جـــامـعـــة مـــولـــود مـعـمـــري- تيـــزي وزو
كليـــة الحقـــوق والعلـــوم السياسيـــة
قســم العلوم السياسية

مذكرة مقدمة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية

نظام أمن المعلومات في الجزائر
دراسة حالة بلدية سوق الإثنين ولاية تيزي وزو
(2017 -2014)

تخصص: سياسات عامة و إدارة محلية

من إعداد الطالبة:
- حمودي كاهنة

تحت إشراف الأستاذة:
– إعباسن زاهية.

أعضاء لجنة المناقشة

- حمداني لوناس.....رئيسا
- إعباسن زاهية.....مشرفا ومقررا
- حاكم فضيلة.....ممتحنا

السنة الجامعية: 2016/

مقدمة

لقد أحدث العالم الالكتروني موجة من التطورات والتغيرات التي مست مجالات العمل، حيث أصبح انتقال المعلومات عبر الشبكة الالكترونية علامة وميزة تحرص على تلبية متطلبات الحياة العملية بالنسبة للإدارة العامة والتقليل من تراكم الأعمال، فانتشار أنظمة المعلومات المحوسبة واعتماد هذه الأخيرة أساسا على قواعد تكنولوجية بدءا بعملية الإدخال وصولا إلى المخرجات ما أدى إلى بروز ظاهرة الاختراق التي دفعت بالمنظمة إلى اقتناء أساليب الحماية لها.

إن نظام أمن المعلومات يعتبر الركيزة الأساسية لسلامة الأعمال، فهي عبارة عن مجموعة من الإجراءات والتدابير الوقائية التي تستخدم لغرض الحماية من الجرائم الالكترونية ومن مهددات استخدام تقنية المعلومات والتي قد تؤثر سلبا على سرية وسلامة المعلومات وتوفرها في الوقت المناسب، لذا قامت العديد من الدول ببذل الجهود اللازمة سواء كان ذلك على المستوى الوطني أو الدولي بوضع قوانين تحول بإدراك هذا الخطر وإعطاء أهمية كبيرة لنظام أمن المعلومات واعتباره من أهم الآليات التي تتيح للمنظمة تنفيذ أعمالها ونشاطاتها بكفاءة وفعالية دائمة وذلك بانتهاج السياسة الأمنية التي تحد من انتشار مثل هذه المخاطر كون هذه الأخيرة لا تكتمل إلا إذا تعاون جميع أعضاء المؤسسة بغية تحقيق التطور والاستمرارية.

وعليه فإن موضوع نظام أمن المعلومات يلعب دورا مهما في حماية الموارد الأساسية للمؤسسة، كما يساهم في توفير الحماية الكافية للمعلومات وسلامتها.

1- أهداف الدراسة:

نسعى من خلال هذا البحث إلى تحقيق مجموعة من الأهداف الأساسية والتي يمكن أن نشير إليها فيما يلي:

- الإحاطة بمختلف المفاهيم المرتبطة بنظام أمن المعلومات.
- التعرف على أنواع المخاطر والمهددات التي تصيب نظام أمن المعلومات.
- الإشارة إلى السياسة الأمنية المتبعة للحد من المخاطر المرتقبة لنظام أمن المعلومات.
- مدى كفاءة الإجراءات الأمنية في الإدارة العامة.
- محاولة إظهار العلاقة بين نظم المعلومات وأمن المعلومات من خلال توضيح دور أمن المعلومات في تجسيد نظم المعلومات.

2- أهمية الدراسة:

تكمن أهمية الموضوع في اعتماد المنظمات على التكنولوجيا في تسيير أعمالها وكذا إظهار المفاهيم الحديثة التي ترتبط بموضوع نظام أمن المعلومات لدعم و تطوير الأعمال الإدارية لهذه المنظمات و التحقق من أنواع الجرائم للتعرف على عناصر بناء السياسة الأمنية و تقديم الإجراءات اللازمة و المعتمدة في الشبكة لتوضيح نقاط الضعف و القوة للوصول إلى نتائج سليمة، حيث يعد نظام أمن المعلومات من أهم التقنيات الحديثة للتسيير في المؤسسة فقد تم تشريع مجموعة من القوانين التي تضمن سلامة النظام.

3- مبررات اختيار الموضوع:

يكمن سبب اختيار الموضوع لدوافع ذاتية ودوافع موضوعية.

أ- المبررات الذاتية:

- الميول الشخصي لمثل هذه المواضيع والرغبة في التعرف على حيثيات استخدامه.
- الرغبة في التعرف على جل المشاكل التي تتعرض لها أنظمة أمن المعلومات .
- معرفة مختلف التشريعات والقوانين التي تعالج هذا الموضوع و طريقة معالجته.

ب- المبررات الموضوعية:

- تقييم مدى كفاءة وفعالية نظام امن المعلومات في المنظمة.
- توضيح حاجة المنظمة إلى الحماية لنظام معلوماتها لضمان الاستمرارية.
- التحسيس بضرورة تطبيق السياسة الأمنية لمختلف وسائل المعلومات.

4- أدبيات الدراسة:

إن أساس بناء هذه الدراسة يعود إلى نتائج الدراسات النظرية والميدانية السابقة والتي عكست أراء الباحثين والمؤسسات التي تطرقت إلى مثل هذا الموضوع، لذا قمنا بدراسة تحليلية لمجموعة من الدراسات ذات الصلة بالبحث وهي:

- الدراسة الأولى:

دراسة عماني عياري تحت عنوان "تدقيق أمن نظام المعلومات الخاص بقسم تكنولوجيا المعلومات والاتصالات"، مذكرة ماستر في التكنولوجيا الحديثة والاتصالات والشبكة، جامعة تونس، 2014.

هدفت هذه الدراسة إلى تقييم نظام المعلومات الخاص بقسم تكنولوجيا المعلومات والاتصال، وتحديد الانحرافات استنادا إلى المعيار الدولي ايزو 27002، حيث اعتمد

الباحث على المنهج التحليلي الوصفي أما من الناحية التطبيقية اعتمد على المقابلات وجمع المعلومات من وثائق المؤسسة بالإضافة إلى الملاحظة، ومن أهم النتائج المتوصل إليها هي أن الأمن هو 75% من المهارات الشخصية والمعرفة، و25 % تكون من المواد ولتحقيق أهداف أمنها تعتمد المؤسسة في المقام الأول على العنصر البشري وثقافة المنظمة.

- الدراسة الثانية:

دراسة عبد الله بن محمد ناصر السحيباني بعنوان "كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات"، رسالة ماجستير، كلية العلوم الأمنية، جامعة نايف بالرياض، عام 1996.

تناولت هذه الدراسة الإجراءات الإدارية المتعلقة بأمن المعلومات في المصارف من عدة زوايا، وإجراءات حماية النظام بعد انتهاء الدوام الرسمي، إضافة إلى الإجراءات المتخذة مع الموظف بعد إنهاء خدماته، وتناولت أيضا تصميم برامج شبكة الاتصال والبرامج التطبيقية كما أشار إلى أهمية وجود نظام أمني في المصرف ضد التسلل والسرقة والتخريب، ومن خلال نتائج دراسته أوصى السحيباني بـ:

- ضرورة إصدار سياسات لأمن المعلومات.
- وجوب توظيف مختصين في مجال امن المعلومات.
- اتخاذ إجراءات تأديبية صارمة بحق مسربي المعلومات في النطاق الداخلي للمصارف.

_ الدراسة الثالثة:

دراسة الهادي محمد محمد (2006)، تحت عنوان "أمن المعلومات في ظل الحكومة الالكترونية".

تناولت الدراسة خدمات نظم المعلومات في البيئة الرقمية وأمن المعلومات حيث ناقش فيها متطلبات الأمن الطبيعي لنظم المعلومات وأهم الأبعاد والمكونات الأساسية المتعلقة

بأمن المعلومات، حيث أوصت الدراسة إلى إقامة سياسة تنظيمية وقانونية لمواجهة مخاطر أمن المعلومات وكذا حماية المواطن وتوعيته بضرورة وأهمية أمن المعلومات في البيئة الرقمية، وتعزيز المبادرات التي تضمن التوازن العادل بين حقوق الملكية الفكرية ومصالح مستخدمي المعلومات في مجال البرمجيات وتخصيص عقوبات إدارية وجنائية حول سوء الاستخدام وتعمد الضرر، إضافة إلى ضرورة إصدار قوانين التي تحدد صحة العقود والوثائق المنشأة من قبل نظم المعلومات.

أهم ما يميز الدراسة الحالية عن الدراسات السابقة:

لقد جاءت دراستنا على نفس منهج الدراسات السابقة من حيث التطرق إلى كافة المصطلحات المتعلقة بنظم أمن المعلومات كما بينت المشاكل و المخاطر التي تتعرض لها الأنظمة من اختراق و تزوير للمعطيات و البيانات الالكترونية إضافة إلى السياسات الأمنية المتبعة من قبل المنظمات إذ تختلف هذه الدراسة عن سابقتها من حيث الدراسة الميدانية التي تم اعتمادها حيث تناولنا فيها واقع نظام أمن المعلومات في الإدارة المحلية و إظهار المعوقات التي تواجهها عند القيام بالمهام الإدارية.

5- مشكلة الدراسة:

إن أهم المشاكل التي تواجه نظام أمن المعلومات في الإدارة العامة يرجع إلى التعامل مع المعطيات الجديدة التي مست برامج نظم المعلومات، وأن مواكبة التكنولوجيا لا يتم إلا باستخدام وسائل الإعلام والاتصال الحديثة وضرورة القيام بتدريب المستخدمين وتحسين أدائهم والرفع من كفاءتهم، مع ضرورة الحد من انتشار مخاطر نظام المعلومات المحتملة حدوثها، لذا سنقوم بطرح التساؤل التالي:

ما مدى مساهمة نظام أمن المعلومات في مواجهة مخاطر نظام المعلومات في الجزائر بصفة عامة و في بلدية سوق الاثنين بولاية تيزي وزو بصفة خاصة؟

وللإجابة على هذه الإشكالية لابد من طرح التساؤلات التالية:

- ما هي المخاطر التي تواجه نظام المعلومات؟
- ما هي الإستراتيجية الأمنية المنتهجة للحد من انتشار هذه المخاطر؟
- ما هي السياسة الأمنية التي تعتمدها الإدارة العامة؟
- فيما تتمثل أهم القوانين والجهود الدولية والجزائرية في مجال نظام أمن المعلومات؟
- ماهو واقع نظام أمن المعلومات في بلدية سوق الاثنين ولاية تيزي وزو؟

6- الفرضيات:

يعتمد كل بحث على تقديم بعض الفروض التي تعتبر مؤشر يستدل به الباحث من خلال التحكم بسياق الدراسة، وانطلاقا من موضوع نظام أمن المعلومات وإبراز مهددات نظام المعلومات سنحاول تطرح فرضية رئيسية مفادها إبراز العلاقة التي تربط بين نظام أمن المعلومات ونظام المعلومات.

من خلال اعتمادنا على الإشكالية المطروحة وبغية الإجابة على التساؤلات بشكل تسلسلي ارتأينا إلى طرح الفرضية التالية:

كلما تعددت مخاطر نظم المعلومات كلما زادت الحاجة إلى انتهاج سياسة أمنية فعالة.

ومن خلال هذه الفرضية سنقوم بصياغة فرضيات ثانوية ونلخصها كالتالي:

- يساهم نظام أمن المعلومات في التقليل من مخاطر نظام المعلومات.
- يتميز نظام أمن المعلومات بالحداثة لاحتوائه على مكونات متطورة وفعالة.
- يشمل تطبيق نظام أمن المعلومات على تقييم أمن المعلومات وإدارة المخاطر المتعلقة بنظام المعلومات.
- تسمح السياسة الأمنية بزيادة الأداء لدى موظفي بلدية سوق الاثنين بولاية تيزي وزو.

7- حدود الدراسة:

تتقيد الدراسة بحدود زمنية ومكانية وهي كالتالي:

- الحدود المكانية: تم إجراء دراسة الحالة في بلدية سوق الاثنين بولاية تيزي وزو.
- الحدود الزمنية: تمت هذه الدراسة في الفترة الممتدة من 2014 إلى 2017 وتتزامن هذه الفترة مع مبدأ تطبيق نظام أمن المعلومات على مستوى البلديات.

8- المناهج الدراسة:

لقد تم الاعتماد في هذه الدراسة على مجموعة من المناهج والاقترابات بهدف دراسة المشكلة المطروحة وكذا بغية إتمام البحث بأسلوب علمي.

أ- المناهج:

يقوم المنهج على إعطاء صورة واضحة للموضوع وإظهار نتائج الدراسة العلمية والتي تخدم مسار المشكلة ووضوحها.

1- المنهج الوصفي: يقوم هذا المنهج على جمع الحقائق والمعلومات ومقارنتها وتحليلها وتفسيرها للوصول إلى تعميمات مقبولة أي دراسة الظاهرة من خلال تحديد خصائصها وأبعادها بهدف الحصول على وصف علمي متكامل و دقيق[1].

[1]- محمد شلبي، **منهجية في التحليل السياسي، المفاهيم، مناهج، اقترابات، الأدوات** (الجزائر: كلية العلوم السياسية والعلاقات الدولية، 1997)، ص 28.

وقد تم استخدامه في وصف وتحليل كل من متغيري الدراسة، نظام أمن المعلومات وأمن المعلومات وتشخيص وضع نظام أمن المعلومات في الإدارة المحلية.

2- منهج دراسة الحالة: هو المنهج الذي يقوم بجمع البيانات العلمية المتعلقة بأي وحدة سواء كانت فردا أو مؤسسة أو نظاما اجتماعيا أو مجتمعا محليا أو عاما، ويقوم أساسا في التعمق في دراسة مرحلة معينة قصد الوصول إلى تعميمات علمية متعلقة بالوحدة المدروسة.
وقد اعتمدنا هذا المنهج في الجانب التطبيقي وقمنا بإسقاطه على بلدية سوق الاثنين بولاية تيزي وزو من خلال التعمق في موضوع الدراسة والتعرف على واقع نظام أمن المعلومات فيها.

ب- الاقترابات:

ومن بين الاقترابات التي تم استخدامها في تحليل هذه الدراسة نجد:

1- الاقتراب القانوني:

يركز هذا المنهج في دراسته على الأحداث والمواقف والعلاقات المبنية على الجوانب القانونية أي مدى التزام تلك الظواهر بالمعايير والضوابط المتعارف عليها والقواعد المدونة وغير مدونة، فهو يهتم بشرعية وعدم شرعية الفعل كما يهتم بالأفعال والجزاءات.

قمنا بإدراج هذا الاقتراب في دراستنا نظرا لاعتمادنا على قوانين تساهم في تكملة ومعالجة موضوع الدراسة وتسهل لنا إبراز آليات وإجراءات التحكم به[1].

2- الاقتراب الاتصالي: هو عملية نقل وتبادل المعلومات بين طرفين أو أكثر أو بين مجموعة إشارات ورموز تبعث من طرف لآخر فهذه العملية بمثابة شريان الحياة للنظام السياسي[2].

