولوجية الحاصلة في المجال الأمني . وعليه فإن مؤشر تحديث التطبيقات والنظم في الفصل السابع من معيار إيزو 27002 غير محقق

5-14- آليات تعزيز أمن المعلومات في مؤسسة الصندوق الوطني للتقاعد :

تتمثل أهم آلية في تحسين وتعزيز أمن المعلومات في تعزيز المعايير الدولية الخاصة بأمن المعلومات ،فمن المعروف أن معظم المعايير الدولة تلم بجميع الجوانب وذلك وفق دراسات ومشاركة أبحاث على المستوى الدولي تهدف إلى تطوير أمن المعلومات، وهذا المصدر من المعلومات يساعدنا وخاصة في مؤسستنا بإتباع معايير دولي يزيد من قدرتنا على حماية نظام المعلومات الخاص بنا ويزيد كذلك من فرص الأمن وعدم التخوف من المعلومة.

لقد كان الهدف من دراستنا هو معرفة مدى تحقيق أمن المعلومات في مصلحة الأرشيف بمؤسسة الصندوق الوطني للتقاعد و ذلك من خلال معرفة :

- الإمكانيات المادية و الكفاءات البشرية بالمؤسسة
- معايير أمن المعلومات المطبقة في مصلحة الأرشيف بمؤسسة الصندوق الوطني للتقاعد
- مهددات و أخطار التي تتعرض لها مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد

6- نتائج الدراسة :

6.1. نتائج عامة للدراسة :

- **الإمكانيات المادية و البشرية لتحقيق أمن المعلومات داخل مصلحة الأرشيف في المؤسسة:** الصندوق الوطني للتقاعد

1. الميزانية:

- تخصيص جزء من الميزانية العامة للمؤسسة الصندوق الوطني للتقاعد وفق ما يحتاجه أمن المعلومات ،في حين غياب ميزانية خاصة بأمن المعلومات .

2. الموارد البشرية:

- عدم كفاية عدد الموظفين داخل مؤسسة الصندوق الوطني للتقاعد للقيام بمختلف المهام الموجودة داخلها.
- امتلاك الموظفين داخل مؤسسة الصندوق الوطني للتقاعد لتقنيات التعامل مع الأجهزة الإلكترونية الحديثة
- المؤهلات البشرية التي يمتلكها الموظفين في مؤسسة الصندوق الوطني للتقاعد غير كافية لتحقيق الأمن المعلوماتي داخلها.
- غياب و عدم وجود الدورات التكوينية للموظفين مؤسسة الصندوق الوطني للتقاعد ،
- عدم وجود الوعي كافي الموظفين بأهمية أمن المعلومات داخل مؤسسة الصندوق الوطني للتقاعد .

3. الموارد المادية:

- المؤسسة تتوفر التأمين لمركز الحاسبات داخل مؤسسة الصندوق الوطني للتقاعد يساعدها على توفير الأمن المعلومات فيها .
- توفر الوسائل الراحة و التجهيزات الضرورية داخل مؤسسة الصندوق الوطني للتقاعد التي تساعد الموظف على تحقيق الأمن المعلومات مؤشر جيد في بلوغ المستوى المطلوب من درجة الامن للمعلومات داخل المؤسسة .
- وجود ترتيب للرصيد الوثائقي حسب المصالح أمر يساعد في عملية الرجوع إلى الوثائق وقت الحالة دون جهد و عناء.

- إعتماد المؤسسة على الرصيد الإلكتروني المرقمن سهل أمر الإطلاع على الوثائق و الرجوع إليها في وقت وجيز.
- عدم إعتماد مؤسسة الصندوق الوطني للتقاعد على شبكة الانترنت في الأعمال اليومية للموظفين .و الرجوع إلى الشبكة المحلية في ذلك.
- توفر الحماية على مستوى الأنظمة و البرامج المعلول بها داخل مؤسسة الصندوق الوطني للتقاعد
- توفر مؤسسة صندوق الوطني للتقاعد على نظم الإنذار المتطورة في التنبؤ بوجود حرائق على مستوى المؤسسة ككل .التي تساعدها في تفادي خطر الحرائق داخلها.
- غياب الوسيلة الإلكترونية المتمثل في كاشفات الإلكترونية البيولوجية داخل مؤسسة الصندوق الوطني للتقاعد .
- إعتماد مؤسسة الصندوق الوطني للتقاعد على الخادم فقط كوسيلة تخزين و حفظ للبيانات و المعلومات .و هو غير كافي
- إعتماد مصلحة الأرشيف لمؤسسة الصندوق الوطني للتقاعد على برامج و أنظمة أمنية لتحقيق الأمن المعلوماتي فيها من أجل تحقيق المصداقية الوثائق الأرشيفية.

- **معايير أمن المعلومات المتبعة داخل مصلحة الأرشيف بمؤسسة الصندوق الوطني للتقاعد**

- وجود تطبيق جزئي للمعايير العالمية لأمن المعلومات داخل مؤسسة الصندوق الوطني للتقاعد دون علمهم بأنها معايير دولية المعمول بها في مجال أمن المعلومات. مثلا فيما يخص التحكم في الوصول لأنظمة او المستخدم في معيار إيزو 27002 فهي إجراءات ضرورية و في نفس الوقت مطبقة داخل المؤسسة
- عدم إعتماد مؤسسة الصندوق الوطني للتقاعد على سياسة واضحة لأمن المعلومات على معيار إيزو 27002 بشكل واضح كان له تأثير على تحقيق منظومة معلوماتية بمقاييس عالمية. وهذا ما هو موضح في جدول التطابق بين المؤشرات ..... و ماهو موجود فعلا بالمؤسسة

- **مؤشرات الخاصة بمعيار إيزو 27002 الخاص بأمن المعلومات**

الفصل	المعيار الرئيسي	المعيار الفرعي	محقق	غير محقق
الفصل الثاني	السياسة الامنية	وثيقة عامة لامن المعلومات		غير محقق
		مؤشر المراجعة لسياسة امن المعلومات		غير محقق
الفصل الثالث	تنظيم الداخلي لأمن المعلومات	توفير الموارد البشرية اللازمة لتحقيق	محقق	
	الأطراف الخارجية	المخاطر ذات الصلة بأطراف الخارجية	محقق	
الفصل الرابع	المسؤولية إتجاه الأصول	الاستخدام الأمثل للأصول	محقق	
	تصنيف المعلومات	التعامل مع المعلومات و تميزها حسب وحساسيته	محقق	
الفصل الخامس	إجراءات سابقة للتوظيف	التوظيف		غير محقق
	بإجراءات أثناء أداء الوظيفة	التعليم و التدريب على امن المعلومات		غير محقق
الفصل السادس	تأمين المناطق	أمن محيط الخارجي	محقق	

		تثبيت المعدات و حمايتها العمل في محيط آمن	محقق محقق	
الفصل السابع	الإجراءات التنفيذية	بتحديد الصلاحيات و المسؤوليات	محقق جزئيا	
	التعامل مع الوسائط	إجراءات التعامل مع المعلومات	محقق	
	الحماية من البرامج الخبيثة	ضبط برامج الخبيثة	محقق	
	إدارة تأمين الشبكات	الضوابط الأمنية للشبكات تحديث نظم التشغيل والتطبيقات		غير محقق
الفصل الثامن التحكم في الوصول	تحكم في البرمجيات و الانظمة	تأمين الأنظمة والبرامج الخاصة بالمنظمة تامين الوصول إلى الأجهزة	محقق محقق	
	بالتحكم في الوصول إلى أنظمة التشغيل	الدخول آمن للمستخدمين	محقق	
	إدارة دخول المستخدم	إدارة كلمة المرور	محقق	
	مسؤوليات المستخدم	إدارة كلمة المرور	محقق	
الفصل التاسع		تخزين الوثائق في مكان آمن	محقق	
	إدارة الثغرات التقنية	التحكم في ثغرات التقنية		غير محقق
	أمن ملفات النظام	حماية بيانات نظم امن المعلومات	محقق	
الفصل العاشر إدارة حوادث أمن المعلومات	إدارة عن حوادث أمن المعلومات	المسؤوليات و الإجراءات	محقق	
	إبلاغ عن حوادث أمن المعلومات	إبلاغ عن نقاط الضعف الامنية	محقق	