تم استخدام هذا الاقتراب في دراستنا لتوضيح الطرق والأساليب المستخدمة للتواصل وتبادل المعلومات بين المرسل و المستقبل

ج)- أدوات جمع البيانات:

تتمثل أدوات جمع البيانات في:

1- المقابلة: تعرف المقابلة على أنها محادثة تتم بين شخصين بهدف الحصول على أنواع المعلومات للاستعانة بها في هذا البحث.
بهدف الحصول على معلومات ذات مصداقية وموثوق بها قمنا بزيارة ميدان الدراسة عدة مرات لنتمكن من جمع المعلومات والمعطيات التي تساعدنا في إتمام هذه الدراسة حيث تمحورت المقابلة مع الأمين العام للبلدية والمكلفة بالإعلام الآلي لتقديم استفسارات حول واقع نظام أمن المعلومات بالبلدية[3].

2- الملاحظة:

---

[1]- محمد شلبي، نفس المرجع السابق، ص 30.
[2]- المرجع نفسه، ص 34.
[3]- عقيل حسين عقيل، **فلسفة مناهج البحث العلمي** (مكتبة مدبولي، 1999)، ص 162.

تعد الملاحظة من الأساليب القديمة لجمع المعلومات فهي عملية تقوم على المراقبة والمشاهدة لسلوك الظواهر المحيطة بنا والمشكلات والأحداث والمكونات المادية والبيئية لمتابعة سيرها واتجاهها وكذا علاقتها بأسلوب علمي منظم ومخطط هادف قصد تفسير وتحديد العلاقة بين المتغيرات[1].

حيث استخدمت الملاحظة في مصالح البلدية لمتابعة طريقة سير العمل داخل الإدارة والعمل الذي تقوم به مهندسة الإعلام الآلي في تنفيذ السياسة الأمنية الخاصة بالبلدية.

9- تحديد المصطلحات:

تستخدم الدراسة مفاهيم ومصطلحات علمية تعطى طابع الموضوعية التي تؤدى إلى الوصول لنتائج ذات مصداقية، وتتمثل هذه المفاهيم في:

- الشبكة المحلية: هي عبارة عن مجموعة من الحاسبات تربط فيما بينها وتوضع على مساحة جغرافية محدودة كمبنى واحد أو مجموعة من المباني قريبة من بعضها البعض[2].

- التخزين: هي قدرة الحاسب على تخزين أكبر عدد ممكن من البيانات والمعلومات والبرامج داخل ذاكرته وتكون بصورة دائمة أو مؤقتة[3].

- البرمجيات: هي مجموعة من القواعد والأوامر (التعليمات) المعدة من قبل الإنسان والتي توجه المكونات المادية للحاسوب بهدف أداء مهمة معينة وتكون وفق تعليمات دقيقة للحصول على نتائج مطلوبة[4].

- جدار ناري: هو مجموعة الأنظمة التي تعمل على تقوية السيطرة للوصول عند استخدامه كجدار ما بين اثنين من شبكات العمل، حيث يستخدم لوضع حدود ما بين الانترنيت الداخلي الخاص بالمؤسسة مع الانترنيت[5].

- الفيروسات: هو برنامج صغير له القدرة على العمل في الخفاء والتكاثر، حيث يعرف على أنه برنامج ينفذ وينسخ نفسه دون معرفة المستخدم[6].

10- تقسيم الدراسة:

من أجل معالجة مضامين وحيثيات هذا الموضوع ضمن الإشكالية السابقة من خلال الوقوف عند مختلف عناصر نظام أمن المعلومات وتوضيح الدور الهام الذي يلعبه في معالجة مخاطر نظم المعلومات قمنا بتقسيم هذا البحث إلى ثلاث فصول وهي:

---

[1]- رحيم يونس، كرو العزاوي، **منهج البحث العلمي** (عمان: دار دجلة، 2007)، ص 150.

[2]- زكرياء أحمد عمار،"حماية الشبكات الرئيسية من الاختراق والبرامج الضارة"، رسالة ماجستير(جامعة النيلين:كلية الدراسات العليا،2011)، ص11.

[3]- نادية لونيس، **أثر التكنولوجيا المعلومات والاتصالات في تفعيل الأعمال التجارية للمؤسسات** (جامعة الجزائر: كلية العلوم الاقتصادية والتجارية، 2011)، ص33.

[4]- نادية لونيس، **المرجع السابق**، ص38.

[5]- سيد أحمد معطي، **واقع وتأثير التكنولوجية الجديدة للإعلام والاتصال على أنظمة البنوك الجزائرية**، رسالة ماجستير (جامعة تلمسان: كلية العلوم الاقتصادية والتجارية، 2012)، ص 102.

[6]- زكريا أحمد عمار، **نفس المرجع السابق**، ص14.

- الفصل الأول: جاء هذا الفصل بعنوان الإطار المفاهيمي لنظام أمن المعلومات حيث تتطرق إلى عدة عناصر خاصة به، إذ يبين ماهية نظام المعلومات وماهية أمن المعلومات وأهم المخاطر التي تهدد نظم المعلومات.
- الفصل الثاني: يتمحور مضمونه في الجهود الدولية والجزائرية في مجال أمن المعلومات وأهم التشريعات التي تعالج هذا الموضوع.
- الفصل الثالث: أما في هذا الفصل فقد تم فيه دراسة واقع نظام أمن المعلومات في الإدارة العامة بحيث ركز في البداية على التعريف بميدان الدراسة ومن ثم تطرق إلى أهم المعوقات التي تواجه نظام أمن المعلومات وفي النهاية قمنا بطرح الحلول التي تتماشى مع الموضوع وتوضيح كيفية معالجة تلك المعوقات.

11- صعوبة الدراسة:

نجد في أي بحث علمي جملة من الصعوبات التي تواجه الباحث.
- صعوبة الحصول على المعلومات والبيانات اللازمة من بلدية سوق الاثنين بولاية تيزي وزو بسبب التكتم النسبي كون المؤسسة تسعى للحفاظ على سرية عملها.
- صعوبة الدراسة الميدانية نظرا لقلة المعرفة الجيدة لدى معظم الموظفين بخصوص هذا الموضوع وعدم وعيهم بأهمية استخدامه في الإدارة وضرورة تطبيقه.
- محدودية الدراسات المهتمة بمجال نظام أمن المعلومات على مستوى الإدارة العامة.

الفصل الأول
الإطار المفاهيمي لنظام أمن المعلومات في الإدارة العامة

تمهيد:

يعد نظام المعلومات الركيزة الأساسية التي ترتكز عليها المؤسسات للحصول على معلومات مناسبة والتي تساهم في صنع واتخاذ القرارات، فنظرا للتدفق الكبير للمعلومات واحتوائها على مصادر مختلفة أدى بالمنظمة إلي تبني هذا النظام واعتباره الوسيلة اللازمة التي ينبغي استخدامها في العمل الإداري لما لها من أهمية بارزة في إدخال ومعالجة المعلومات والبيانات التي تحتاجها المنظمة في تسيير شؤونها إضافة إلي قدرته علي حفظ تلك المعلومات واسترجاعها في فترة زمنية قصيرة و بأقل جهد ممكن.

وفي ظل التطور السريع الذي لحق بنظم المعلومات بانتقاله من بيئة تقليدية إلي بيئة أكثر حداثة والتي يتم فيها الاستخدام المكثف للوسائل والأجهزة الالكترونية وسهولتها أصبحت تشكل تهديدا كبيرا بالنسبة لهذه النظم، فأضحى من الضروري اتخاذ التدابير اللازمة للحد من انتشار هذه المخاطر والوقاية منها، لذا لابد من إتباع إجراءات أمنية صارمة والتي تدعو إلي حماية النظام ومكوناته والحرص على سلامة المعلومات وسريتها بهدف الحصول علي الكفاءة والفعالية داخل المؤسسة لتحقيق التطور في شتي مجالاتها.

وبهذا الصدد سنتطرق في هذا الفصل إلي دراسة كافة المفاهيم المتعلقة بنظام أمن المعلومات حيث تم تقسيمه إلي مبحثين وهما:

المبحث الأول: ماهية نظام المعلومات.

المبحث الثاني: ماهية أمن المعلومات.

المبحث الأول: ماهية نظام المعلومات.

يمثل نظام المعلومات أحد العناصر المهمة والضرورية لأي مؤسسة فهي ميزة أساسية ينجم عنها توفر المعلومات التي تساعد المؤسسة في إنجاز مهامها بدقة متناهية والتي تضمن الاستمرارية والثبات، فعلى المؤسسة أن تسعي إلي الحفاظ علي نظام معلوماتها عن طريق القيام بمراقبته وحمايته من أي تدخل، وكذا تقييم مدي كفاءته على المستوي الداخلي لها، فمصطلح النظام جزء لا يتجزأ منه، فبدون نظام لا وجود لمعلومة صحيحة وثابتة.

المطلب الأول: تعريف النظام ومكوناته.

أصبح النظام عنصر فعال في تسيير شؤون المؤسسات فقد بات من بين المفاهيم الأكثر تداولا وانتشارا في جميع المجالات فله دور كبير في ترسيخ الإمكانيات وتفعيل وإتاحة الخدمات الضرورية لبناء وتطور المؤسسة.

1- مفهوم النظام:

يمتاز النظام بصفة التكامل والتماسك بين أجزاءه فنجد أن لكل مجال نظام خاص به فهو يمثل عمود كل منظمة فهذا المصطلح لقي تعريفات عديدة، حيث سنتطرق إلي البعض منها وهي كالتالي:

التعريف 1: النظام كلمة مشتقة من المصطلح اليوناني " system " ويقصد به تسلسل العمليات بين مجموعة من الأجزاء والتي يتم استخدامها في مجال علمي[1].

التعريف 2: النظام عبارة عن تناسق وتوافق أجزاءه بغية تحقيق الأهداف المرسومة والمدروسة بشكل واضح وسليم[2].

التعريف 3: ويعرف النظام أيضا على أنه العلاقة الموجودة بين بيئة النظام والنظم الفرعية له والقائمة علي تحقيق أهداف معينة[3].

ومن خلال هذه التعريفات نستنتج أن النظام هو مجموعة من العناصر والأجزاء والأنظمة التي تربطهم علاقة تكاملية وتفاعلية غاياتها تحويل هذه المكونات إلي أهداف ونتائج يسعي النظام لتحقيقها.

2- مكونات النظام:

يتكون النظام من وحدات ومكونات تعمل معا بشكل منتظم ومتناسق لتشكل وظيفة كلية له وهي كالتالي[4]:

أ- المدخلات input: وتتمثل في مختلف الموارد التي تدخل النظام سواء كان من البيئة الداخلية أو الخارجية ليتم معالجتها وقد تكون علي شكل بيانات أو جهود بشرية ...الخ.

ب- المعالجة processing: وهي عبارة عن عمليات تحويلية تقوم بتحويل المدخلات إلي مخرجات مثل الحسابات القائمة على البيانات وغيرها.

ج- المخرجاتoutput: هي النتائج التي تم الحصول عليها من عملية التحويل ويتم نقل هذه النتائج إلي الجهات المعنية مثل المعلومات الإدارية التي يتم نقلها إلي مستخدميها.

---

[1] - خاد راجم، **أثر نظام معلومات الموارد البشرية على أداء العاملين، دراسة حالة، مؤسسة شي علي بسطيف**، رسالة ماجستير(جامعة ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير 2011)، ص 35.

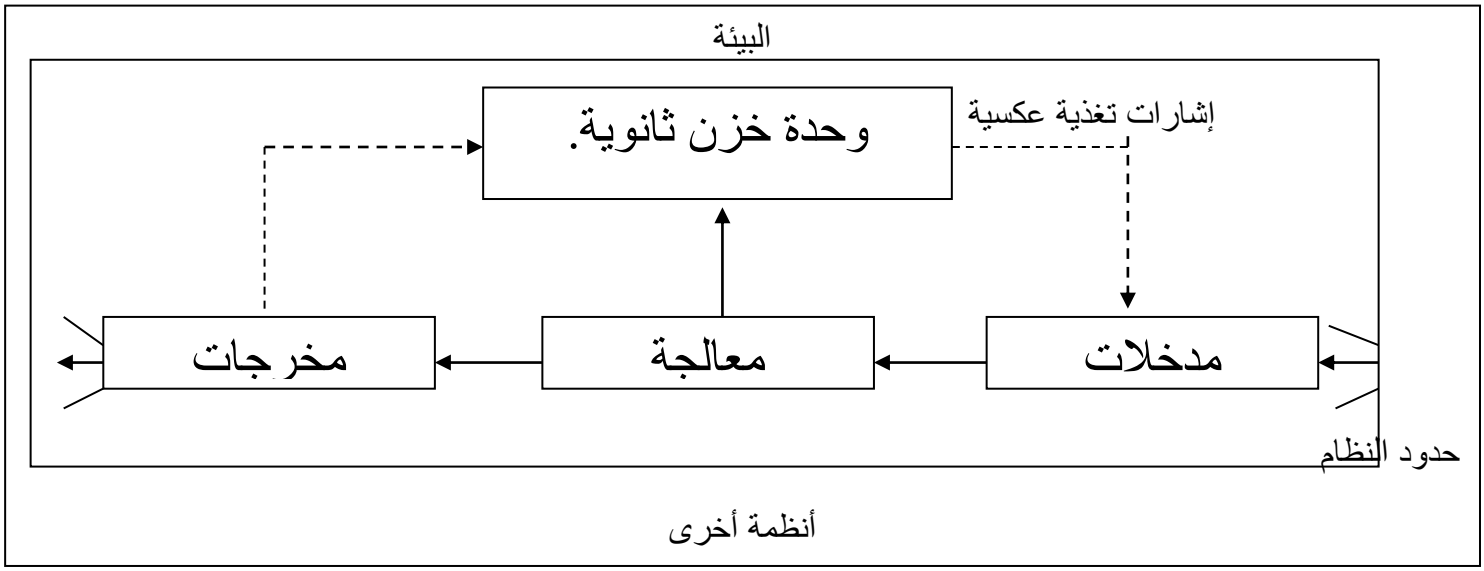
[2] - عمر أحمد همشري، **الإدارة الحديثة للمكتبات ومراكز المعلومات** (عمان: دار الصفاء للنشر والتوزيع، ط2، 2010)، ص 388.

[3] - همشري، **المرجع نفسه**، ص 389.

[4] - عماد الصباغ، **نظم المعلومات ماهيته، مكوناته** (الدوحة: جامعة قطر، 2000)، ص 13.

د- التغذية العكسية: تعمل علي تقويم نتائج عمل النظام وتصحيح أهدافه فهي تمثل أداة إرشادية لأنشطة النظام، وهي جزء من المدخلات إذ تقوم باسترجاع البيانات لإعادة صياغتها للوصول إلي هدف معين.

الشكل رقم (1-1): مكونات النظام



المصدر: عماد الصباغ، نظم المعلومات ماهيتها ومكوناتها (الدوحة: جامعة قطر، 2000)، ص 15.

يوضح الشكل رقم (1-1) أن عناصر النظام متداخلة فيما بينها فهي تعمل بشكل متسلسل فإذا حدث خلل علي مستوي أي عنصر من عناصره فقد يؤدي إلي تلاشي النظام وكذا عدم قدرته علي تنفيذ مهامه وتحقيق الهدف المسطر، لأن ذلك الارتباط الذي تتسم به هذه العناصر تعطيه صفة التكامل والتماسك والاستمرارية.

المطلب الثاني: خصائص النظام وأنواعه.

للنظام عدة خصائص وأنواع تبرز مكانته وأهميته في مختلف المجالات لأنه يلعب دورا فعالا في تبني معظم السياسات ووفرة الإمكانيات التي تتيح الطرق اللازمة في تحقيق كافة الأهداف.