الفصل الحادي عشر	إدارة عمليات أمن المعلومات و استمرارية العمل	حماية نظم المعلومات من الأعطال	محقق	
الفصل الثاني عشر	التوافق مع السياسات و المعايير	الامتثال للسياسات و المعايير المتبعة		غير محقق

الجدول رقم يمثل مؤشرات معيار إيزو 27002 لأمن المعلومات

مهددات و معيقات أمن المعلومات و طرق الحماية منها داخل المؤسسة

- تعتبر مخاطر الفنية و التقنية و المتمثلة في المخاطر التقنية نجد الفيضانات و الرطوبة اما فيما يخص المخاطر الفنية نجد سوء الترتيب و عدم إحترام التسلسل في الترتيب و الإهمال أكبر مهدد لأمن المعلومات يمكن ان تتعرض له المعلومات داخل مؤسسة الصندوق الوطني للتقاعد .
- نسبة الخسائر التي يمكن أن تسببها مهددات امن المعلومات داخل مؤسسة الصندوق الوطني للتقاعد متوسطة .
- عدم تعرض معلومات المؤسسة الصندوق الوطني للتقاعد لأي خطر سواء القرصنة أو الإختراق يبين أن المنظومة الأمنية المعلول لابس بها و تفي بغرض تحقيق الامن المعلوماتي في المؤسسة
- إعتماد مؤسسة الصندوق الوطني للتقاعد على الشبكة المحلية و وضع برامج لتغيير كلمات السر كإجراءات أمنية لمواجهة خطر القرصنة و الإختراق داخل المؤسسة.
- عدم تعرض الأنظمة و البرامج المعمول بها في مؤسسة الصندوق الوطني للتقاعد لخطر الفيروسات و ذلك بإعتمادها على برامج الحماية من الفيروسات مثل Kasperky.
- إعتماد موظفو مؤسسة الصندوق الوطني للتقاعد على تحديد العقبات التي تقف في طريق توفير الأمن المناسب كإجراء لمواجهة تهديدات أمن المعلوم اتداخلها
- الجدار الناري و برامج مكافحة الفيروسات طرق للحماية الامنية للمعلومات داخل مؤسسة الصندوق الوطني للتقاعد.
- إتباع على تحديد الشخص المخول له بالوصول إلى المعلومات كإجراء لحماية المعلومات من خطر الأشخاص غير مخول لهم بالوصول إليها في مؤسسة الصندوق الوطني للتقاعد.

- عدم وجود تحديث مستمر للنظم حماية المعلومات و النظم الامنية داخل مؤسسة الصندوق الوطني للتقاعد .

6.2. نتائج على ضوء الفرضيات:

الفرضيات الفرعية:

- الفرضية الأولى والتي مفادها أنه: تتوفر مصلحة الأرشيف على الإمكانيات المادية و الكفاءات البشرية اللازمة لت××حقيق الامن المعلوماتي داخلها:الفرضية محققة جزئيا و ذلك لنقص في بعض الكفاءات البشرية و الإمكانيات المادية .
- الفرضية الثانية و التي مفادها أنه : تطبق مصلحة ارشيف للصندوق الوطني للتقاعد لولاية تيسمسيلت على معيار إيزو 27002 في تحقيق الأمن المعلوماتي داخلها: الفرضية هنا محققة جزئيا لأن المؤسسة تعتمد على نظامها الداخلي و هي تطبق بعض مؤشرات معيار 27002 لأمن المعلومات بدون دراية .
- الفرضية الثالثة و التي مفادها أنه :تعتبر الفيروسات و البرمجيات الضارة من بين المعوقات التي تحول دون تحقيق أمن المعلومات في مصلحة أرشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت: الفرضية هنا غير محققة تعتمد مصلحة الأرشيف المؤسسة على تعتمد على طرق و إجراءات وقائية لا بأس بها.

الفرضية الرئيسية:

و التي مفادها :يؤثر الأمن المعلوماتي إيجابا في الحفاظ على سرية المعلومات داخل مصلحة الأرشيف الصندوق الوطني للتقاعد لولاية تيسمسيلت الفرضية محققة جزئيا و ذلك لسبب نقص بعض الإمكانيات المادية و الكفاءات البشرية و عدم مطابقتها لمعيار إيزو 27002 لأمن المعلومات

8- اقتراحات الدراسة :

- ضرورة توفير نسبة ثابتة من الميزانية لأمن المعلومات داخل المؤسسة .
- زيادة عدد الموظفين داخل مصلحة الأرشيف
- القيام بدورات **تكوينية** وندوات تحسيسية حول مخاطر الاختراق وآليات الدفاع منها
- تدريب الموظفين بشكل مناسب لزيادة وعيهم حول أهمية المعلومات ادراكهم كيفية التعامل مع التقنيات الحديثة وتعاملهم مع التهديدات الأمنية المحتملة أو الأخطاء التقنية التي تصيب النظام وكيفية التعامل معها
- اقتناء برامج وآليات شاملة لحماية نظام المعلومات من الأخطار و التهديدات
- اقتناء برنامج حماية من الفيروسات من موردين عالمين مشهورين أو محليين يتبعون معايير عالمية
- مؤسسة الصندوق الوطني للتقاعد مطالبة أن تحدث نظم المعلومات بشكل مستمر لأنه ومع التطور الحاصل من الخطر البقاء في نفس النظام وعدم تحديثه
- القيام بتقييم دوري في شكل تقارير مصدرها النظام والموظفون لأجل فحص مستوى النظام ومعرفة كل ما يتعرض له وما يحصل له خلال فترات معينة
- توفير المزيد من نظم المراقبة والكاميرات الأمنية والأمن لحماية المعلومات داخليا
- يمكن استخدام الانترنيت كمكان لتوفير معلومات عن المؤسسة ووضع ملفات تعريفية عن الرصيد الأرشيفي وعن بعض المعلومات في اطار تسهيل وصول المعلومة للمستفيدين عن بعد مع الحذر من وضع نظام المعلومات على الشبكة .
- على مؤسسة الصندوق الوطني للتقاعد أن تحاول متابعة المعايير الدولية مثل معيار إيزو 27002 في مجال أمن المعلومات واستيفاء أهم المواصفات ونتائج الدراسات

خاتمة:

تعتبر معلومة مؤسسات المعلومات فيها رأس مالها الفكري والمادي وخاصة المعلومات الرسمية والقيمة أو التي تحمل صفة تاريخية مفيدة، لذا لا بد من القيام بخطوة لا يمكن الاستغناء عنها أو التهاون في اعتمادها اي توفير حماية كاملة عبر خطوات و أساليب خاصة بالأمن المعلوماتي الذي يعرف بأنه علم مختص بتأمين المعلومات من المخاطر التي تهدده، باختلاف أنواع الوثائق و البيانات الموجودة فيها نجد الوثائق الأرشيفية بحيث هي أكثر محتويات الأرشيف ومحور رصيده، الذي يمثل الموروث التاريخي للأمم ،ويبدو أن اتباع التطور قد الزم بالضرورة استخدام المعلومات الالكترونية. و قد يشغل ها المجال لدى العديد من المؤسسات، كما منح أمن المعلومات فرصة لمؤسسات الأرشيف في تبني نظم الكترونية والاعتماد على قدرات الحاسوب والتكنولوجيا وقواعد البيانات والبرمجيات في بيئة آمنة،