أولا: خصائص النظام:

يمتاز النظام بعدة خصائص منها[1]:

1- هدف النظام: يسعي النظام إلي تحقيق أهداف وغايات مختلفة وللوصول إلي هذه الأهداف لابد من تحديد مجموعة من الأهداف الفرعية لكل عنصر من عناصره والتي تنجم عنه هيكلة وتصميم جيد له والذي ينبع عنه تحقيق الهدف الأعلى والعام للنظام ككل.

2- بيئة النظام: تعتبر البيئة عنصر هام للنظام، فهذا الأخير يتفاعل مع العناصر التي تأتي من خارجه إذ يؤثر ويتأثر بها.

3- مكونات النظام: يتم إدخال المكونات الرئيسية للنظام علي شكل مدخلات حيث يتم معالجتها وتحويلها إلي مخرجات مرغوب فيها.

4- الرقابة والضبط: تقوم هذه العملية علي منع النظام من الانحراف عن هدفه، حيث تقوم وظيفة استرجاع النتائج بالتدقيق ومقارنة المخرجات الناتجة بمعايير موضوعة مسبقا وإرجاع هذه النتائج إلي النظام في مرحلة الإدخال لتوجيه عملية التشغيل.

5- حدود النظام: هي الخطوات التي تهدف إلي تحديد عناصر النظام، حيث تظهر جميع مكوناته ومدى مساهمتها في تحقيق الغايات المرجوة.

6- مستويات النظام: يحتوي النظام علي عدة نظم فرعية والتي تكون جزء من النظام الأكبر وتابع له، ولتحديد مستويات النظام لابد من أن نكون علي دراية كاملة بشبكة النظم وكيفية استخدامها.

7- الاتصال: وهي عملية التبادل بين طرفين أو أكثر والتي تصبو إلي استرجاع النتائج وضمانها.

إن لخصائص النظام خطوط و آليات تقوم بتحديد محتوى النظام وفصلها عن كل ما يدخل ويخرج من بيئة النظام، إذ تسعي هذه العناصر إلي تحقيق هدف واحد ومشترك.

ثانيا: أنواع النظم.

تحتاج النظم إلي طريقة استخدام منتظمة من شأنها معرفة طريقة تصنيفها وتمييزها بأعلى الدرجات إذ نجد أن هذه النظم تنقسم إلي عدة أنواع منها[2]:

1- النظم المجردة / النظم المادية:

تتكون أجزاء النظم المجردة من مفاهيم ومصطلحات تهدف إلي إعطاء تفسير واضح للظواهر المحيطة بنا سواء كانت ظواهر طبيعية أو اجتماعية وأحسن مثال النظريات.

[1] - إسماعيل مناصرية، **دور نظام المعلومات الإدارية في الرفع من فعالية عملية اتخاذ القرارات الإدارية**، رسالة ماجستير (جامعة مسيلة: كلية العلوم التجارية وعلوم التسيير، 2014)، ص 48.

[2] - فايز جمعة النجار، **نظم المعلومات الإدارية منظور إداري** (عمان: دار حامد للنشر والتوزيع، ط2، 2010)، ص41.

أما النظم المادية فهي نظم ملموسة تستخدم أشياء ومكونات وحتى أفراد لبلوغ غايتها، وهذا النوع يكون عادة مبني علي النظم المجردة.

2- النظم المفتوحة / النظم المغلقة:

يتفاعل النظام المفتوح مع بيئته بحيث يؤثر فيها و يتأثر بها وتعتبر المنظمات ونظم المعلومات أمثلة لهذا النوع من النظم.

أما النظم المغلقة فهي نظم لا تتأثر ببيئتها حيث توفر مدخلاتها ذاتيا كالتنظيمات البيروقراطية.

3- النظم الثابتة / النظم المتغيرة:

يستخدم النظام الثابت بآليات محددة سابقا ويكون شبه مطلق أي يمكن التنبأ بسلوكه مستقبلا مثل نظام البرنامج الحاسوبي.

أما فيما يخص النظام المتغير فهو يعمل في حدود آلية معينة ومستمرة إذ لا يمكن التنبأ بسلوكياته مثل النظم الإدارية والمالية.

4- النظم الدائمة / النظم المؤقتة:

النظم الدائمة هي النظم التي تستمر لمدة زمنية طويلة في إجراء الأعمال رغم التغيرات التي لحقت بها والتطورات التي حدثت له مثل النظام السياسي.

أما النظم المؤقتة فتنشأ لغرض محدد لتحقيق هدف معين ويعمل في نطاق فترة زمنية محددة وبعدها ينتهي النظام.

نستخلص بأن أنواع النظم تقوم بإعطاء الفهم الواضح للمستخدم والاستيعاب الأمثل لهذه التصنيفات ومعرفة كيفية استخدامها في نطاق عملهم.

المطلب الثالث: ماهية المعلومات وخصائصها.

تلعب المعلومات دورا فعالا ومهما في الإدارة الحديثة حيث تمثل المادة الأساسية التي يبني عليها القرار، فنجد أن معظم المؤسسات تسعى للحفاظ علي هذا المورد وذلك بتوفير الإمكانيات اللازمة لضمان الاستخدام الأمثل لها والوصول إلي أحسن النتائج التي تطمح لها المؤسسة[1].

أولا: مفهوم المعلومة information.

لقد تنوعت التعريفات المقدمة للمعلومات ومن أبرزها ما يلي:

التعريف1: المعلومات هي أداة للتطبيق ونتيجة العمليات الموجودة، فهي ذات خصائص مشتركة فالمعرفة عالمية في صفاتها والمعلومات محددة أما البيانات ضرورية[2].

[1] - فايز جمعة النجار، **نفس الرجع السابق**، ص 41.

[2] - ذياب البداينة، **الأمن و حرب المعلومات**، (عمان: دار الشروق، 2002)، ص 60.

التعريف2: تعريف المعلومة حسب dictionnaire des medias لفرانسيس بال "هي نتاج الاستعمالات حول موضوع معين، تصف العلاقات في متناول الشخص المعني أو الهيئة المعنية"[1].

أما باتيرون فيعرفها علي أنها "عنصر أو نظام يمكن أن ينقل بواسطة إشارة أو مجموعة من الإشارات"[2].

أما Tomstonier فيرى بأن" المعلومات هي إحدى الخصائص الأساسية للكون، شانها شان المادة والطاقة فهي ليست مقصودة علي فئة معينة لكنها جزء من نظام يعرض عملية التنظيم، فإذا كانت الكتلة هي التعبير عن المادة والقوة هي التعبير عن الطاقة فإن التنظيم هو التعبير عن المعلومات"[3].

ومن خلال هذه التعريفات يمكن أن نستنتج أن المعلومات هي مجموعة من البيانات والعناصر التي يتم معالجتها وتحليلها لتصبح ذات دلالة ومنفعة لمستخدميها، بعد أن نزيل الغموض عنها ونعطى لها صورة واضحة، فهذه العناصر تكمن في:

- للحصول علي معلومات يجب توفر بيانات يتم معالجتها.
- تعطى المعلومات معنى وفهما واضحا للهدف المرغوب.
- إرساء الشفافية وزيادة المعرفة لدى المستخدم.

ثانيا: خصائص المعلومات.

يلتزم نظام المعلومات في أي مؤسسة بشرط تقديم معلومات تساهم في سهولة اتخاذ القرارات، وذلك عن طريق استخدام خصائص تحدد ميزة هذا الأخير وقابليته لتلبية متطلبات المؤسسة ومن هنا تستوقفنا خصائص المعلومات التالية[4]:

1- الدقة: وتشمل قابلية المعلومات في تلبية حاجيات المستفيد بصبغة الدقة المتناهية فمعظم الأخطاء الواردة في المعلومات ناتجة عن عدم صحة البيانات التي تم إدخالها والعكس صحيح، كما نجد نوع المعلومة وطبيعة الاستخدام والمستوى الإداري وكذا طبيعة المعايير المستخدمة في القياس وغيرها تساهم في إرجاع صحة البيانات المستخدمة في المعلومة أمر نسبي.

---

[1] - balle Francis, **dictionnaire des medias,** (paris : Larousse,1998), p124.

[2] - عبد الغاني زغنوف، المعلومة وأهميتها في المجتمع المعلوماتي، **مجلة البحوث والدراسات الإنسانية**، (سبتمبر 2014)، نقلا عن patteyron.EA, Le **management de l'information à l'organisation,** 1996. ص 152.

[3] - أحمد نافع المدادحة، عدنان عبد الكريم الذيابات، **اقتصاديات المعلومات والمعرفة** (عمان: مكتبة المجتمع العربي للنشر والتوزيع، 2014)، نقلا عن Tomstonnier, information and the Internal, structure of the universe cited,1990 ، ص100.

[4] - مراد مرمي، **أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة الجزائرية،** شركة chi ali profiplax بسطيف، رسالة ماجستير (جامعة سطيف: قسم العلوم الاقتصادية، 2010)، ص 19.

2- التوقيت: إن الوقت المناسب يساعد في إيصال المعلومة للمستفيد وأي تأخر يؤدي إلى إنقاص قيمة المعلومة وعدم استغلالها في الوقت اللازم.

وهناك أسباب عدة لعدم توفر المعلومة في وقتها وهي كالتالي:

- انفراد النظام العام عن باقي الإدارات الأخرى وبذلك عدم درايتها للوقت المناسب لحاجة هذه الأخيرة إلى المعلومات.
- استخدام وقت أطول من أجل إنتاج معلومات.
- نقص فهم الإدارات المستفيدة لتقنية توفير المعلومات في الفترة اللازمة، وهذه الأسباب تؤدي إلى فشل المؤسسة في اتخاذ قراراتها.

3- الوضوح: لتحقيق الوضوح في المعلومة والاستفادة منها في المجال المطلوب لابد أن تكون بعيدة عن الغموض وسهلة للفهم المباشر.

4- المرونة: وهو تأقلم المعلومة وتعدد أوجه استخدامها لفائدة المستخدمين فكلما كانت المعلومة مستخدمة من طرف تطبيقات متعددة كانت أكثر مرونة والعكس صحيح.

5- الشمول: يجب أن تكون المعلومة أكثر إحاطة بمشكلة البحث وذلك يساعد الإدارة في تسيير مهامها المختلفة عن طريق إيضاح المستفيد لجميع المعطيات اللازمة عن الظاهرة، وبذلك سهولة إيجاد معلومات كافية.

6- القابلية للمقارنة: إن صحة المعلومات تكمن في قابليتها للمقارنة مع باقي المعلومات لمؤسسة ما، وغالبا ما تقارن المعلومات في مجال نشاط واحد.

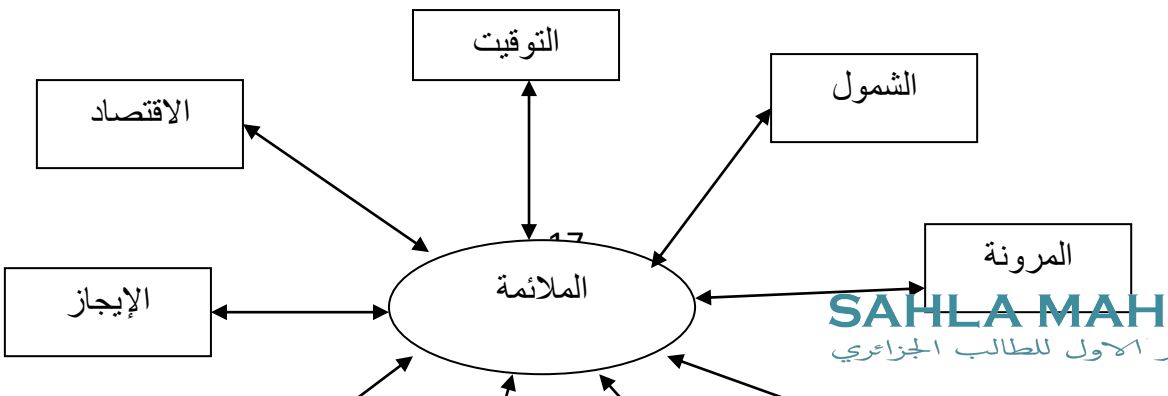
7- الإيجاز: يجب على المعلومات أن تكون مختصرة بحيث يتم ذكر المطلوب فقط بمراعاة الحالات الاستثنائية.

8- الموضوعية: وهنا نقصد عدم التحيز، وتعطي المعلومة دون أية رغبة شخصية أو تدخل من طرف معين، أو الانحياز لرؤى معينة، بشكل يتسم بالصدق في المضمون مما يضمن الرجوع إليها عند الحاجة.

9- اقتصادية: تكمن فائدة استخدام المعلومات في قابلية نجاحها وذلك راجع للجانب المالي الذي تتحمله المؤسسة للحصول على المعلومات المرغوبة، فالخاصية الاقتصادية تكمن في إيجاد أكبر قدر ممكن من المعلومات وذلك بأقل التكاليف.

- وفي الأخير فالملائمة هي النتيجة المرجوة من تطبيق خصائص المعلومات على الظواهر والدراسات والشكل الأتي يبين ذلك.

الشكل رقم (2-1): خصائص لملائمة المعلومات.



المصدر: خالد رجم، أثر نظام معلومات الموارد البشرية علي أداء العاملين، دراسة حالة مؤسسة شي علي بسطيف خلال 2011، رسالة ماجستير (ورقلة، كلية العلوم الاقتصادية)، ص 38.

ويضيف بعضهم خصائص أخرى للمعلومات ومنها ما يلي[1]:

النمو والتجدد: في هذه الخاصية تظهر لنا أن المعلومات في تطور ونمو مستمر إذ تتزايد نظرا للاستعمال المكثف وتعدد أنواعها ومصادرها.

التشكل: تأتي المعلومات بصيغ مختلفة ومتنوعة فيمكن أن نجدها علي شكل رسومات أو صور أو قوائم أي تكون حسب الاستخدام المطلوب.

النقل: للمعلومات قنوات عدة للتنقل والوصول إلي المستفيد فهي تأخذ أنماط مختلفة كالكتب أو الاسطوانات...الخ.

الاندماج: لدى المعلومات قدرة عالية في الانخراط مع العناصر المتنوعة فيمكن أن نكوّن بها عدة جمل وأفكار منسجمة مع بعضها البعض مشكلة نص وجملة مفيدة وجديدة إذ يمكن استخلاص هذه العبارات من نصوص سابقة.

الوفرة: تمتاز المعلومات بالوفرة لما لها من ايجابيات تمنح للمستخدم الفهم و كذا ينجر عنه الزيادة في الطلب إضافة إلي الاستفادة منها في كثير من المجالات.

النسخ: تنوعت وسائل حفظ المعلومات لتجدب ضياعها وكذا ضمان الاستخدام السليم لها أثناء الحاجة إليها.

التحقق: إمكانية مراجعة وفحص المعلومات المقترحة لضمان صحتها ودقتها.

يظهر من خصائص المعلومات أن هذه الأخيرة تحتمل الصدق أو الكذب أي أن لها ايجابيات تعود بالمنفعة للمستفيد كما لها سلبيات تؤثر عليه إما علي مستوي شخصي أو في مجال عمله،حيث أن خضوع المعلومة لهذه الاحتمالات راجع إلي التدفق السريع لها.

[1] - مصطفى ربحي عليان، **اقتصاد المعلومات**، (عمان: دار صفاء للنشر والتوزيع، 2010)، ص114.

المطلب الرابع: مصادر وأنواع المعلومات.

تكون المعلومات دون فائدة تذكر حتى يتم استخدامها من طرف الفرد لتحقيق غرض معين وتنتقل هذه المعلومات عن طريق مصدر معين، فهذا الأخير يمكّن الفرد من الحصول علي معلومات تحقق له احتياجاته وترضى اهتماماته[1].

أولا: مصادر المعلومات.

تعددت مصادر المعلومات إلي فئات مختلفة نظرا لاختلاف الباحثين في تصنيف وتقسيم هذه المصادر من نوع لأخر وهي كالتالي[2]:

1- المصادر الوثائقية: يشمل هذا المصدر على ثلاث أصناف من المعلومات بحيث يمكن أن تأتي علي شكل تصورات وأفكار معروفة مثل أعمال المؤتمرات أو تقارير بحوث ويطلق عليها أوعية المعلومات الأولية.

أما فيما يخص أوعية المعلومات الثانوية فهي تقوم بالاعتماد علي المعلومات الأولية في صياغة عملها حيث تسعي إلي إعادة عرض المعلومات الموجودة في الأوعية الأولية للمعلومة وتمثل مفتاح الأوعية الأولية ومثال ذلك الكتب الدراسية والمستخلصات...الخ.

إضافة إلي وجود أوعية من الدرجة الثالثة والتي تساعد الباحث في أداء بحثه والاستفادة من مختلف المعلومات الواردة في أوعية المعلومات الأولية والثانوية وأحسن مثال الكتب السنوية.

2- المصادر غير وثائقية: تختلف الجهات المعنية بإصدار المعلومات حيث يمكن أن تكون جهات رسمية كأجهزة الدولة أو مراكز البحوث كما يمكن أن تكون من طرف جهات غير رسمية كاللقاءات الجانبية أثناء المؤتمرات.

3- المصادر العامة والمتخصصة: ويعتمد هذا المصدر علي الموضوع الذي تم معالجته وتناوله قد يهتم بالقضايا المتعلقة بالشأن العام أو الخاص.

4- مصادر المعلومات المطبوعة وغير مطبوعة: فهذه الطريقة توضح كيفية استخراج المعلومات والأشكال التي تأتي عليها فيمكن أن نجدها علي شكل كتب ومنشورات كما يمكن أن تكون علي شكل أقراص واسطوانات.

5- المصادر التقليدية وغير تقليدية: أي تصنف المعلومات هنا حسب بعدها وحداثتها.

ثانيا: أنواع المعلومات.

[1] - مصطفى ربحي عليان، **نفس المرجع السابق**، ص 114.

[2] - غالب عوض النوايسة، **مصادر المعلومات في المكتبات ومراكز المعلومات**، (عمان، دار صفاء للنشر والتوزيع، ط2، 2015)، ص ص 33-35.

لقد تعدد استخدام المعلومات في معظم المؤسسات نظرا لاختلاف مستوياتها الإدارية وما لها من أهمية في صناعة القرار ما يعطي تصنيف ينبع عنه الفهم الواضح للمعلومة ومن بين هذه التصنيفات نجد ما يلي:

أ- معيار مصدر المعلومات: يمكن تصنيف هذا المعيار إلي عدة أنواع فالمعلومات تشمل علي مجالات مختلفة قد تكون معلومات عسكرية تتعلق بأسرار عسكرية كالاستخبارات وكذا طرق ضبط وتواصل المسئولين العسكريين، بالإضافة إلي معلومات متعلقة بالعمليات المالية ونظم الأعمال ووجود معلومات شخصية تهتم بالحالة المدنية للفرد ومختلف مجالات الائتمان والاتصالات المرتبطة به.

فمصدر المعلومات نجده أيضا ينبع من داخل وخارج المؤسسة، فهذه الأخيرة تعالج مختلف القضايا والأحداث، والبيانات والأوضاع الناتجة من البيئتين الداخلية والخارجية لها.

ب- المعلومات الأولية والثانوية: تقوم المعلومات الأولية بتقديم تفسيرات جديدة للوقائع والحقائق بغرض الاستفادة منها وتأخذ أنماط مختلفة كالكتب أما المعلومات الثانوية فتكون تابعة للمعلومات الأولية إذ تعتمد عليها في استخلاص أفكارها كالمعاجم والموسوعات[1].

ج- المعلومات الرسمية والغير رسمية: المعلومات الرسمية هي معلومات موثقة ومؤكدة حيث يعتمد عليها في صناعة القرار وتصدر من جهات معروفة كالدستور والقوانين لكن لا تكون متوفرة لنا دائما، أما المعلومات الغير رسمية فهي معلومات تساهم في صناعة العديد من القرارات ويعتمد عليها إثر عدم توفر المعلومات الرسمية حيث تحتمل هذه القرارات الصواب أو الخطأ لذا لابد من الحذر لبلوغ صحة القرار إذ نجدها علي أشكال عدة كالتوقعات والإشاعات أو الخبرات[2].

ونشير أيضا إلي وجود تصنيفات أخرى لهذه الأنواع حيث نجدها تصنف إلي ثلاثة فئات رئيسية وهي:

1- المعلومات الانمائية: وهي معلومات تقوم بمساعدة الفرد وتهيئته وتنمية قدراته الفكرية وتحسين مستواه الثقافي لتوسيع معارفه والتي تمكنه من انجاز عمله.

2- المعلومات التعليمية: وتقوم علي أساس التعليم والتعلم إذ تكمن في إعطاء الفرد الدروس الكافية لاستيعاب المعلومات وضمان الاستخدام الأمثل لها.

3- المعلومات الإنجازية: يقوم هذا النوع بإنجاز مختلف الأعمال المقررة وذلك بالرجوع إليها عند الحاجة فهو يساعد الإداري علي إتمام عمله بكل دقة[3].

---

[1] - البداينة، **المرجع السابق الذكر**، ص58.

[2] - زغنوف، **المرجع السابق الذكر**، ص155.

[3] - عامر ابراهيم قنديلجي، حسن رضا النجار، **علم المعلومات والنظم والتقنيات**، (عمان: دار المسيرة للنشر والتوزيع والطباعة، 2015)، ص23.

وفي هذا الصدد نجد أن أنواع المعلومات لا تقتصر فقط علي هذه المجموعات فهنالك عدة أنواع أخري تبين نوع المعلومة المستخدمة إذ نستطيع أن نجد معلومات سياسية أو اجتماعية أو عسكرية أي تصنف هذه الأخيرة ضمن المواضيع المتناولة.

المطلب الخامس: ماهية نظام المعلومات ومكوناته.

في ظل التزايد والتراكم المستمر والهائل للمعلومات، أصبحت معظم المؤسسات تشكو من نمط إدارة هذه المعلومات مما أدى إلي إيجاد طريقة تساهم بشكل أو بأخر في معالجة ونقل المعلومات بين مختلف الجهات إذ نجد أن نظام المعلومات هو الوسيلة المثلي لذلك، حيث سنتطرق في هذا المبحث إلي إبراز ماهية نظام المعلومات وأهم مكوناته.

أولا: مفهوم نظام المعلومات.

يعرف نظام المعلومات علي أنه مجموعة من العناصر المتفاعلة مع بعضها ومع محيطها لجمع البيانات وتحليلها لإنتاج معلومات تؤدي إلي صناعة القرارات[1].

ويعرفها الدكتور قنديلجي علي أنه مجموعة من العناصر البشرية والآلية التي تعمل معا علي تجميع البيانات ومعالجتها طبقا لقواعد معينة بغرض إتاحتها للباحث علي شكل معلومات مفيدة تساعده علي اتخاذ القرار[2].

كما تعرف أيضا علي أنها الإجراءات النمطية التي تقوم بجمع المعلومات ومعالجتها وكذا خزنها واسترجاعها وتوزيعها بهدف دعم اتخاذ القرار داخل المنظمة[3].

وبصفة عامة يمكن تعريف نظام المعلومات علي أنه ذلك النظام الذي يضم عدة مكونات وموارد وبرامج وأجزاء متفاعلة ومتجانسة فيما بينها مشكلة عمليات وبيانات يتم معالجتها للحصول علي معلومات مفيدة وسليمة، والتي تساعد المنظمة علي صنع واتخاذ القرار.

يشمل نظام المعلومات علي عناصر ومكونات أساسية والتي تشكل الموارد الضرورية له وهي كالتالي[4]:

---

[1] - الصباغ، **المرجع السابق الذكر**، ص11.

[2] - قنديلجي، **المرجع نفسه**، ص 40.

[3] - عبد الحكيم معوج، أمن نظام المعلومات وأهميته في ظل تطورات تكنولوجيا المعلومات والاتصالات، **مجلة فكر ومجتمع**، (الجزائر، طاكسيج كوم،2015)، ص 246.

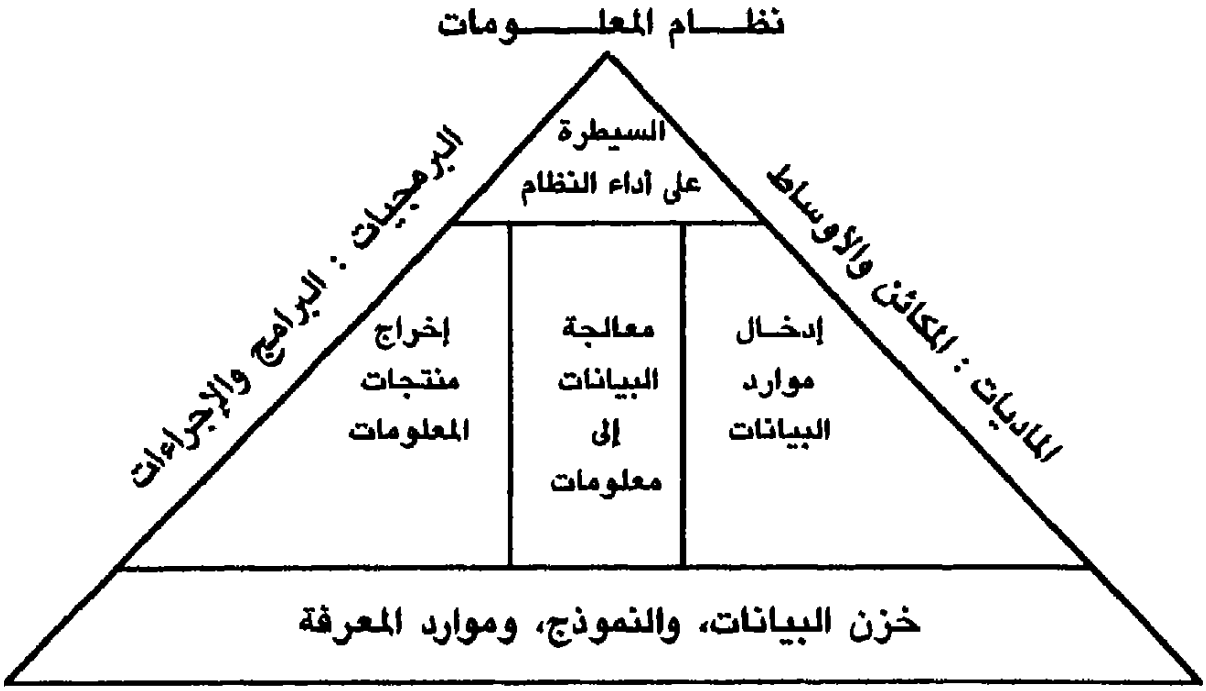
[4] - أحمد نافع المدادحة، **نظم المعلومات المحو سبة ودورها في مجال المكتبات**،(عمان: مكتبة المجتمع العربي للنشر والتوزيع،2014)، ص19.

1- الموارد البشرية: وهم الاختصاصيين الفنيين الذين يقومون بتشغيل النظام وإدارته بطريقة فنية والسعي إلي تطويره واستمرار يته، فهم يصممون النظام بناءا علي المتطلبات المعلوماتية للمستخدم النهائي.

2- المستخدمين النهائيين: وهم الأفراد الذين يستفيدون من المعلومات التي ينتجها النظام حيث يستخدمونها لأغراض عدة ومتنوعة.

3- الموارد المادية: وتشمل مختلف المصادر والأجهزة التي يتم فيها نقل المعلومات والبيانات فهي لا تقتصر فقط علي الحواسب بل تضم كل الأغراض التي يستخرج عليها المعلومات بشتى أشكالها.

الشكل (3-1) نموذج عن مكونات نظام المعلومات.



المصدر: عماد الصباغ، **نظم المعلومات ماهيتها ومكوناتها** (الدوحة: جامعة قطر، 2000)، ص21.

يوضح لنا الشكل الهرمي رقم (3-1) أن هناك علاقة بين عناصر نظام المعلومات حيث يسعى هذا الأخير إلي إظهار الدور الفعال الذي يلعبه كل عنصر إضافة إلي أن العناصر تتفاعل مع بعضها البعض مكوّنة عمل متجانس ومتكامل تطمح المؤسسة لانجازه.

4- موارد البرمجيات: وتمثل مختلف التعليمات التي تقوم بمعالجة البيانات وكذا البرامج الموجة للاستخدام الأمثل لهذه الأجهزة.

5- موارد البيانات: تعتبر البيانات مورد مهم في المنظمة حيث يتم استخدامه بشكل فعال إذ تضمن فائدته للمستخدم النهائي في المنظمة، وقد تأخذ البيانات أشكال عدة كالبيانات الرقمية التي تصف التعاملات الجارية داخل المنظمة.

6- موارد الشبكات: أصبح هذا النوع مهما لإدارة الأعمال الإلكترونية والعمليات التجارية فقد تنوّعت شبكات الاتصال وهي في تطور مستمر ودائم حيث تعبر عن وجود نظام المعلومات في المؤسسة.

تستهدف مكونات نظام المعلومات إلي المعرفة اليقينية بكافة الوسائل والطرق التي ينبغي استخدامها وإتباعها لسير عمل المؤسسة وضمان نجاحها علي مستوى الإداري[1].

المطلب السادس: خصائص، وأنواع، وفوائد نظام المعلومات.

يتميز نظام المعلومات بمجموعة من الامتيازات التي تعطيها خاصية الوضوح والاستمرارية في إطار تنفيذ الأعمال المبرمجة علي مستوى المؤسسة وكذا قدرته علي حفظ واسترجاع المعلومات المختلفة والضرورية للمؤسسة.

أولا: خصائص نظام المعلومات.

يقوم نظام المعلومات علي توفير العديد من الصفات الأساسية التي تبرز صحة أداء النظام لوظائفه ومدى كفاءته، وهي كالتالي[2]:

1- التوافق: لتقييم نظام المعلومات لابد من مراعاة الظروف البيئية التي يعمل فيها سواء بتحديد نوعية المدخلات والمخرجات أو بتلبية احتياجات المستخدم، فعلى نظام المعلومات أن يكون منسجما ومتوافقا مع البيئة المحيطة به.

2- شبكات الاتصال: تمثل هذه الشبكات إحدى القنوات التي تضمن تدفق المدخلات والمخرجات بين الأنظمة، فنتائج نظام معين قد تكون من مدخلات نظام آخر، مما يوضح أن عامل الاتصال متوافر بين الأنظمة الفرعية وبأن النظام يتميز بالفعالية في انجاز وظائفه.

3- التغذية العكسية: هي أسلوب التعامل ما بين النظام وبيئته الخارجية واستيعابه لمختلف النتائج والظروف الناجمة عن هذه العلاقة فالوقت يمثل العامل الأساسي الذي يحدد قيمة عمل النظام.