و هذا ما تم من خلال دراستنا التي تمحورت حول أمن المعلومات على مستوى مصلحة الأرشيف ومدى مساهمته في تحقيق السرية للمعلومات و الوثائق الأرشيفية من خلال ما تم عرضه من تفاصيل مهمة عن المعلومات والبيانات وطرق حمايتها والتهديدات التي تواجهها، و قد توصلنا إلى نقص إمكانيات المادية و الكفاءات البشرية نتج عنه ضعف في المنظومة الأمنية بمصلحة الأرشيف وفق ما جاء به معيار إيزو 27002 لأمن المعلومات بالإضافة إلى عدم كفاية عدد و وعي الموظفين بأهمية أمن المعلومات داخلها سوف يؤثرا سلبا في تحقيق أمن المعلومات على مستواها ،فإنه من ضروري توفير الإمكانيات اللازمة التي بدورها تساهم في توفير ظروف عمل مناسبة تدعم مهام الموظفين، مع الحرص على تطبيق معيار إيزو 27002 لأمن المعلومات كونه يقدم الكثير للمؤسسة في مجال أمن المعلومات و تساعدهم على الأداء الجيد للوظائف و الارتقاء بها، بالإضافة إلى تحسين سبل وقاية المعلومات في كل اشكالها سواء الالكترونية او الورقية وتحسين وضع أمن المعلومات الالكتروني في المؤسسة الصندوق الوطني للتقاعد.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

المصادر

1. القرآن الكريم
2. ابن المنظور. قاموس لسان العرب، دار المعارف ،تونس،1980.

المراجع

الكتب :

3. باييروشون ميرفي، فريد. تر . محمد سعد طنطاوي. علم التشفير. مؤسسة الهنداوي للتعلم والثقافة، 2016.
4. بركات عبد العزيز، مقدمة في التحليل الإحصائي لبحوث الإعلام. الدار المصرية اللبنانية،2017
5. جمال محمد لينا، الجرائم الإلكترونية. دار خالد الحياني للنشر والتوزيع،عمان،2010
6. حسن، أيمن عبد الله فكري. الجرائم المعلوماتية. الرياض: مكتبة الملك فهد،1434
7. خالد ممدوح، إبراهيم. أمن المعلومات الإلكترونية. الإسكندرية : الدار الجامعية، 2008.
8. خالد، محمد خالد. أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الإلكتروني. الإسكندرية: المركز العلمي لتبسيط العلوم للنشر، 2006
9. خولي ،جمال، الوثائق الإدارية بين النظرية والتطبيق، القاهرة، الدار المصرية اللبنانية،1993
10. دشلي، كمال، منهجية البحث العلمي، مديرية الكتب والمطبوعات الجامعية، 2016
11. دليل حفظ الأرشيف، وزارة شؤون الرئاسة، المركز الوطني للوثائق والبحوث. ابو ظبي، الإمارات العربية المتحدة.
12. الدوه حي، صلاح. مقدمة في التشفير. سورية: من منشورات الجامعة الافتراضية السورية، 2018
13. ساري، محمد خالد. اتجاهات في امن المعلومات وامانها. الرياض: العبيكان للنشر، 2017
14. سالم، عبود، الألوسي، مالك محمد محجوب. الأرشيف تاريخه، أصنافه، إدارته. بغداد : الحربة للنشر والطباعة، 1979
15. السيد، محمد إبراهيم. مقدمة في تاريخ الأرشيف ووحداته. القاهرة: دار الثقافة للنشر والتوزيع، 1998
16. الشريف، عبد المحسن. تقييم وثائق الأرشيف: معايير وإجراءات. القاهرة: دار الثقافة العلمية، 2001.
17. شهيدي، أمحمد بن الدين محمد. أمن الشبكات من مخاطر التهديدات الالكترونية ودوره في تعزيز التجارة الالكترونية جامعة أدرار، 2006.
18. ضرضام، جابر عطوش آل مواس. جريمة التجسس المعلوماتي . مصر: المركز العربي للدراسات والبحوث العلمية،2017
19. الطائي، محمد عبد المحسن. إدارة أمن المعلومات. عمان: دار الثقافة للنشر والتوزيع، 2010.
20. طويلة، جميل حسين. البرمجيات الخبيثة، MALWARE سوريا
21. الظاهر، نعيم إبراهيم. طريق نحو الحكومة الإلكترونية. الأردن: عالم الكتب الحديث، 2014. ص 82.
22. العامري، اسامة موسى. اتجاهات إدارة المعلومات. عمان، دار أسامة للنشر والتوزيع،2010.

23. عبد الصادق، عادل. الفضاء الإلكتروني والثورة في شؤون أجهزة الاستخبارات الدولية. القاهرة: مركز الأهرام للدراسات السياسية والاستراتيجية، 2013.
24. عناية، غازي، البحث العلمي، دار المناهج للنشر والتوزيع،عمان،الأردن،2014
25. العنبكي، طه حميد حسن، العقابي نرجس زابر ،أصول البحث العلمي في العلوم السياسية، دار لأمان،الرباط،2015
26. العوادي، أوس مجيد غالب. الأمن المعلوماتي السبيراني. مركز البيان للدراسات والتخطيط،2016
27. غادة، موسى عبد المنعم. أساسيات تكنولوجيا المعلومات والاتصال. مصر :دار المعرفة الجامعة، 2016.
28. الغثبر، خالد بن سليمان، القحطاني، محمد بن عبد الله. أمن المعلومات بلغة ميسرة.، مركز التميز لأمن المعلومات،: الرياض، 2009.
29. الغثبر، خالد بن سليمان، بن هيشة، سليمان بن عبد العزيز. الاصطياد الإلكتروني: الأساليب والإجراءات المضادة. الرياض: مركز التميز لأمن المعلومات، 2009.
30. الغرابي احمد بن عبد الله. الأرشفة الإلكترونية في المملكة العربية السعودية: دراسة لواقع الوزارات والمؤسسات شبه الحكومية،الرياض:2008.
31. فايز جمعة النجار،نظم المعلومات الإدارية منظور إداري:– MANAGEMENT INFORMATION SYSTEMS MANAGERIAL PERSPECTIVE. عمان: دار الحامد للنشر والتوزيع، 2009
32. الفتال، حميد ناصر، صادق، دلال. أمن المعلومات. عمان: دار اليازوري للنشروالتوزيع،2008.
33. فتوح جمعة، صفاء، مسئولية الموظف العام في إطار تطبيق نظام الإدارة الإلكترونية. مصر : دار الفكر والقانون، 2014
34. فيصل محمد عبد الغفار. الحرب الإلكترونية، دار الجنادرية للنشر والتوزيع، عمان. 2016.
35. قبسي، محمد. علم التوثيق في الوطن العربي. بيروت: دار الآفاق الجديدة، 1980.
36. القحطاني، ذيب بن عايض. أمن المعلومات. الرياض : مدينة الملك عبد العزيز للعلوم والتقنية ،2015.
37. الكافي، مصطفى يوسف. الحكومة الإلكترونية في ظل الثروة العلمية التكنولوجية المعاصرة. دمشق: دار ومؤسسة رسلان للنشر، 2009
38. المصري، عبد الصبور عبد القوي علي. التنظيم القانوني للتجارة الالكترونية. الرياض: مكتبة القانون والاقتصاد، 2012.
39. مصطفى أمينة، صادق. إدارة الأزمات والكوارث في المكتبات. القاهرة : الدار المصرية اللبنانية، 2002.