4- التكلفة: تسعى هذه الخاصية إلي تحقيق التوازن بين قيمة المعلومات وتكلفتها أي أن المعلومات التي يوفرها النظام تتناسب مع قيمتها أثناء الاستخدام.

5- استخراج المعلومات: لإعداد المعلومات لابد من التقيد بالفترة الزمنية المحددة لأن أي تأخر يؤدي إلي نقص في قيمة المعلومات بحيث يصبح معناها بلا فائدة.

6- التوجيه: تخضع عملية التوجيه إلي قواعد وقوانين تضمن لها الصحة والدقة في معانيها حيث يجب مراعاة تقديم المعلومات بكمية معتبرة وأن تكون مناسبة وذات نوعية ومصدر سليم.

تمتاز خصائص نظام المعلومات بالشمولية لما لها من عناصر مهمة تساهم في تحديد الإجراءات اللازمة اتخاذها أثناء استخدام هذا النظام في المؤسسات الإدارية أو الاقتصادية.

---

[1] - أحمد نافع المدادحة، **المرجع السابق**، ص 19.

[2] - محمد جمعون، مونير مناعي،**أهمية نظام المعلومات التسويقي في اتخاذ القرارات التسويقية**، رسالة ماستر(جامعة البويرة، كلية العلوم الاقتصادية والتجارية،2014)، ص45.

ثانيا: أنواع نظام المعلومات.

- لقد تعددت التقسيمات المقدمة لنظم المعلومات و يمكن تصنيفها كالتالي[1]:

1-**نظم معالجة المعاملات transaction processing Systems:(tps)** تعد هذه النظم من أهم النظم فهي تلعب دور مهم في طريقة التعامل والتبادل بين مختلف الأطراف، حيث تقوم بإدارة العمل بشكل روتيني إذ تستفيد المنظمة من جميع وظائفه وتعاملاته من تسويق وإنتاج وحتى تصنيع...الخ.

2- نظم أتمنة المكاتب office automation Systems (OAS): يعتمد هذا النظام على الوسائل التكنولوجية لتسيير عمله، إذ يكمن في مختلف التقنيات والأنظمة الالكترونية المبرمجة لفائدة مساعدة العاملين على انجاز عملهم، بكل دقة وتمعن.

3- نظم المعلومات الإدارية management information Systems(mis): وهي النظم التي تهتم بتوثيق مختلف المعلومات المتعلقة بالإدارة و التي تساهم في إعطاء طابع الشمول إذ تساعد مدير المنظمة على قدرة الحصول على مختلف البيانات والوثائق المتعلقة بالإدارة والعاملين بها.

4- نظم دعم القرار décision support Systems:(DSS) هي منظومة مخصصة لمعالجة كافة انشغالات ومشاكل الغير مهيكلة وشبه مهيكلة، حيث تضم مجموعة من النماذج والبرامج، والأدوات التي تقدم حلول تضمن خدمة القرار بشتى أنواعه.

5- نظم مشغلي المعرفة Works Systems knowledge: وهذا النوع يضمن إدخال معارف جديدة والتوسع المعرفي في مختلف المجالات والتي تخدم القرارات غير مهيكلة في المنظمة.

6- نظم معلومات المديرين التنفيذيين exécutive information Systems: تعتمد هذه النظم على مختلف المعلومات الواردة من البيئة الخارجية وكذا الموجودة داخل محيط المؤسسة، إذ تشمل تلبية متطلبات الإدارة و ضرورة توفير معلومات تساعدها على اتخاذ القرار، وكذا مختلف الأخبار المتعلقة بظروف العمل التنافسي وكذا التهديدات التي تعيق سير عمل الإدارة ونجاح المنظمة ككل.

إن أنواع نظام المعلومات لا تقتصر فقط على جانب واحد فهي تتعدى جوانب مختلفة فقد نجدها تحتوي على تقنيات تقليدية أو حديثة في التعامل مع المعلومات وتخزينها، وكذا إبراز الامتداد الجغرافي لهذه النظم فقد نجدها تطغى على حدود دولة واحدة أو تكون على مستوى

[1] - فايز جمعة النجار،"نظم المعلومات وأثرها في مستويات الإبداع"، **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**، م(26)، ع (2) (2010)، ص261.

وطني أو مؤسساتي إضافة إلي تحديد الخدمات الإدارية المتنوعة التي يتم تنفيذها وبرمجتها وكل هذه الأنواع تسعى إلي تحقيق هدف مشترك[1].

ثالثا: فوائد نظام المعلومات.

تعتبر نظام المعلومات عمود كل مؤسسة إدارية تطمح إلى تحقيق التطور في شتى مجالاتها حيث تساعد في سير الأعمال وكذا اتخاذ القرارات اللازمة في الوقت المناسب وتتمثل هذه الأهمية في[2]:

- **السرعة:** حيث يتوفر سهولة وسرعة توثيق المعلومات وكذا تخزينها واسترجاعها.
- **الدقة**: تجد أن دقة المعلومات تؤدي إلى انخفاض معدلات ارتكاب الأخطاء عند عملية جمع وتخزين ومعالجة ونشر المعلومات.
- **توفير الجهد:** فهذا العنصر يبرز لنا أن النظم التقليدية منعدمة في مختلف استخدامات المؤسسة وأن العامل الالكتروني لعب دورا كبيرا في عملية معالجة وتخزين المعلومات وذلك بأقل الجهود والتكاليف.
- **كمية المعلومات**: حيث نجد أن هناك قدرة عالية في توفير وبث المعلومات على مستوى المؤسسة في ظل توفر الحواسيب .
- **الخيارات المتاحة في الاسترجاع**: نجد أن التقنيات الحديثة تعطي نوع من المرونة والدقة في توفر عنصر استرجاع المعلومات وقت الحاجة إليها.

وتتبع أهمية نظام المعلومات أيضا في[3]:

- يؤدي استخدام نظم المعلومات إلى تلبية احتياجات الإدارة العليا وتأمين كل المعلومات التي تحتاجها وكذا مساعدتها على رسم سياستها وتنفيذ مهامها.

- تكون نظم المعلومات التقليدية مفيدة وفعالة للمؤسسات الصغيرة مما يحدد الأبعاد والأشكال المتمركزة فيها وتميزها بالاستقرار في تنفيذ نشاطها.
- إن انتشار المؤسسات وتوسع نشاطها وكذا فعاليتها يحتاج إلى المزيد من المعلومات الذي تؤدي إلى اتخاذ القرار المتعلق بتحديد الأهداف والمعايير اللازمة إتباعها وملائمة هذه القرارات مع الفعاليات الداخلية والخارجية لها.

المبحث الثاني: ماهية نظام أمن المعلومات.

إن الحاجة الملحة للمعلومات في الحياة العملية جعلت الإنسان يرجعها هدف رئيسي وملاذ دائم له في مختلف ميادين حياته الاجتماعية والسياسية وبين الماضي والحاضر،لان

---

[1] - فايز جمعة النجار، **نفس المرجع السابق**، ص 261.

[2] - رجم، **مرجع سابق**، ص47.

[3] - عدنان محمد قاعود،" **دراسة وتقييم نظام المعلومات المحاسبية الالكترونية في الشركات الفلسطينية**"، رسالة ماجستير (جامعة غزة: كلية التجارة،2007)، ص30.

الحصول على المعلومات أمر ضروري نظرا لأهميتها والتي تعدت المجال الإداري والجامعي والاجتماعي، لذا أبى المجتمع إلى أن يحمي هذه المعلومات لتجنب تعرضه لحالات فوضى حياتية عارمة وهذا من خلال توفير الحكومات للسبل الكفيلة لسلامة مختلف أنواع المعلومات،إذ نجد أن الحروب الحالية أصبحت حروب معلوماتية،فمن واجب أي دولة كانت صيانة دفاعها المعلوماتي، فحلول موجة المعلومات والاتصالات أدى إلى تضخم الجرائم الالكترونية مما يستوجب وضع تقنية أمنية سليمة في ظل حماية وسلامة المعلومات سواء الشخصية أو الإدارية فتطبيق نظام امن المعلومات ضروري لتفادي الوقوع في الأخطاء.

لذا سنتطرق في هذا المبحث إلى إبراز مختلف المفاهيم المتعلقة بنظام أمن المعلومات ومكوناته الأساسية[1].

المطلب الأول: نبذة تاريخية عن امن المعلومات.

لقد أشار المؤلف Alexander klimburg أن أمن المعلومات في إطار غير محكم وهذا ما أشارت إليه منظمة حلف الشمال الأطلسي عام 2013 في أثارها الجانبية على أمن دول المنظمة نظرا للابتكارات التقنية المتزايدة في تلك الفترة ومن جانب أخر أخذ العاملون في مختبرات الأبحاث في الستينات والسبعينات نظرة استغراب لتكنولوجيات المعلومات لعدم اقتناع قادة الصناعة بأن هذه التقنيات ستغير العالم، وفي 1943 قام الرئيس التنفيذي لشركة IBM المدعو thomas Watson بالتنبؤ بواقع تكنولوجيات المعلومات ووجود سوق عالمية لمنتجاتها ولربما سيحتوي هذا الأخير على خمسة أجهزة حاسبات فقط، وفي عام 1977 أقر رئيس شركة المعدات الرقمية Ken Olsen أنه لا يوجد سبب يدعو لأي فرد أن يمتلك جهاز كمبيوتر في منزله، أما في منتصف الستينات ظهرت نجاحات شملت الدوائر الرقمية والانترنيت والحواسيب الشخصية، وفي السبعينات ظهرت شبكات الاتصالات السمعية والبصرية والاتصالات الهاتفية الخلوية، بعدها جاءت واجهات المستخدم الرسومية في 1984، وفي 1990 ظهر نظام التشغيل Windows، أما الشبكة العالمية فقد ظهرت في 1991، وفي1998 ظهرت تقنية Google وتم إطلاق أول نموذج من appel i phone وذلك في 2007 ويليه جهاز i pad في 2010.[2]

إن الذين يستثمرون في هذه التقنيات قد أصبحوا أغنياء بشكل مثير للدهشة لكن هناك إخفاقات كبيرة في المنتجات التي أظهرت إمكانية كبيرة في النجاح، وبفشل هذه التقنيات

[1] - محمد عبد حسين الطائي، ينال محمود الكيلاني، **إدارة أمن المعلومات**، (عمان: دار الثقافة للنشر والتوزيع،2015)، ص 09-10.

[2] - محمد عبد حسين الطائي، **نفس المرجع السابق**، ص 10.

تراجع امن المعلومات رغم أن البعض يرجعها موجة سريعة للابتكارات وذلك حسب المصطلح الذي أطلق عليها بالتسونامي (technami) إلا أن هذه الأخيرة جلبت معها أثار جانبية وعواقب غير مقصودة وأهمها انعدام امن المعلومات وهذا ما أضفى وجه القلق بسبب عدم التحكم في هذه التقنيات والابتكارات الحديثة.

توفر تكنولوجيا المعلومات ضمانات محدودة لمنتوجاتها وفي حالة وجود خلل في البرمجيات فان التراخيص تحمي المزود من أي عواقب تسببها خلل تلك البرمجيات.

المطلب الثاني: مفهوم نظام أمن المعلومات.

أولا: تعريف نظام أمن المعلومات:

- **الأمن (Security):** هي مجموعة من الإجراءات الوقائية لتفادي وقوع ضرر كالسرقة أو التخريب، وكذا خرق لأمن المعلومات حين حدوث أي تهديد ينجم عنه فقدان ممتلكات ومعلومات سواءا شخصية أو مؤسساتية، وتشمل جميع مجالات الحياة[1].

- **أمن المعلومات**: هو تحول تدريجي لمجتمع ما من حالة صناعية إلى حالة معلوماتية وهنا فالمعلومات تؤثر وتغير مفهوم الأمن وذلك يندرج التطور والتنقل في أساس القوة من الأرض إلى الآلة وأخيرا إلى المعلومات، فنجد أن الأمن أصبح الكتروني[2].

- يعرف أمن المعلومات أيضا علي أنه مجموعة الإجراءات التي تهدف إلي الحفاظ علي سرية المعلومات والأجهزة والبرمجيات بما في ذلك المتعلقة بالعاملين في هذا المجال[3].

- أمن المعلومات هو استخدام مختلف الإجراءات والوسائل التي تضمن الحماية اللازمة لكافة البرامج والأجهزة المستخدمة في معالجة المعلومات وضمان سلامتها لأنها تمثل المورد والميزة الأساسية التي ينبغي لأي مؤسسة الحفاظ عليها[4].

- **نظام أمن المعلومات:** هو عبارة عن مجال تنافسي يضمن للمدراء سلامة المعلومات وسريتها وأنها محمية حتى من المؤسسة، فهذه المعلومات تكون مجرد طريقة لتسهيل عمل الإدارة، فامن نظام المعلومات يسعى إلى حماية الأدوات والمعلومات المتعلقة بالشركة وأنها تقوم بالاعتماد على جميع مكونات امن المعلومات لتوعية مستخدميها وتفادي الوقوع في خطر استخدام معلومات خاطئة تضر بسلامة الشركة وتطورها[5].

وفي الأخير يظهر لنا أن أمن المعلومات يعتمد علي تقنيات وبرامج تطمح إلي تبني سياسة أمنية هادفة إلي تحقيق التوازن والتكامل بين عناصره وكذا توفير الوقاية والحماية لكافة المعلومات التي يتلقاها النظام.

---

[1] - خالد ياسين الشيخ، **امن نظم المعلومات والرقابة**، رسالة ماجستير (جامعة دمشق:المعهد العالي للتنمية الإدارية، 2010) ص2.

[2] - ذياب البداينة، **مرجع سابق الذكر**، ص 102.

[3] - ندى إسماعيل جبوري، حماية أمن أنظمة المعلومات، **مجلة تكريت للعلوم الإدارية والاقتصادية**، م(7)، ع(21) (2011)، ص76.

[4] - حسن طاهر داود، **الحاسب وأمن المعلومات** (الرياض: مكتبة الملك فهد الوطنية، 2000)، ص23.

[5] - معوج، **مرجع سابق الذكر**، ص247.

- للحفاظ على أمانة وسرية المعلومات، لابد من انتهاج سياسة أمنية تضم مكونات تضمن لها سرية تلك المعلومات وهذه المكونات هي:

أ- **سرية المعلومات (data confidentiality):** إن أمن المعلومات يرشدنا إلى اتخاذ مجموعة من التدابير والاحتياطات اللازمة لتفادي الاطلاع على مختلف المعلومات السرية سواء الشخصية منها أو المالية أو المعلومات العسكرية من طرف الأشخاص الغير مصرحين لذلك[1].

ب- **سلامة المعلومات (data integrity):** في هذا النوع يبرز لنا ضرورة التأكد من محتوى المعلومات وأنها لم تتغير ولم يتم العبث فيها وتدمير أجزاءها، فسلامة وصحة المعلومات تؤدي بأي مؤسسة إلى اتخاذ قرارات سليمة تضمن الاستمرارية والنجاح لأي عمل مبرمج.

فعلي سبيل المثال نقدم قائمة الأسماء الفائزين في مسابقة التوظيف، حيث يجدر الإشارة إلى ضرورة حماية وأمن هذه القوائم من التغيير المحتمل، فهنالك من يقوم بالعبث بها قصد حذف بعض الأسماء المرشحين ويضع أسماء غيرها مما يسبب ارتباك بين الناس ويحرج الجهة المعينة، وهذا يؤدي إلى تفاقم المشاكل بسبب تخريب المعلومات بأنواعها ومصادرها[2].