مقالات الدوريات :

40. بجاجة عبد الكريم، المبادئ التوجيهية من الكوارث ومراقبتها، دراسة رقم 11.الإمارات:المجلس الدولي للأرشيف، فبراير 2008.
41. بربار، نور الدين. دور الأمن المعلوماتي في تفعيل نشاط الصيرفة الإلكترونية. مجلة الاقتصاد والتنمية ،ع 02، 2014
42. بودوشة، أحمد. التشريعات ودورها في دعم وتطوير الأرشيف الوطني. مجلة المكتبات والمعلومات. مج 02،ع 03،ديسمبر 2003

43. جوهري عزة فاروق عبد المعبود، طه محمد طه حسن. أمن المعلومات رقمية وسبل حمايته في ظل التشريعات الراهنة .في مجلة المركز العربي للبحوث والدراسات في علوم مكتبات والمعلومات. مج 6،ع 12،يونيو 2019.
44. دخيل، أحمد نوري، سعد، عبد السلام. اختراقات أمن المعلومات وطرق تفاديها. المجلة الدولية المحكمة للعلوم الهندسية وتقنية معلومات. مج 2،ع 2،يونيو 2012
45. ربيعي، حسين. المجرم المعلوماتي –شخصيته وانصافه. مجلة العلوم الانسانية جامعة محمد خيضر بسكرة، ع40، جوان 2015
46. سامية عبد القادر محمد أحمد، سارة شمو شاع الدين. الأرشفة الإلكترونية وواقعها في دار الوثائق بالسودان. المؤتمر الدولي العشرين للاتحاد العربي للمكتبات والمعلومات. ديسمبر 2009. المملكة المغربية: الدار البيضاء..
47. الشريف، أشرف عبد المحسن. أمن وحماية المستندات الالكترونية على بوابة الحكومات العربية. مجلة الاتحاد العربي للمكتبات والمعلومات. ع 16، 2016 .
48. شوابكة، عدنان عواد. دور إجراءات الأمن المعلومات في الحد من مخاطر أمن المعلومات في جامعة الطائف. في: مجلة دراسات وأبحاث، مج 11،ع 04،أكتوبر 2019.
49. عبادة أحمد العربي، المعايير الدولية لسياست أمن المعلومات دراسة تحليلة لمعايير المنظمة الدولية للتوحيد القياسي إيزو 27002 ومدى تطبيقها في الجامعات العربية، مجلة مكتبة الملك فهد الوطنية، مج 19،ع 02 .أكتوبر 2013.
50. العربي، أحمد عبادة. معيار المنظمة الدولية للتوحيد السياسي إيزو 27002 لسياسات أمن المعلومات. مجلة جامعة الطيبة للآداب والعلوم الإنسانية. ع7. سعودية،1436ه
51. عزون زهية، الحفظ الوقائي للوثائق الأرشيفية ،مجلة علم المكتبات،ع06
52. فاروق، عزة عبد المعبود، الجوهري، حسن طه محمد طه. أمن المعلومات الرقمية وسبل حمايتها في ظل التشريعات الراهنة. مجلة المركز العربي للبحوث والدراسات في علوم مكتبات والمعلومات، مج 6 ،ع 12 ،يونيو 2019.
53. قماز، شعيب، صحراوي، عبد العزيز. الحكومة الإلكترونية ومساعي استتباب الأمن المعلوماتي: الإمارات العربية المتحدة نموذجا. مجلة الحقوق والعلوم السياسية. ع 11 جانفي 2019.
54. ليتم، فتيحة. ليتم، نادية. الامن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، ع 12
55. مأمون العزب، أمن المعلومات في فضاءات الانترنت الأشياء، مجلة التقدم العلمي، ع 99. كويت، 2017.
56. مولاي أمحمد؛ ختير فوزية. المتطلبات التقنية للأرصدة الأرشيفية: مشروعات رقمنة الأرشيف الجزائري نموذجا. المؤتمر الدولي العشرين للاتحاد العربي للمكتبات والمعلومات. ديسمبر 2009. المملكة المغربية: الدار البيضاء.
57. نوفيل حديد، كريبط حنان، أمن المعلومات ودورة في مواجهة الاعتداءات الالكترونية على نظام معلومات المؤسسة ،المؤسسة، ع03، 2014، ص 190.

الأدلة و المعايير

58. الوقاية من الكوارث والخطط الاستعجالية، دليل إيفلا 2006.

القوانين والمراسيم :

59. طويلي، محمد. منشور رقم 3 المؤرخ في 02 فبراير 1919 الخاص بتسيير وثائق الأرشيف، مديرية العامة للأرشيف الوطني

المذكرات :

60. أحمد حسني صالح عوض الله. أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعات الأردنية. مذكرة دكتورا، جامعة السودان للعلوم والتكنولوجيا، 2018.
61. آن سعيد، إبراهيم عبد الواحد. سياسات أمن المعلومات وعلاقتها بفعالية نظم المعلومات الإدارية. مذكرة ماجستير، تخصص: إدارة أعمال، جامعة الأزهر. غزة،2015.
62. بحبح فاطمة الزهراء، بن عروس الجوهر، رقمنة أرشيف البنوك: التنمية المحلية(BDL)فرع مستغانم وحدة رقم 834 دراسة حالة، مذكرة لنيل شهادة الماستر في علم المكتبات :تخصص نظم المعلومات وتكنولوجيا الحديثة و. التوثيق. جامعة عبد الحميد بن باديس،مستغانم.2016
63. بغداد، محمد. الأمن المعلوماتي وسبل حمايته في الجزائر. مذكرة ماستر تخصص تسيير وإدارة الجماعات المحلية. جامعة سعيدة،2018.
64. بن دوف أسماء، بوطيبة بن قلاوز عبد الله، التحولات التكنولوجية في إدارة العمليات الأرشيفية: دراسة ميدانية بمصلحة أرشيف ولاية مستغانم، مذكرة لنيل شهادة ماستر في علم المكتبات: تخصص تكنولوجيا وهندسة المعلومات، جامعة عبد الحميد بن باديس،مستغانم.2019.
65. بن ضيف الله، فؤاد. أمن المعلومات ضرورة معرفية أم ترف تكنولوجي. مذكرة دكتورا. جامعة باجي مختار، عنابه
66. بودويرة طاهر؛ تثمين رأس المال البشري في ميدان أرشيف بين التكوين وممارسة المهنة، مذكرة لنيل شهادة الماجستير في علم المكتبات :تخصص نظم المعلومات، جامعة منتوري،قسنطينة.2009.
67. بوربابة، صورية. قواعد الأمن المعلوماتي. مذكرة لنيل شهادة دكتورا في العلوم :تخصص علوم قانونية، الجامعة جيلالي يابس، سيدي بلعباس،2015
68. بوسمغون، إبراهيم. تكنولوجيا المعلومات وتطبيقاتها في مجال الأرشيف: ولاية قسنطينة نموذجا. مذكرة مقدمة لنيل شهادة الماجستير في علم المكتبات.: تخصص: إعلام آلي وتقني. الجامعة منتوري قسنطينة،2009.
69. بوطيبة بن قلاوز عبد الله،بن درف أسماء. التحولات التكنولوجية في إدارة العمليات الأرشيفية :دراسة ميدانية بمصلحة ارشيف ولاية مستغانم،2019.مذكرة ماستر: تخصص تكنولوجيا وهندسة المعلومات .مستغانم.
70. تاقة مليكة، مناجمنت أرشيف التأمينات الاجتماعية لوكالة وهران: إشكالية الإتلاف، مذكرة لنيل شهادة ماجستير في علم المكتبات والعلوم الوثائقية، جامعة ألسانيا،وهران.2012.