ج- **ضمان الوصول إلى المعلومات والموارد الحسابية (Availability):** إن سلامة وسرية المعلومات لها دور مهم و فعال، لكن إذا ما كان هناك صعوبة في الوصول إليها والاطلاع عليها واستخدامها، تصبح بلا منفعة ولا جدوى منها، لأن هذه المعلومات تم استغلالها من طرف مهاجمين بشتى الطرق لحرمان المستفيد من استخدامها، وكذا غرضه هو حذف لتلك المعلومات أو عرقلة استمرار العمل، لذا لا بد من ضرورة التأكد من أن النظام الخاص بالمعلومات لازال في الخدمة وأنه ذات فائدة ويتميز بالاستمرارية[3].

تندرج مكونات أمن المعلومات في إعطاء نظرة مهمة إلي مختلف البرامج والأجهزة التي ينبغي حمايتها والتقنيات اللازمة إتباعها أثناء إجراء تعديل لأي معلومة أو طريقة المعالجة والاسترجاع.

المطلب الثالث: أبعاد ومخاطر أمن المعلومات.

ترتكز امن المعلومات علي أبعاد عدة وهي كالتالي[4]:

- إن امن المعلومات مرادف لأمن الحاسب بمختلف مظاهره بما في ذلك امن الشبكات والحاسوب، أمن تكنولوجيات المعلومات وأمن نظام المعلومات...الخ، رغم أن معظم

---

[1] - خالد بن سليمان الغثير، محمد بن عبد الله القحطني، **أمن المعلومات** (الرياض: فهرسة مكتبة الملك فهد الوطنية أثناء النشر، 2009) ص23.

[2]- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **أمن المعلومات الاليكترونية**، (الإسكندرية: دار الفكر الجامعي: 2005) ص13.

[3] - بن سليمان، بن عبد الله، **مرجع سابق الذكر**، ص23.

[4] - الطائي، الكيلاني، **مرجع سابق الذكر**، ص ص 38-42.

التعريفات ركزت فقط علي وجه الحصر في مختلف استخداماته غلي سبيل المثال حماية البيانات الالكترونية، وكل مفهوم متعلق بأمن المعلومات يعتبر فرع من فروع وبذلك تغطي البني التحتية والعمليات والخدمات والنظام وغيرها.

- يركز أمن المعلومات علي تامين كافة موارد المعلومات في المنظمة وذلك من خلال جهود مبذولة لتحقيق غايات جوهرية إلا وهي السرية، والتوفر، السلامة، المسؤولية وقابلية التدقيق وتقوم إدارة امن المعلومات بتحقيق الحماية اليومية لضمان استمرارية العمل وذلك بتحديد المخاطر والتهديدات المترتبة عن هذه الأخيرة وكذلك وضع سياسة أمن المعلومات والتقيد والتنفيذ للضوابط والمعايير.
- إن أمن المعلومات بطبيعته ليس بالمحكم ولا المانع ولم يبلغ حد الكمال فلا يوجد من يقدر علي إزاحة خطر استخدام الغير سليم أو المتقلب للمعلومات وكل ما عليه هو تناسب قيمة المعلومات مع مستوى أمن المعلومات المطلوبة.
- وجوب إستراتيجية ملائمة لأمن المعلومات في المنظمة والتي تتناسب مع طبيعة تكنولوجية المعلومات وتطبيقاتها في نظم المعلومات في شبكة الاتصالات المستخدمة داخل المنظمة ويتم تعديل هذه الإستراتيجية وفقا للتغيرات التي تحصل في هذه التكنولوجية مما يستوجب توفر خطة عمل شاملة لأمن المعلومات وذلك بسهولة الفهم والإدراك من قبل أعضاء المنظمة.
- ضرورة وجود علاقة بين الجهات المسؤولة لضمان مشاركة جميع الأطراف بهدف تفعيل هذه المشاركة فمن الضروري جعل أمن المعلومات جزءا أساسيا من الوصف الوظيفي في المنظمة[1].
- إن تعدد جهات الاختراق لأمن المعلومات يتعذر معرفة الجهة الحقيقية من ورائها وهذه الجهات قد تكون أفراد عاملون في مهام الاستلام والتسليم أو المحققون الزائرون بهدف الاطلاع، المستشارون، العملاء والجواسيس المنافسين وغيرهم.
- تختلف جوانب التي تتعرض للاختراق باختلاف طبيعة المعلومات مثلا في المستشفيات يركز الاهتمام علي سجلات المرضى وفي التسويق تكون إستراتيجية التسويق هي المهمة.
- هناك أنواع عدة لخروقات أمن المعلومات منها طرق اختراق أمن المعلومات ومجالاته، طبيعة عرض المعلومات وطرق المستخدمة في معالجتها، تحديثها واسترجاعها، وكذا توصيلها إلي المستفيد والرقابة عليها.
- تدرج امن المعلومات في حالاتها الراهنة في اهتماماتها ونطاقه ويكمن اختصار هذا التدرج في أربعة مراحل موضحة في الجدول الأتي:

المرحلة	طبيعة التركيز	طبيعة الاهتمام

[1] - الطائي، الكيلاني، **مرجع سابق الذكر**، ص ص 42.

المرحلة الأولى	أمن تشغيل الأجهزة	الأمن يدور حول تحديد الوصول والاطلاع علي المعلومات من خلال منع الأفراد الغير مسرح بهم بالتلاعب بالأجهزة
المرحلة الثانية	أمن الحاسب ذاته	اتخاذ الإجراءات اللازمة لضمان أمن مواقع الحواسيب ومرافقها وإعداد التسهيلات المختلفة
المرحلة الثالثة	أمن البيانات	بعد الاستخدام الواسع للحاسب وتطبيقاته لابد من إقرار سياسة أمنية لحماية البيانات المختلفة
المرحلة الرابعة	أمن المعلومات	المحافظة علي سرية المعلومات وإتاحتها

الجدول (1-1)

مراحل تطور مفهوم أمن المعلومات وطبيعة اهتماماته

يوضح الجدول أن مفهوم أمن المعلومات يمر بمراحل تبين من خلالها البرامج الواجبة حمايتها والتي تضمن سلامة وسرية المعلومات والبيانات بشكل متدرج ومنظم.

ثانيا: مخاطر أمن المعلومات.

يتعرض أمن المعلومات إلي عدة مخاطر وتهديدات تؤثر سلبا علي مصادر المعلومات، حيث نلاحظ أن هذه التهديدات لا تكون الكترونية فقط بل يمكن أن تكون من طرف أحد أفراد المؤسسة أو بسبب حادث يؤدي إلي ضياع المعلومات، وفي هذا الصدد سنتطرق إلي ذكر عدة أنواع منها[1]:

أولا: خرق الحماية المادية: ويتم هذا الأسلوب عن طريق استخدام أربع تقنيات تساعد على خرق للمعلومات من طرف المهاجم فيتبع الأساليب التالية:

1- التفتيش في مخلفات التقنية (dumps ter diving): حيث يعتمد المهاجم في هذه التقنية على جميع مخلفات المؤسسة فيسعى جاهدا إلى إيجاد هذه المعلومات على مستوى المواد التي تركتها المؤسسة أو القمامة الخاصة بهم سعيا إلى العثور على ما يحتاجه وكذا استخدام مخرجات الكمبيوتر وكذا الأقراص التي تم الاستغناء عنها لتبديلها.

[1] - بن سليمان، بن عبد الله، **المرجع سابق الذكر**، ص23.

2- الالتقاط السلكي wiretapping: حيث يتم هنا استخدام التواصل السلكي مع الشبكة.
3- استراق الأمواج eavesdropping on émanations: يتم استخدام لاقطات لتجميع الموجات المنبعثة من النظم باختلاف أنواعها.
4- إلغاء الخدمة: وهنا يقصد به الأضرار والعوائق التي تمنع تقديم الخدمة المطلوبة.

ثانيا: خرق الحماية المتعلقة بالأنظمة داخليا وخارجيا:

إذ نجد أن الجهة الداخلية تمثل أكبر مشكل لدى المنظمة، حيث أن اختراق وكذا مختلف الهجمات التي مست المعلومات يكون داخل المنظمة، إذ نجد أن المهاجم ينتمي إلى المنظمة ويعمل في إطارها الداخلي مما يصعب تفادي هذا النوع فهو يمثل الخطر الأكبر لأي مؤسسة كانت، فمعظم تلك الهجمات ناتجة عن عدة أسباب ودوافع أدت بالفرد إلى شن هجوم ضد أنظمة المعلومات للجهة التي يعمل فيها، وتتمثل هذه الأسباب فيما يلي:

- **عدم الرضا**: فهذا السبب يرغم صاحبه باستخدام أساليب تضر المؤسسة التي يعمل فيها، حيث أن انتقامه يكون في تخريب نظم المعلومات لدى هذه الأخيرة مما يعطيه نوع من راحة الذات.
- استعراض مواهبهم وقدراتهم على استخدام عدة أساليب وكذا تمكنهم في اختراق الأنظمة والفخر بالمعرفة اليقنة لكن يحدث العكس فهذا الاختراق يؤدي إلى المساس بالنظام وكذا هشاشته.
- بغية تحقيق مكاسب مالية ضخمة من وراء الابتزاز بسرقة معلومات سرية وخاصة.

ثالثا: خرق الحماية المتصلة بالاتصالات والمعطيات:

1-هجمات المعطيات data attacks: في هذه العملية يتم التطرق إلي ثلاث برامج وهي[1]:
- **النسخ غير المصرح به للمعطيات unauthorized copying of data:** وهذه العملية ينتج عنها الدخول غير المصرح به للنظام، وذلك بالاستيلاء علي مختلف النسخ المتعلقة بالمعطيات وتتضمن المعلومات والبيانات والبرمجيات.
- **تحليل الاتصالات traffic analysis:** وفي هذه المرحلة يتم فيها التجسس على مختلف الاتصالات والارتباطات المرتبطة بالنظام، لإبراز نقاط الضعف لدى المستخدمين وممارسة مختلف أساليب الرقابة من اجل استخلاص فترة الهجوم المناسبة على حركة النظام.
- **القنوات المخفية covert channels**: حيث يقوم المهاجم هنا بإخفاء مختلف المعطيات والمعلومات التي تم الاستيلاء عليها في موضع معين من النظام، وتعتبر صور من اعتداءات التخزين.

2- هجمات البرمجياتsoftware attacks: في هذا النوع توجد عدة أساليب يتم بواسطتها الدخول إلى النظام ومحاولة تدميره وكذا الاحتيال عليه والعبث بمختلف الوظائف والمعطيات

[1] - الجنبيهي، **المرجع السابق**، ص24.

الخاصة به، وهذا الاختراق يؤدي إلى الاستيلاء على معظم البيانات وكذا الوصول إلى البرامج بطريقة تقنية ومن بين هذه الأساليب نجد أن الشخص يستخدم طرق تقليدية وبسيطة لتنفيذ احتياله كاستخدامه للبرمجيات الخبيثة والمضرة بالمعطيات، إضافة إلى نقل المعلومات عبر أنفاق النقل...الخ.

رابعا: الهجمات والمخاطر المتصلة بعمليات الحماية.

تسعى هذه العملية إلى شن مختلف الهجمات التي تضر بالنظام كالعبث بالبيانات ومحاولة تغييرها وخلق بيانات وهمية أثناء الإدخال أو الاستخراج، وكذا استخدام هجمات نشر الفيروسات على مستوى الانترنيت وإلهام المستخدمين بضرورة التقيد ببعض الخطوات من اجل حفظ بياناته وهذا الأسلوب شائع في مختلف استخدامات المؤسسات، إضافة إلى استخدام أسلوب المسح والنسخ الذي يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة مثلا: كلمة السر...الخ.

وهناك تصنيف آخر لمخاطر امن المعلومات وذلك لوجود عدة أنواع من البيانات والتي تحتاج إلي تخزينها وهذه البيانات في حد ذاتها معرضة للتهديدات وفقا لذلك نصنف الأخطار المحتملة التي تتعرض لها نظام المعلومات إلي[1]:

- الأخطار البشرية: تحدث هذه الأخيرة أثناء عملية البرمجة وتجميع البيانات وإدخالها للنظام وتمثل هذه الأخطار الغالبية العظمى في مشاكل الأمن والسلامة في المنظمة.
- الأخطار البيئية: والتي تتمثل في الكوارث الطبيعية كالزلازل والعواصف التي تتسبب في تعطيل تيار كهربائي ونشوب حرائق، زيادة إلى تعطيل أنظمة التبريد والتكييف وغيرها. وهذه الأخطار تسبب في توقيف التجهيزات لفترات طويلة بسبب الإصلاحات اللازمة.

الجرائم المحسوبة: تسبب خسارة كبيرة من خلال الاستخدام والوصول والتعديل لإدارة نظم المعلومات وقد تكون جريمة الحاسوب بريئة نسبيا مثل الاستخدام الغير مفوض للحاسبات أو خطرة كاستخدام الحاسبات لإرسال موجودات المنظمة لحساب منظمات أخرى وهي كالتالي: فيروسات الحاسب، القرصنة، جرائم الفضاء الرقمي.

- مشاكل جودة النظام: أن البرمجيات والبيانات الناقصة تسبب تهديدا لنظم المعلومات، وذلك يظهر في خسائر في الإنتاجية والخطر الغير مكتشف في برمجيات ائتمان المنظمة إضافة إلى أخطار البرمجيات وضعف البيانات.

ومن جهة أخرى نجد أن هناك تهديدات أحرى تمس شبكات أمن المعلومات، ويمكن حصرها فيما يلي[2]:

---

[1] - جبوري، **المرجع السابق**، ص 77.

[2] - زكرياء أحمد عمار، **حماية الشبكات الرئيسية من الاختراق والبرامج الضارة**، رسالة ماجستير(بغداد: كلية الدراسات العليا،2011)، ص34.

- **تهديدات غير منظمة:** تتشكل من أفراد غير متوقعين الذين يقومون بقرصنة شبكات الانترنت بأدوات كسر كلمات المرور والنصوص المغلفة، إن تشغيل أدوات القرصنة تعد مصدر خطر للشبكة وتزداد بزيادة مهارة هؤلاء الأفراد في امتلاكهم أدوات مستخدمة للقرصنة.

- **تهديدات منظمة:** تكون بسبب تنافس تقني من طرف قراصنة يعرفون ثغرات نظم التشغيل بفهم وتطوير واستخدام تقنيات القرصنة المعقدة وذلك باختراق مؤسسات والشركات غير محمية وهذه الجماعات غالبا ما تتعلق بقضايا السرقة والاحتيال.

- **تهديدات خارجية:** تأتي من طرف أفراد خارج المنظمة عن طريق دخولها الشبكات من طرف الانترنيت أو خطوط الهاتف.

- **تهديدات داخلية:** وهنا بامتلاك الشخص حق الوصول إلى شبكة المنظمة أو بامتلاكه حق الدخول الفيزيائي لاماكن وجود أجهزة و معدات الشبكة.

ويمكن حصر ثلاث نقاط ضعف أساسية تزيد من تهديدات أمنية لنظام المعلومات وهي:

- نقاط ضعف تكنولوجي.
- نقاط ضعف الإعدادات.
- نقاط الضعف في سياسات الحماية.

يمكن القول أن المخاطر التي تتعرض لها أمن المعلومات متعددة وذلك لتعدد المعلومات، وتزايد نسبة الاختراق بزيادة أهمية المعلومة وكلما كانت المعلومة ذات أهمية كان الاختراق أكثر توسعا في النظام.

المطلب الرابع: إستراتيجية أمن نظام المعلومات.

لكل نظام معلومات استراتيجيات تبين مدى الحماية الفعلية لبياناتها وذلك بالاعتماد على أسس و المتمثلة في[1]:

1- تقييم أهمية المعلومات من اجل حماية أفضل لها: إن عناصر نظام المعلومات ليس لديها نفس الطريقة في الحماية، ولحماية كامل المعلومات في نفس المستوى يتطلب مخرجات باهضة ولهذا فان النظام المعلوماتى يعمل على تشخيص المعلومة قبل وضع أسس حمايتها، والهدف هو إيجاد توافق بين الوسائل من أجل حماية أنفسنا من التهديدات.

2- كيفية تحديد ما يجب أن يكون محمي: يجرد أجزاء النظام (الأجهزة المستعملة والتطبيقات المتوفرة) أي ليسهل على مسير المؤسسة من درايته بمدى انتشار معلومات في

[1] - معوج، **مرجع سابق الذكر**، ص 248.

مؤسسة وذلك كخطوة أولى نحصر الموارد الداخلية للمؤسسة بما في ذلك البريد الالكتروني والبيانات الهامة وموارد الشركة المستغلة والممتلكة من طرف موفر خارجي والمستغلة من قبله لصالح المؤسسة.

3- ترتيب المعلومات حسب قيمتها: تتكون المعلومات من معلومات سرية ومعلومات عامة، وتقسيمها مترتب على مالك المعلومات أو الإدارة العليا ولترتيب المعلومات وضعنا محددات تبين لنا مدى سرية المعلومات وهي كالتالي:

- فائدة المعلومات.
- أهمية وقيمة المعلومات.
- حجم الخسائر التي قد تلحق بالمنشأ عند كشف المعلومات وكذا عند حدوث تعديل أو تلف فيها.
- مختلف القوانين واللوائح الخاصة بحماية المعلومات.
- هل حقا المعلومات تؤثر بالأمن القومي؟
- من المصرح باستخدام الانترنيت؟
- من سيقوم بصيانة المعلومات وكيف ستحفظ وأين؟
- من المسئول عن إعادة إصدار المعلومات؟
- أي نوع من المعلومات يحتاج إلى تصنيف خاص؟[1]

4- تقييم المخاطر: هذه المرحلة تقوم على تحديد كافة التهديدات والاحتمالات التي تحدث ضرر، وتشمل هذه المخاطر الداخلية والخارجية إذ تقوم بدراسة مدى التأثير الذي تحدثه وكذا تكلفة الأضرار التي تسببها سواءا لنظام المعلومات أو للمؤسسة[2].

5- بناء سياسة أمن ملائمة: نجد أن هذه السياسة تقوم على عاملين ألا وهما: تحديد المبادئ الرئيسية وكذا تامين نظام المعلومات:

أ- تحديد المبادئ الرئيسية: تقوم على تحديد ثلاث أهداف وإبراز فعاليتها:

- تكامل نظام المعلومات الذي يعطى دقة وتكامل المعلومة إضافة إلى حسن التشغيل.
- ضمان الوصول إلى البيانات بسرية تامة.
- توافر نظام المعلومات الذي يقوم على تحديد مختلف الموارد المتوفرة عند الحاجة لان السياسة الأمنية لابد أن تعطى تحديدا هام لإبعادها،أي تحديد أبعادها الثلاث: البعد الاستراتيجي التنظيمي والتقني فهي تساهم في تحديد طريقة العمل وكذا تقسيمه إضافة إلى الوسائل المعتمدة لضمان الحماية.

[1] - معوج، **مرجع سابق الذكر**، ص 248.
[2] - المرجع نفسه، ص 248.

ب- تأمين نظام المعلومات: يقوم على وضع تدابير وقائية سواءا المتعلقة بالأدوات المستخدمة أو سلوك المستخدمين، وقبل اللجوء إلى هذه التدابير لابد من المؤسسة أن تثبت مدى قدرتها على تنفيذ نشاطها، وإبراز الحد الأقصى لمقدار المعلومات التي تضيع دون المساس بنشاطها.

وكذا ما هي المدة المستغرقة لاستعادة نشاطها دون المساس بأداء المؤسسة وهذا يبين قدرة المؤسسة على حماية معلوماتها وكذا كيفية استعادتها في حالة حدوث أي خطر.

ج- التدابير الوقائية: يضمن عدم انقطاع النشاط وذلك بتحديد وتيرة ونوع النسخ الاحتياطي لكل فئة من المعلومات، إضافة إلى توفير الأدوات اللازمة والأساسية للحماية والتي تشمل مكافحة الفيروسات، مكافحة البريد المزعج، إضافة إلى استخدام عدة تقنيات تضمن الوصول إلى البيانات عن طريق كلمة السر.

د- التدابير العلاجية: وهذه التدابير تستخدم حين كوارث فهي تساعد على استعادة النسخ الاحتياطي الأخير إضافة إلى تشغيل التطبيقات وإعادة تشغيل الآلات، فا لتدابير الوقائية معرضة دائما لخطر محدق بها مما ينجم عنه استخدام هذه التدابير.

6- التوازن بين مرونة الوصول وصلابة الحماية: تتطلب الحماية الأمنية تحدي وجهد ومال، ويقع على مهندسي الشبكات مسؤولية إدارة سياسات الأمان إذ نجد أن مدراء الشبكات يسعون للوصول إلي الشفافية وذلك عن طريق الأخذ بالقضايا التالية استمرارية الاتصال والأداء، سهولة الاستخدام وقابلية الإدارة والتوفر، كما يجب على مسؤولي الشبكات الالتزام بالصفات المحفزة على أداء واجباتهم والمتمثلة في إثبات الشخصية وكذا التحلي بروح المسؤولية والخصوصية وضمان سلامة البيانات.

ومن جانب آخر تقوم العناصر الرئيسية لحماية الشبكة أمنيا بالاستخدام الناجح لتقنيات الشبكات لحماية البيانات من الاختراق وتتضمن حلول الحماية لهذه الشبكات على خمسة حلول وهي التعريف بالهوية، حماية الحدود وسرية البيانات إضافة إلي إدارة السياسات وإدارة الحماية الأمنية[1].

7- التوعية بالحماية الأمنية: تعتمد هذه الخاصية على تدريب المستخدم وتعليمه على أساسيات الحماية الأمنية المتبعة في المنظمة حيث يشمل هذا التدريب على كيفية تصميم وتركيب أنظمة الشبكات وصيانتها ويتضمن مناهج التدريب على المعلومات ومختلف التقنيات التي تتماشى مع تطور أجهزة الشبكة وكذا أنظمة تشغيلها، كما تنص أيضا على توعية الأفراد المسؤولين عن أمن الشبكات بضرورة التقيد بحماية المسائل المهمة في

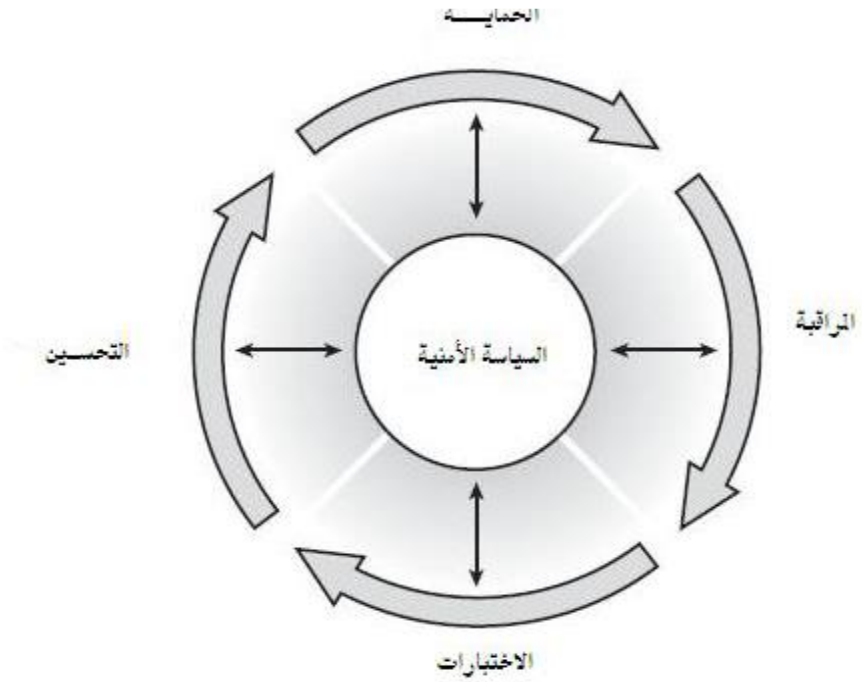
[1] - زكرياء أحمد عمار، **مرجع سابق**، ص 26.

المنظمة والالتزام بإتباع قواعد سياسات الحماية قبل توصيل الشبكة المحلية للمنظمة بالمركز وتتمثل هذه القواعد في[1]:

- اختيار المعايير والخطط اللازمة لتنفيذ الضوابط الأمنية.
- التنبأ بالمخاطر الممكنة واتخاذ التدابير المناسبة للحماية الأمنية.
- توفير التدريب الكافي للمستخدمين.
- تبني سياسة أمنية موحدة و موثقة.
- تعزيز استخدام ضوابط تنزيل البرامج.
- وضع خطة طوارئ لاستعادة البيانات عند حدوث كوارث.

8- عجلة الحماية الأمنية: تستخدم هذه العجلة للتأكد من وجود الإجراءات اللازمة للحماية وإدراك مواطن الضعف، حيث تلعب هذه العجلة دورا مهما في تطبيق التشغيل التجريبي للتحديثات ووصولها إلي تشغيل نهائي ينبع عنه الإنتاج المستمر، حيث يرتكز محور العجلة على السياسة الأمنية أما إطاراتها تتمحور في أربعة أقسام وهي الحماية والمراقبة والاختبارات والتحسين، إذ لا يتم دوران العجلة إلا إذا تم تطوير سياسة الحماية التي تتناول تحديد كافة متطلبات المؤسسة بطريقة متكاملة كتحديد هدف والغرض من الحماية وكذا توثيق مواردها ومعرفة مختلف مخططات برامج المؤسسة ومخازنها.

الشكل رقم (4-1): عجلة الحماية الأمنية



[1] - عمار، **المرجع نفسه**، ص ص 30-38.

المصدر: زكريا أحمد عمار، **حماية الشبكات الرئيسية من الاختراق والبرامج الضارة،** رسالة ماجستير (بغداد: كلية الدراسات العليا،2011)، ص39.

يوضح لنا الشكل أن السياسة الأمنية في تطور مستمر إذ لابد من معرفة أجزاء هذه السياسة لإدراك طريقة تبنيها وتشغيلها حيث من الضروري البدء بوضع خطة للحماية قبل إجراء أي عمل وإعداد كافة التجهيزات الملائمة ثم وضع مراقبة عليها وبعدها إجراء اختبار تجريبي لضمان سلامة هذه التقنية ونجاحها وفي الأخير يتم القيام بتحسين هذه الطريقة ومعالجتها ليتم عرضها واستخدامها على الواقع العملي والتنظيمي[1].

المطلب الخامس: معايير أمن المعلومات.

تسعى كل منظمة إلي ضبط الأحكام المتعلقة بأمن المعلومات وذلك باستخدام معايير ذات صلة والتي تتيح الحماية السرية وكذا توفر المعلومات ونظم المعلومات، إذ تجدر الإشارة إلي أن تطور تكنولوجيا المعلومات يؤدي إلي تزايد المعايير وسنستعرض بعض من هذه المعايير المستخدمة على نطاق واسع وهي كالتالي[2]:

- مجموعة (ISO 27000) تعتبر من المعايير المهمة في إدارة أمن المعلومات والتي تم تحديثها من قبل المنظمة الدولية للمعايير

- سلسلة وثائق (NIST SP 800) وهذه الوثيقة تم نشرها من شعبة أمن الحاسبات التابعة لمعهد الوطني الأمريكي للعلوم والتكنولوجيا وتتألف هذه السلسلة من مائة وثيقة.

- مكتبة البنية التحتية لتكنولوجيا المعلومات (TTIL) تهدف إلي تحسين الأنساق مع العمليات التي طبقت ونفذت، ويستخدم (TTIL) في نطاق واسع وفي جميع أنحاء العالم كما ساهمت في تطوير المعايير الدولية (ISO 20000) على إدارة خدمة تكنولوجيا المعلومات.

- رقابة تكنولوجيا المعلومات (COBIT) الصادرة عن معهد حوكمة تكنولوجيا المعلومات (ITGI) وجمعية تدقيق نظم المعلومات (ISACA) هدفها تغطية نطاق الحوكمة والتخطيط والتنظيم إضافة إلي نشر الإصدار الخامس من (COBIT 5) عام 2012 ويتضمن على منشورات منفصلة ومخصصة لأمن المعلومات.

- هيئة إدارة البيانات للمعارف (BMBOK) حيث تتعامل هذه الهيئة مع جميع جوانب موارد البيانات حيث تبنى هذه الهيئة تحت ظل مراعاة إستراتيجية أمن المعلومات للمنظمة وثقافتها.

[1] - الطائي، الكيلاني، **مرجع سابق**، ص 104.

[2] - المرجع نفسه، ص 104.

وفي الأخير نستنتج أن تنفيذ هذه البنود والقوانين يتم من خلال تحسين مستوى الموظف وتدريبه على مختلف الأجهزة والإمكانيات المستخدمة في تنفيذ وظيفته والتماشي مع مختلف التغيرات التي تطرأ داخل المؤسسة وضمان التحسين المستمر.

خلاصة الفصل:

لقد حاولنا في هذا الفصل إلى إبراز مكانة نظام أمن المعلومات الذي يعد من أهم التقنيات الحديثة التي يجب على كل مؤسسة تبنيها والسير في نمطها فهذا الأخير يقوم بتقييم مدى كفاءة وفعالية المؤسسة داخليا، إضافة إلى الأساليب والخطوات اللازمة اعتمادها لضمان الحماية الكاملة لمختلف البيانات والمعلومات الخاصة بالمؤسسة، ومع تعدد أساليب القرصنة والاستيلاء على مختلف المعلومات المحمية لمؤسسة ما، توجب خلق امن دائم وشامل لتفادي الهجمات المباغتة من طرف قراصنة الانترنيت وتتزايد المخاطر من فقدان العديد من المعلومات في المؤسسات في ظل تزايد واكتشاف وسائل خرق جديدة للمواقع الرسمية والأمنية ورغم الجهود المبذولة من طرف أنظمة الحماية للمعلومات إلا أن هناك طابع قرصني في مختلف المواقع.

إن الحديث عن المعلومات يستوجب ذكر شموليتها سواءا في المجال الإداري أو مجالات أخرى، ونظام المعلومات نظام مركزي خاصة في المؤسسات والمعلومة هي لب المعرفة الحقيقية للأشياء فوجود المعلومة يعنى سهولة التقيد بنظام البحث لأي ميدان كان.

الفصل الثاني
الجهود الدولية والجزائرية في مجال نظام أمن المعلومات

تمهيد:

لقد أصبح اختراق أنظمة المعلومات خطرا يقلق العديد من المنظمات، فرغم تنوّع أساليب الحماية التي تنتهجها هذه الأخيرة إلا أن هناك ارتفاعا محسوسا في معدل الاختراقات باختلاف وسائله المستخدمة أما عن طبيعة الأخطار التي تواجه نظم المعلومات فنجدها عديدة ومتنوعة فقد تكون مقصودة كسرقة المعلومات أو غير مقصودة كالكوارث الطبيعية والأخطاء البشرية.