71. حافظي، زهير. الأنظمة الآلية ودورها في تنمية الخدمات الأرشيفية: دراسة تطبيقية بأرشيف بلدية قسنطينة. مذكرة دكتورة، جامعة منتوري،قسنطينة،2008
72. درار نسيمة ،الامن المعلوماتي وسبل مواجهة مخاطر في التعامل الإلكتروني دراسة مقارنة، شهادة لنيل دكتورا في قانون الخاص، جامعة أبو بكر بلقايد، تلمسان .2016.
73. دلهوم، انتصار .تسيير الأرشيف في المؤسسات العمومية والإدارات العمومية دراسة ميدانية بولاية سوق أهراس
74. دلهوم، انتصار، تسيير الأرشيف في المؤسسات والإدارات العمومية: دراسة ميدانية بولاية سوق أهراس، مذكرة ماجستير، جامعة منتوري،قسنطينة،2006
75. الدنف. أيمن محمد فارس. واقع إدارة أمن نظم المعلومات في الكليات تقنية بقطاع غزة وسبل تطويرها. ماجستير إدارة الأعمال جامعة الإسلامية غزة، 2013.
76. شاشو، ابراهيم، بن عطية، محمد عدة، واقع الأرشيف في ظل التطورات التكنولوجية الحديثة: مصلحة أرشيف ولاية وهران نموذجا. مذكرة ماستر، تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة ابن باديس،مستغانم2018.2019.
77. طارس، أحمد بن علي عبد الله. رؤية استراتيجية لتحقيق الأمن المعلوماتي في هيئة التحقيق والادعاء العام في المملكة العربية السعودية. مذكرة الماجستير: الدراسات الاستراتيجية .جامعة نايف العربية للعلوم الأمنية،الرياض،2015
78. علي محمود مصطفى خليل، منى غربي محمد إبراهيم. الدور التأثيري لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبة الإلكترونية -دراسة ميدانية، جامعة بنها.
79. قاني مخطارية، دوار فاطمة. حفظ الوثائق الأرشيفية في المصالح الولائية: دراسة ميدانية مصلحة أرشيف ولاية مستغانم نموذجا، 2015.2016.مذكرة ماستر: تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق: مستغانم.
80. القحطاني، منصور بن سعيد. مهددات الأمن المعلوماتي وسبل مواجهتها: دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية المملكة العربية السعودية. رسالة ماجستير :تخصص تسيير وإدارة الجماعات المحلية، جامعة نايف،الرياض،2008.
81. قدايفة، أمينة. استراتيجية أمن المعلومات ،محاضرة: .جامعة أمحمد بوقرة بومرداس، الجزائر
82. لعيدي فاطمة، بن نونة فضيلة، ترتيب وتصنيف ارشيف المؤسسات الاقتصادية أرشيف مؤسسة سوناطراك بمصلحة GP1-Z أرزيو نموذجا، مذكرة لنيل شهادة ماستر في علم المكتبات والمعلومات تخصص نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة عبد الحميد بن باديس ،مستغانم. 2016.
83. محمد خير، عزات كساب، متطلبات نجاح نظام إدارة الوثائق الإلكترونية في الهيئة العامة للتأمين و المعاشات –فلسطين-مذكرة لنيل شهادة الماجستير في إدارة الأعمال ،الجامعة الإسلامية،غزة.2008.
84. مرابطي حسان، الاطلاع على الأرشيف بين التشريع والواقع دراسة ميدانية بأرشيف مديرية الموارد المائية بسكرة، مذكرة لنيل شهادة الماستر: تخصص إدارة المؤسسات الوثائقية والمكتبات. جامعة محمد خيضر،بسكرة.2019.

85. مرابطي، حسان الدين. الإطلاع على الأرشيف بين التشريع والواقع: دراسة ميدانية بأرشيف مديرية الموارد المائية بسكرة. مذكرة، ماستر: تخصص: إدارة مؤسسات وثائقية والمكتبات، جامعة محمد خيضر بسكرة،2019

86. معاذ. أحمد عبد الرزاق. أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة سودان :جامعة أم درمان الإسلامية معهد البحوث والدراسات العالم الإسلامي . أطروحة ماجستير، 2016

87. مقراني، قدور. تقييم مدى مساهمة أمن المعلومات الإلكترونية في الحد من مخاطر نظم المعلومات: دراسة حالة مؤسسة اتصالات الجزائر. ماستر أكاديمي طور الثاني: تدقيق ومراقبة التسيير، جامعة قاصدي مرباح ورقلة الجزائر،2015.

88. مكيلودي، زكية. إسهامات تكنولوجيا المعلومات في أمن الأرشيف: دراسة حالة أرشيف ولاية مستغانم نموذجا، مذكرة ماستر ،تخصص: نظم المعلومات التكنولوجية الحديثة والتوثيق، جامعة عبد الحميد بن باديس مستغانم،2017

89. ينجح، خديجة. قصري، فطيمة. واقع استخدام التسيير الإلكتروني للوثائق في ميدان الأرشيف: دراسة ميدانية لأرشيف وزارة العمل والتشغيل والضمان الاجتماعي. مذكرة ماستر في علم المكتبات .جامعة جيلالي بونعامة خميس مليانة،2016/2015

90. يوسف، خليل يوسف عبد الجبار. مدى فاعلية إجراءات الرقابة في توفير أمن المعلومات الإلكترونية في شركات الصناعية الأردنية. مذكرة ماجستير: محاسبو والتمويل ،جامعة الشرق الأوسط،الأردن،2013.

الوابوغرافيا:

91. Mehideb Sara، Smartphone application in the economic sphère متاح على الرابط: http://www.books.google.dz

92. أبو الشامات غالية، أنواع مناهج البحث، جامعة الجزيرة الخاصة، ص 03.متاح على الرابط: http://www.jude.edu.sy

93. إليو، لودوليني، تر أحمد إبراهيم المهدوي، مبادئ وقضايا علم الأرشيف،بنغازي،2018،ص 142.متاح على الرابط: http://www.books.google.dz ..

94. أمن المعلومات في المؤسسات. في:مجلة تكنولوجيا الاتصالات والمعلومات،2017.متاح على الرابط: http://www.titmag.net.ye

95. إيكان سومية. أدوات البحث العلمي، جامعة حسيبة بن بوعلي، شلف. متاح على الرابط: http://wwwuniv.dz .

96. بالمفلح، فاتن سعيد. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى. السعودية: جامعة الملك عبد العزيز. متاح على الرابط http://www.kau.edu.sa

97. التوعية في أمن المعلومات. مركز التميز لأمن المعلومات. الرياض،2020. متاح على الرابط: http://www.coeia.ksu.edu.sa .

98. جبرا، كمال محمود. التأمين وإدارة المخاطر. القاهرة: الأكاديميون للنشر والتوزيع، 2015. متاح على الرابط: http://www.google.books.dz

99. حربي، خالد بن نواف. أمن والحماية في الانترنت. السعودية، متاح على الرابط : http://www.Mudhesh.netpdf .

100. دسوقي أحمد، فايزة. بصمة اليد والعين والقياسات الحيوية في امن المعلومات، تاريخ الصدور 2010/11/21. متاح على الرابط: http://www.lahaonline.com

101. دهب، علي محمد التشفير وأمن المعلومات. جامعة كردفان، كلية دراسات الحاسوب والإحصاء، سودان، 2016. متاح على الرابط: http://www.kutub.info.pdf

102. الشنيفي، نوف علي. البرامج التجسسية spyware أنواعها وطرق الحماية منها. بوابة كنانة اونلاين،2011،متاح على الرابط : http://www.kenanaonline.com

103. الطيطي، خضر مصباح إسماعيل. أساسيات أمن المعلومات، 2010 .متاح على الرابط: http://www.books.goole.dz

104. عبد الحليم. مبادئ امن المعلومات،أسس،2017/04/14،متاح على الرابط : http://www.aodus.org/t/topi1971.

105. عبد الهادي، محمد فتحي. الاتجاهات الحديثة في المكتبات والمعلومات، ع 18. ،2002. متاح على الرابط: http://www.books.google.dz

106. فتحي، أسامة. فيروسات الحاسب، 2008متاح على الرابط : http://www.download.internet-pdf-ebook.com

107. الليبدي، إبراهيم محمد. تامين المنشآت. مركز الإعلام الأمني. متاح على الرابط: http://www.policemc.gov.bh/msms-store/pdf .

108. محمد مصطفى محمد علي، الأرشيف الإلكتروني، ص 1،متاح على الرابط: http://www.dspace.mahdi.edu.sd

109. مسعودي، عبد الهادي، الأعمال المصرفية الإلكترونية: Electronic Banking،اليازوري،2016، متاح على الرابط: http://www.books.google.dz

110. مهدي محمد جواد محمد أبو عال، مجتمع البحث وعينته. كلية التربية الأساسية، جامعة بابل،2018، متاح على الرابط: www.basiceducation.uobabylom.edu.iq

111. وليام، ستولينج. أساسيات أمن الشبكات تطبيقات ومعايير،2011. ص 108.متاح على الرابط: http://www.books.google.dz

الملاحق

الملحق رقم 01

جامعة الجيلالي بونعامة خميس مليانة

كلية العلوم الإنسانية والاجتماعية

قسم العلوم الإنسانية

تخصص: إدارة المؤسسات الوثائقية والمكتبات

المستوى : الثانية ماستر

استمارة المقابلة

في إطار التحضير لنيل شهادة الماستر في علم المكتبات تخصص إدارة المؤسسات الوثائقية والمكتبات، نرفق هذه الاستمارة لتغطية الجانب التطبيقي للبحث المعنون : **أمن المعلومات بمصلحة أرشيف الصندوق الوطني للتقاعد ولاية تيسمسيلت**

من إعداد :

- عدة فاطمة

إشراف الأستاذة:

بوصحراء سعاد

السنة الجامعية : 2019- 2020

استمارة المقابلة

المحور الأول: الإمكانيات المادية و البشرية لتحقيق أمن المعلومات داخل مصلحة الأرشيف في المؤسسة؟

1- الإمكانيات المادية و البشرية التي توفر الأمن للمعلومات داخل مصلحة الأرشيف

- **الميزانية :**

1. ماهي مصادر تمويل المؤسسة

1- الوزارة الوصية ☐

2- ليس لها تمويل ☐

3- مصادر أخرى ☐

2. هل يتم تخصيص ميزانية خاصة بأمن المعلومات داخل مؤسستكم؟

نعم ☐ ☐

2-1. إذا كانت إجابة بنعم هل هي كافية أم لا في توفير أمن المعلومات داخل مصلحة الأرشيف؟

- **الموارد البشرية:**

3. ما هو عدد الموظفين و مؤهلاتهم ؟

المؤهلات	العدد	طبيعة التوظيف

4. هل عدد الموظفين

كافي ☐ غير كافي ☐

5. هل يمتلك الموظفون تقنيات التعامل مع الأجهزة الإلكترونية الحديثة المعتمدة لديكم ؟

نعم ☐ لا ☐

6. هل لمؤهلات البشرية التي يمتلكها الموظفين كافية لتحقيق الأمن داخل المؤسسة؟

نعم ☐ لا ☐

7. هل يتلقى موظفون دورات تكوينية على أحدث التقنيات المستعملة في أمن المعلومات؟

نعم ☐ ☐

7.1. إذا كانت الإجابة بنعم كيف كان هذا التكوين ؟

1. داخل المؤسسة مع خبير و مختص ☐

2. إرسال الموظفون لتلقي تكوين خارج المؤسسة ☐

3. تكوين أحد الموظفين في مؤسسة المختصة تم يتم تقديم ما تكون عليه لزملائه ☐
4. إرسال الموظفون لتلقي تكوين (تربص) خارج المؤسسة ☐

8. ما هو مستوى التكوين الذي يتحصل عليه الموظف لديكم في المؤسسة؟

1. عالي ☐
2. متوسط ☐
3. منخفض ☐

9. في رأيك هل ترى أن الموظفين يمتلكون وعي كافي بأهمية أمن المعلومات؟

نعم ☐ لا ☐

9.1. إذا كانت الإجابة بنعم من خلال ماذا يتجسد ذلك؟

1. الانضباط و التحلي بسلوكيات المهنة. ☐
2. السير وفق السياسة الأمنية المرسومة من طرف المؤسسة ☐
3. معرفة كيفية التعامل مع المشاكل الامنية. ☐

- **موارد المادية**

10. هل موقع مركز الحاسبات و تصميم الهندسي للبناية مناسبة للحفاظ على أمن المعلومات داخل مصلحة الأرشيف؟

نعم ☐ لا ☐

1.10 إذا كانت الإجابة بلا لماذا؟

.....

.....

11. المؤسسة تحتوي على

وسائل الراحة	متوفرة	غير متوفرة
تهوية		
إنارة		
التدفئة		

12. الأثاث و التجهيزات المتواجدة في مصلحة الأرشيف

الإمكانيات	عددها	كافي	غير كافي
كراسي			
خزائن			
مكاتب الموظفين			
الحاسبات الإلكترونية			
مخزنات الطاقة			
الماسحات الضوئية			
الطابعات			
آلات النسخ			
الكاشفات البيولوجية			
كاميرات المراقبة			
أجهزة التبريد و التهوية			
وسائط الإلكترونية			
أجهزة الإنذار الحرائق			
مطافئ الحرائق اليدوية			

- **الموارد المادية**

13. ما هي طبيعة تكوين الرصيد الوثائقي لديكم في مصلحة الأرشيف ؟

1. تكوين طبيعي كافي ☐
2. عن طريق الدفع ☐
3. حصول علية من مصادر أخرى ☐

14. ما هو نوع ترتيب الرصيد الوثائقي داخل مصلحة الأرشيف ؟

1. حسب المصالح ☐
2. ترتيب زمني ☐
3. ترتيب أبجدي ☐

15. هل الرصيد الوثائقي مرقمن ؟

نعم ☐ لا ☐

1.15 إذا كانت الإجابة بنعم ماهي درجة الرقمنة؟

كلي ☐

جزئي ☐

16. هل تتوفر المؤسسة على شبكة الانترنت؟

نعم ☐ لا ☐

17. هل تتم الحماية على مستوى الأنظمة و البرامج داخل المؤسسة؟

نعم ☐ لا ☐

1.17. إذا كانت الإجابة بنعم كيف تكون الحماية؟

2. كلمات السر و المرور ☐

3. تحديث التلقائي البرامج و الانظمة ☐

4. التخزين و النسخ الاحتياطي ☐

18. ماهي نظم الإنذار التي تساعد في اكتشاف الاخطار المتوقعة داخل مصلحة الأرشيف؟

1. أجهزة الإنذار للبوابات و المنافذ ☐

2. أجهزة إنذار الحريق ☐

3. أجهزة إنذار الخزائن ☐

19. هل تعتمد المؤسسة على كاشفات إلكترونية البيولوجية كوسائل للحماية؟

نعم ☐ لا ☐

1.19. إذا كانت الإجابة بنعم فيما تتمثل:

2. بصمات الأصابع ☐

3. قزحية العين ☐

4. التعرف على الصوت ☐

20. فيما تتمثل وسائط التخزين المستعمل لديكم في مصلحة الأرشيف من أجل حفظ البيانات و المعلومات؟

1. الأقراص الصلبة ☐

2. الأقراص المرنة ☐

3. فلاش ديسك ☐

4. وسائط أخرى ☐

21. على ماذا يتم الاعتماد في الحصول على وسائط التخزين ؟

1. حسب الحاجة ☐
2. سياسة اقتناء و شراء ☐
3. أمر آخر ☐

1.21. إذا كانت هناك سياسة فيما تتمثل هذه السياسة؟

.....

.....

.....

.....

22. ماهي طريقة معالجة وسائط التخزين التي تعتمدونها؟

.....

.....

.....

23. ماهي البرامج و أنظمة التشغيل المعمول بها داخل مصلحة الأرشيف ؟

24. NETWORK ☐

25. SECURITY ONION ☐

26. SURICATA ☐

24. هل تفي هذه البرامج و الأنظمة بغرض توفير أمن المعلومات داخل المؤسسة ؟

نعم ☐ لا ☐

1.24. إذا كانت الإجابة بلا لماذا؟

.....

.....

25. هل هناك حماية للأنظمة و البرامج داخل مصلحة الأرشيف ؟

نعم ☐ لا ☐

1.25. إذا كانت الإجابة بنعم كيف تكون الحماية؟

1. كلمات السر و المرور ☐
2. تحديث التلقائي البرامج و الانظمة ☐
3. التخزين و النسخ الاحتياطي ☐

26. كيف تتم حماية المعلومات على مستوى الأنظمة و البرامج داخل مصلحة الأرشيف لمؤسستكم؟

1. تحديد الأشخاص المصرح لهم بالاطلاع على المعلومات ☐
2. إجراء الرقابة الداخلية على جميع الإجراءات المطبقة داخل المؤسسة ☐
3. اختيار كلمات المرور و تحديثها دوريا ☐

27. هل الإمكانيات متاحة (مادية، مالية، تقنية) الموظفين لتأدية أعمالهم داخل المؤسسة؟

كافية ☐ غير كافية ☐

1-14. إذا كانت غير كافية فيما يكمن هذا النقص؟

.....

.....

المحور الثاني: معايير امن المعلومات المتبعة داخل مصلحة الأرشيف

28. رتب حسب الأولوية مكونات أمن المعلومات التي تتوفر عليها مصلحة الأرشيف؟

1. أمن الأفراد و الإدارة ☐
2. أمن الوثائق في مركز الحاسبات ☐
3. أمن أنظمة التشغيل و البرمجيات ☐
4. أمن أجهزة الحاسبات إلكترونية ☐

29. هل تعتمد المؤسسة على معايير عالمية و دولية لأمن المعلومات ؟

نعم ☐ لا ☐

1.29. إذا كانت الإجابة بنعم فيما تتمثل هذه المعايير المتبعة من طرفكم؟

2. معيار إيزو 27002 ☐
3. معيار COBIT 5 ☐
4. معيار ITIL ☐
5. معيار آخر ☐

2.29. إذا كانت الإجابة بلا فكيف يتم تسير المؤسسة ؟

1. وجود قانون داخلي للمؤسسة لأمن المعلومات ☐
2. سياسة وطنية متبعة في أمن المعلومات ☐
3. دساتير و تشريعات وطنية لأمن المعلومات ☐
4. معايير خاصة بكم

30. هل المعايير المعتمدة حاليا من طرف مؤسستكم تلبي الحالة في توفير الأمن المعلومات؟

1. ضمان سرية والحماية المعلومات ☐
2. سهولة حفظها و حمايتها ☐
3. سهولة و السرعة في المعالجة ☐

31. هل حققت هذه المعايير الأمن اللازم للمعلومات في مصلحة الأرشيف ؟

نعم ☐

لا ☐

نوعا ما ☐

32. رأيك هل غياب المعايير العالمية يؤثر في تحقيق الأمن المناسب للمعلومات داخل مصلحة الأرشيف؟

نعم ☐ لا ☐

إذا كانت الإجابة بنعم في ماذا يؤثر هذا الغياب؟

.....

.....

33. في رأيك ما الذي سوف تضيفه هذه المعايير في حال اعتمادها داخل مؤسستكم ؟

.....

المحور الثاني :مهددات و معيقات أمن المعلومات و طرق الحماية منها داخل المؤسسة

34. ما نوع المخاطر و التهديدات التي تتعرض لها المعلومات داخل مصلحة الأرشيف؟

1. مخاطر مادية ☐
2. مخاطر بشرية ☐
3. تهديدات إلكترونية ☐
4. مخاطر تقنية و فنية ☐

35. كم تقدر نسبة الخسائر التي تسببها تلك التهديدات لأمن المعلومات؟

1. عالية ☐
2. متوسطة ☐
1. منخفضة ☐

36. هل تم في يوم من الأيام قرصنة النظام داخل المؤسسة؟

نعم ☐ لا ☐

1.36. إذا كانت الإجابة بنعم من طرف من كانت القرصنة؟ و ماهي دوافعهم؟

الهاكر ☐ الكراكرز ☐

37. دوافع المقرصنون في اختراق الانظمة؟

1. العبث و اللهو ☐
2. انتقام ☐
3. الربح المادي ☐

38. ماهي الإجراءات المتبعة مواجهة هذه القرصنة؟

.....

.....

39. هل تعرضت الأجهزة الإلكترونية للاختراق في يوم ما في مؤسستكم؟

نعم ☐ لا ☐

1.39. إذا كانت الإجابة بنعم ما هو نوع الاختراق التي تعرضت له؟

1- اختراق الخادم ☐
2- اختراق الأجهزة الرئيسية ☐
3- اختراق البيانات ☐

40. ماهي الطرق و الإجراءات المعتمدة من طرف مؤسستكم في مواجهة هذا الإختراق؟

.....

.....

41. هل تعرضت الأنظمة و البرامج لديكم لخطر الفيروسات في يوم من الأيام؟

نعم ☐ لا ☐

1.41 إذا كانت الإجابة بنعم ماهي أشهر انواع هذه الفيروسات؟

1. حصان طروادة ☐
2. الدودة ☐
3. برامج الإنزال ☐

42. فيما تتمثل الإجراءات الوقائية لمواجهة خطر الفيروسات داخل مصلحة الأرشيف ؟

1. برامج مكافحة الفيروسات ☐
2. إجراء الفحص على البرامج المحملة أو المنزلة من الانترنت ☐
3. احتفاظ بنسخة من البرامج و الملفات الموجودة على الحاسب ☐

43. ماهي أساليب مواجهة تهديدات أمن المعلومات أكثر استخداما داخل مصلحة الأرشيف ؟

1. تحليل المخاطر الناتجة عن الانتهاك ☐
2. تحديد مستوى الحالي لظهور مخاطر الانتهاك ☐
3. تحديد العقبات التي تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية ☐

44. ماهي طرق المتبعة للحماية الأمنية للمعلومات من أجل تحقيق الأمن المعلوماتي في مصلحة الأرشيف ؟

1. الجدار الناري ☐
2. التشفير ☐
3. برامج مكافحة الفيروسات ☐
4. نظم المراقبة و الكاميرات الإلكترونية ☐

45. هل توجد إجراءات الحماية لأمن المعلومات عبر الشبكة في المؤسسة؟

نعم ☐ لا ☐

إذا كانت الإجابة بنعم ماهي هذه الإجراءات؟

1. عنونة الشبكات بوضع عناوين لجميع الأجهزة المرتبطة بالشبكة ☐
2. متابعة جميع محاولات الدخول إلى النظام ☐
3. اتخاذ إجراءات مراجعة الشبكة بعد تشغيلها ☐
4. إشراف على الشبكة من قبل فنيين مختصين ☐

46. ماهي الإجراءات المتخذة لحماية أمن المعلومات من خطر الأشخاص غير مخول لهم من الوصول إلى المعلومات؟

1. استعمال هوية ممغنطة ☐
2. توقيع الإلكتروني ☐
3. بصمة اليد ☐

47. ماهي اقتراحاتكم حول الضروريات اللازمة التي من شانها و تحسين توفير أمن المعلومات داخل المؤسسة؟

.....

.....

.....

48. فيما تتمثل آليات المستعملة في تعزيز أمن المعلومات لديكم؟

1. الاستراتيجية الأمنية لأمن المعلومات ☐
2. التشريع و القانون ☐
3. العاملون ☐
4. تطبيق المعايير الدولية الخاصة بأمن المعلومات ☐

الملحق رقم 01

FICHE TECHNIQUE

AVANTAGE	IDENTIFICATION	OBSERVATION
1	**PENSION DE RETRAITE (RETRAITE À 60 ANS)**	
W	**RETRAITE PROPORTIONNELLE**	
Z	**RETRAITE SANS CONDITION D'AGE**	
3	**PENSION DE REVERSION**	
L	**ORPHELIN(E) MINEUR. (DROIT DIRECTE)**	
H	**ORPHELIN(E). HAND (DROIT DIRECTE)**	
P	**PENSION A.S.C PÈRE (DROIT DIRECTE)**	
M	**PENSION A.S.C MÈRE (DROIT DIRECTE)**	
7	**ALLOCATION DE RETRAITE**	
F	**REVERSION ALLOCATION DE RETRAITE**	
K	**ORPHELIN(E) MINEUR. (ALLOCATION DE RETRAITE)**	
D	**ORPHELIN(E).HAND (ALLOCATION DE RETRAITE)**	
R	**PENSION A.S.C PÈRE (ALLOCATION DE RETRAITE)**	
S	**PENSION A.S.C MÈRE (ALLOCATION DE RETRAITE)**	
E	**REVERSION ALLOCATION PENSION INV**	

وثيقة تمثل طريقة العمل في نظم التقاعد

الملحق رقم 02

سعة تخزين في الرفوف المدمجة المتحركة

الملحق رقم 03

المركز الجهوي للأرشيف بعين تموشنت

الملحق رقم 04

Centrale Sécurité Contre Incendie et Hygiène

:C N°: 98 A 211 1422
IIF N°: 162 0640 0005 7144
:OMPTE BDL N°: 00500466 400 2277 64 011 - TIARET
:ODE NIS: 1962 0640 00057 41
ldresse: Rue KAIDI Ahmed route d'Alger - TIARET
V° de Tél. Portable: 0771 31 12 38

TIARET, le: 05/11/2017

Facture N°049/2017

DOIT: C.N.R - Tissemsilt

N°	Quantité	Désignation	Prix Unitaire	Montant
		RECHARGE		
01	01	Dératisation (Klyrat)	8 500,00	8 500,00
02	01	Désinfection (Lactilique)	8 000,00	8 000,00
			TOTAL HT	16 500,00
			TVA 19%	3 135,00
			TOTAL TTC	19 635,00

Arrêtée la présente facture à la somme de :
Dix Neuf Mille Six Cent Trente Cinq Dinars Algériens.

Le Fournisseur

C.S.C.I.H
Ets. RACHID TAZDAIT
Rue Hamdani Aâda - TIARET
Rc :98 A 2111422

فاتورة الشركة المكلفة بعملية التطهير

الملحق رقم 05

Lois et décrets :

- Loi n°83-12 du 2 juillet 1983 relative à la retraie
- Décret n°85-31 du 09 février 1985 fixant les modalités d'application du titre II de la loi n°83-12 du 2 juillet 1983 relative à la retraite
- Décret n°85-32 du 9 février 1985 relatif à la validation, au titre de la retraite, de certaines périodes de travail accomplies avant le 1 er janvier 1985
- Décret exécutif n°90-215 du 14 juillet 1990 portant intégration d'un élément de rémunération dans l'assiette de calcul de la pension retraite
- Décret exécutif n°90-364 du 10 novembre 1990 portant intégration de l'indemnité spécifique globale servie à certains personnels de l'enseignement supérieur dans l'assiette de calcul de la pension de retraite
- Décret exécutif n°90-395 du 1 er décembre 1990 portant extension à certaines catégories de personnels de la recherche des dispositions du décret exécutif n° 90-364 du 10 novembre 1990 portant intégration de l'indemnité globale servie à certains personnels de l'enseignement supérieur dans l'assiette de calcul de la pension de retraite et du décret exécutif n° 90-365 du 10 novembre 1990 fixant les conditions d'indemnisation des productions scientifiques et pédagogiques des enseignants relevant du ministère aux universités
- Loi n°91-01 du 08 janvier 1991 relative à la retraite des veuves de chouhada
- Décret législatif n° 94-05 du 11 avril 1994 modifiant la loi n°83-12 du

2 juillet 1983 relative à la retraite

Décret législatif n° 94-10 du 26 mai 1994 instituant la retraite anticipée

Ordonnance n°96-18 du 06 juillet 1996 modifiant et complétant la loi n°83-12 du 2 juillet 1983 relative à la retraite

Décret exécutif n°96-310 du 18 septembre 1996 complétant le décret n°85-31 du 9 février 1985 fixant les modalités d'application du titre II de la loi n°83-12 du 2 juillet 1983 relative à la retraite

Ordonnance n°97-13 du 31 mai 1997, modifiant et complétant la loi n° 83-12 du 2 juillet 1983 relative à la retraite

Arrêté du 16 avril 1997 portant organisation interne de la caisse nationale des retraites (CNR)

Décret présidentiel n°98-333 du 20 octobre 1998 portant modalités de validation, au titre du droit à la pension de retraite, des années de service accomplies par les hommes de troupe contractuels au sein de l'armée nationale populaire

Loi n°99-03 du 22 mars 1999 modifiant et complétant la loi n°83-12 du 2 juillet 1983 relative à la retraite

Loi n°83-11 du 2 juillet 1983 relative aux assurances sociales

Ordonnance n° 96-17 du 6 juillet 1996 modifiant et complétant la loi n° 83-11 du 2 juillet 1983 relative aux assurances sociales

Loi n° 83-15 du 2 juillet 1983 relative au contentieux en matière de sécurité sociale

Décret n° 85-33 du 9 février 1985 fixant la liste des travailleurs assimilés à des salariés en matière de sécurité sociale

Décret exécutif n° 92-07 du 4 janvier 1992 portant statut juridique des caisses se sécurité sociale et organisation administrative et

financière de la sécurité sociale

Ordonnance n° 95-01 du 21 janvier 1995 fixant l'assiette des cotisations et des prestations de sécurité sociale

Décret exécutif n° 96-208 du 5 juin 1996 fixant les modalités d'application des dispositions de l'article 1 er de l'ordonnance 95-01 du 21 janvier 1995 fixant l'assiette des cotisations et de prestations de sécurité sociale

Loi n° 99-10 du 11 novembre 1999 modifiant et complétant la loi n° 83-15 du 2 juillet 183 relative au contentieux en matière de sécurité sociale

Arrêté du 11 mai 1997 fixant les règles et les modalités de coordination des régimes de sécurité sociale des salariés et des non-salariés

الملحق رقم 06

الوسائل المستعملة في عملية الرقمنة