لذا نجد أن أمن المعلومات له دورا كبيرا لكل المؤسسات الحكومية منها أو الخاصة وقد أصبح ضرورة ملحة في ظل التطورات المستمرة في تقنية المعلومات وما صاحبه منتطورات أخرى تخص أساليب اختراق البيانات لذا حرصت العديد من المنظمات العالمية والوطنية لوضع معايير وقوانين تساهم في ضبط أمن المعلومات بالمؤسسة.

ومن هذا المنطلق سنقوم في هذا الفصل إلي إبراز مختلف السياسات والتوجيهات التي تتضمنها هذه المعايير والتي تساهم في تطوير إدارة نظام امن المعلومات في المؤسسة لضمان الحماية الأفضل لنظامها وسلامته لذا تم تقسيمه إلي مبحثين هما:

المبحث الأول: الجهود الدولية في مجال أمن المعلومات.

المبحث الثاني: الجهود الجزائرية في مجال أمن المعلومات.

المبحث الأول: الجهود الدولية في مجال أمن المعلومات.

إن التطور الهائل الذي مس جميع وسائل الإعلام وتقنيات المعلومات صاحبه ظهور مهددات جديدة ومتنوعة في الساحة العلمية والعملية والمرتبطة بأمن المعلومات والذي يدعو إلى أخذ التدابير اللازمة لأمن نظم المعلومات للحد من انتشار الجرائم والمخاطر الالكترونية، لهذا قامت منظمة المقاييس الدولية ISO بتطوير سلسلة متخصصة بحماية المعلومات وهي ISO 27001 والتي يطلق عليها نظم إدارة حماية المعلومات.

المطلب الأول: مفهوم المواصفة الدولية ISO 27001.

1- تعريف المواصفة الدولية الايزو:

الايزو ISO: هي منظمة دولية للتوحيد القياسي تأسست عام 1947 وهي شبكة تصدر عنها مواصفات دولية في العديد من المجالات، تضم أكثر من 110 دولة، يوجد مقر المنظمة في جنيف بسويسرا ومهمتها التنسيق للنظام بأكمله ويتم نشر ما يقارب 1,100 مواصفة ايزو سنويا[1].

المواصفة الدولية ISO 27001: تقوم بتحديد متطلبات إنشاء وتطبيق ومراقبة وتحسين نظام إدارة أمن وسرية المعلومات من خلال مخاطر العمل التي تتعرض لها المؤسسة إذ تسعى إلي تطبيق هذه المتطلبات بما يتماشي مع احتياجات تلك المؤسسة حيث يمكن أن تطبق هذه المواصفة من أية جهة مهما كان نشاطها وعملها، حيث صممت هذه المواصفة بغية إرساء الضوابط الأمنية الملائمة والتي تحمي الأصول المعلوماتية لكل مؤسسة، ومن أبرز الجهات المستفيدة نجد البنوك والشركات الصناعية والتجارية وحتى الجهات الحكومية والعسكرية[2].

مواصفة ISO27001 : تقوم بتزويد المنظمات الصناعية والخدمية بتوجيهات لتطبيق نظم إدارة حماية المعلومات، والتي تشتغل طبقا لمتطلبات المعايير الدولية، إذ تمس هذه المواصفة أصول المؤسسة من هيكل تنظيمها والسياسات المنتهجة إضافة إلي مصادر المعلومات الخاصة بالمؤسسة وكذا مختلف الإجراءات التي تتخذها[3].

تعتبر المواصفة الدولية 27001 الصادرة عن المنظمة الدولية للتوحيد القياسي ISO في عام 2005 تطوير للمواصفة البريطانية BS7799 الهادفة للحفاظ على أمن وسرية المعلومات، وفي عام 2013 تم إدخال بعض التعديلات وإبراز متطلبات جديدة تتماشى مع التقدم التكنولوجي الذي طغى على الأجهزة الالكترونية وكذا البرامج والتقنيات المتبناة لمساعدة

---

[1] - نظم إدارة الجودة"، في: **http¡//www.gcKw.com/ISO-FAQS-AR.asp ? SPID=67**، (2017/07/24).

[2] - الشريف بوفاس، فاطمة الزهراء طلحي، "نحو بناء نظم لإدارة حماية المعلومات في المؤسسات الجزائرية"، **المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقظة الإستراتيجية ونظم المعلومات في المؤسسة الاقتصادية**، أيام 30/29 أفريل 2014، جامعة باجي مختار عنابة، ص7.

[3]- بوفاس، طلحي، **نفس المرجع السابق.**

المنظمات على الإنشاء والمحافظة على نظامها، إذ صدرت عن منظمة الايزو مجموعة من معايير أمن المعلومات والتي تدعى مواصفات نظم إدارة أمن المعلومات ايزو 27000 والتي تتكون من ستة معايير فرعية وهي:

-27001: المتعلقة بالأسس والمفردات.

- 27002: قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات.

- 27003: دليل تنفيذ إدارة أمن المعلومات.

- 27004: قياس فعالية نظم إدارة أمن المعلومات.

- 27005: إدارة مخاطر أمن المعلومات.

- 27006: دليل لعملية المصادقة على نظام إدارة أمن المعلومات[1].

- ايزو27001: هو نموذج دوري يعرف بـ **PDCA** وهو اختصار ل -plan-do-check Act يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وتوثيق نظام إدارة امن المعلومات داخل المنظمة، إذ نجده عادة ينطبق على جميع أنواع المنظمات حيث يمر هذا النموذج بأربع مراحل متتابعة:

أ- الخطة (plan): تعني تأسيس نظام لإدارة أمن المعلومات.

ب- التنفيذ (Do): وهو البدء في تنفيذ الخطط وتشغيلها.

ج- التحقق (check): أي مراجعة النظام بعد تنفيذه.

د- العمل (Act): صيانة وتحسين النظام[2].

معيار ايزو 27002: أصدر أيضا هذا المعيار في 2005 واهتم بالتطبيق الفعلي للأسس والقواعد التي تم إعدادها بواسطة المعيار السابق أي أن هذا المعيار بمثابة الخطوط التي يجب الالتزام بها بعد مرحلة التطبيق وذلك بهدف حماية الأصول التكنولوجية وتوفير الأمان لها وكذلك محاولة تجنب الوقوع في مخاطر التشغيل الالكتروني[3].

وفي الأخير نستنتج أن معيار الايزو27001 هو معيار متكامل يسعى لبناء نظام أمن معلومات فعال ومستمر يتماشى مع التطورات الحاصلة، وقابل للتقييم مرتين في السنة إذ يعطى مزيد من الثقة بالجهة المعنية حول سلامة وسرية المعلومات.

---

[1]- أحمد عبادة العربي،" معيار المنظمة الدولية للتوحيد القياسي ايزو27002(ISO/IEC27002) لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية"؟، **مجلة جامعة طيبة للآداب والعلوم الإنسانية**، م(4)، ع(7) (2014)، ص279.

[2]- منتديات اليسير للمكتبات وتقنية المعلومات، "المعايير العالمية لأمن المعلومات"، في:

http://www.alyaseer.net/Vb/Shouwthread.php ?t=25671، **(** 2017/07/29).

[3] - سامح رفعت أبو حجر، أمنية محمد عبد العزيز،"دور آليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر أمن المعلومات للحد من التلاعب المالي الالكتروني في الوحدات الالكترونية "في:

http://www.Kantakji.com/media/175569/%D8%AF/%D9%88%D8%B1-%D8%A2% D9% 84% D9% ...(2017/08/02**)**

المطلب الثاني: أبعاد ومميزات تطبيق المواصفة القياسية.

I. مميزات معيار امن المعلومات:

تعد ISO 27001 مواصفة متقدمة تقوم بتلبية متطلبات المنظمة وذلك من خلال إقامة نظام إدارة أمن المعلومات، حيث تعتبر أيضا مدخلا للتحسين المستمر للنظام ككل إذ نجد أن هذه المواصفة تملك مميزات تبين كيفية تطبيقها للحصول على نظام امن معلومات فعال ومتطور يمتاز بالسرية وهي كالتالي[1]:

- ✓ الموافقة مع متطلبات الرقابة للحفاظ على امن المعلومات.
- ✓ وضع تخطيط فعال للضوابط الداخلية والتي يتناسب مع بيئة الأعمال وحجم نشاط المنظمة.
- ✓ بناء سياسات وإجراءات موثقة على أساس تقييم المخاطر ووضع نظم لمعالجة المخاطر المتوقعة.
- ✓ التقليل من تكاليف إعادة الإنشاء إذا تعرضت المعلومات للاختراق والفقدان.
- ✓ تجسيد وحدات تنظيمية ذات سياسات متكاملة وموحدة بشأن التعامل مع إدارة أمن وسرية المعلومات.
- ✓ نشر الوعي لدى الموظفين في إطار إنجاز الأعمال بمفهوم إدارة أمن المعلومات.
- ✓ التميز بالكفاءة و الفعالية في تشغيل إدارة نظم المعلومات.
- ✓ ضمان الاستمرارية في العمل في حالة وقوع الأزمات.
- ✓ الاعتماد على ضوابط أمنية مناسبة لحماية المعلومات.
- ✓ زيادة الثقة بين الموظفين في إطار إنجاز الأعمال.

يتسم معيار ISO بالسهولة في كشف مختلف البرمجيات المصابة والمعدية والمضرة بالمؤسسة كما يميز بين النظم الموجودة فيها وأن كل منظمة تطبق نظام خاص بها كما يتسم بمنهجية سليمة تدعو إلى زيادة الثقة بالمؤسسة.

II. أبعاد المواصفة القياسية ISO27001:

يحتوى معيار أمن المعلومات ISO27001 على 12 فصلا والذي يشمل على 39 معيارا رئيسيا و133 معيارا فرعيا إذ نجد أن هذه المعايير تقوم على أربعة عناصر رئيسية وهي:

[1] - شهادة الأمن و السلامة ISO 27001، في:-**http://www.iehad.com/index.php/2011-10-03.12-05-37.html. 36/2012-06-21-22-31-**، (2017/08/09).

- تبين أهداف المعيار الأساسية الموجودة داخل المؤسسة.
- تبرز كمية الضوابط المحققة لأهداف المعيار.
- تقدم معلومات مفصلة وتوجيهات تدعم تطبيق الضوابط.
- إعطاء معلومات إضافية تكون مفيدة كالمعلومات القانونية[1].

الجدول رقم (1-2) يوضح المعايير الرئيسية والفرعية لمعيار27001 لسياسات أمن المعلومات.

الفصول	عناوين الفصول	عدد المعايير	
		الرئيسية	الفرعية
الفصل الأول	تقييم المخاطر و معالجتها	مقدمة نظرية	
الفصل الثاني	السياسة الأمنية	1	2
الفصل الثالث	تنظيم أمن المعلومات	2	11
الفصل الرابع	إدارة الأصول	2	5
الفصل الخامس	أمن الموارد البشرية	4	21
الفصل السادس	الأمن المادي والبيئي	2	13
الفصل السابع	إدارة العمليات والاتصالات	10	32
الفصل الثامن	التحكم في الوصول	7	25
الفصل التاسع	اقتناء وتطوير وصيانة نظم المعلومات	6	16
الفصل العاشر	إدارة الحوادث الأمنية للمعلومات	2	5
الفصل الحادي عشر	إدارة استمرارية الأعمال	1	5
الفصل الثاني عشر	الامتثال و التوافق	3	10
الإجمالي	**12**	**39**	**133**

المصدر:أحمد عبادة العربي،"معيار المنظمة الدولية للتوحيد القياسي (ISO/IEC27002) لسياسات أمن لمعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية"، **مجلة جامعة طيبة للآداب والعلوم الإنسانية**، م(4)، ع(7)(2014) ص280.

من خلال هذا الجدول سنقوم بعرض أهم معايير ايزو 27001 وأبرز التوصيات والضوابط التي تتشكل كل منها.

1- تحليل المخاطر ومعالجتها: يقوم هذا الفصل بإعطاء كيفية تقدير حجم المخاطر وتحديد أثرها إذ يتم هذا التقييم بشكل دوري بغية معالجة الثغرات الأمنية الحاصلة في المتطلبات

[1] - أحمد عبادة العربي ، **مرجع سابق الذكر**، ص280.

الأمنية وأهم الضوابط التي جاءت في هذا الفصل خاصة بمعالجة مخاطر الأمن وتتمحور في[1]:

- تقليص المخاطر بتطبيق الضوابط اللازمة.
- التوافق مع القوانين المحلية والدولية.
- ضوابط التشغيل.
- الموازنة بين تطبيق وتشغيل الضوابط والأخطار المتوقع حدوثها من الثغرات الأمنية.

2- السياسة الأمنية: تسعي هذه السياسة إلي تقديم التوجيه والمساندة والتوصية إداريا وتتمثل توجيهات التطبيق في[2]:

- إنشاء منتدى لأمن المعلومات على مستوى الإدارة العليا في المنظمة.
- تقديم حملات وبرامج للتوعية والتدريب على أمن المعلومات.
- ضرورة وجود وثيقة عامة لسياسة أمن المعلومات تتضمن رؤية المنظمة لإدارة أمن المعلومات وكذا حاجة هذه المنظمة إلي خطة طوارئ وتعميم هذه الوثيقة على جميع الأطراف المنسوبين للمنظمة سواء الجهات الخارجية أو الداخلية منها مع ضرورة تحديد الإجراءات اللازمة اتخاذها عند وجود خلل في نشاط ما يؤدى إلي عدم التوافق مع السياسة.

3- تنظيم أمن المعلومات: يهدف هذا البعد إلى تنظيم وإدارة أمن المعلومات داخل المنظمة من حيث موافقة الإدارة العليا على الوثيقة وتحديد الأدوار والمسؤوليات أما من الناحية الخارجية تكون عن طريق التعاقدات[3]، حيث يتكون معيار التنظيم الداخلي من 8 معايير فرعية أما التنظيم الخارجي فله 3 معايير فرعية والجدول الآتي يوضح ذلك:

---

[1]- أحمد عبادة العربي ، **مرجع سابق الذكر**، ص 281.

[2]- محمد محمد الهادي،" توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية "، في: **http://www.cybrarians.info/journal/n...o-Secuirty.htm**، (2017/08/16).

[3]- محمد محمد الهادي، **نفس المرجع.**

الجدول رقم (2-2): المعايير الفرعية لمعيار تنظيم أمن المعلومات.

التنظيم الداخلي لأمن المعلومات	التنظيم الخارجي
- التزام الإدارة العليا بأمن المعلومات - التنسيق بين الإدارات العليا بأمن المعلومات - تحديد المسؤوليات - ترخيص مراجعة أمن المعلومات - الاتفاقية السرية - التواصل مع الجهات المختصة - التواصل مع الجهات ذات العلاقة - المراجعة الدورية لأمن المعلومات	- تحديد المخاطر ذات الصلة بالأطراف الخارجية - المعالجة الأمنية عند التعامل مع العملاء - المعالجة الأمنية عند التعامل مع الأطراف الخارجية

المصدر: أحمد عبادة العربي، "معيار المنظمة الدولية للتوحيد القياسي (ISO/IEC27002) لسياسات امن لمعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية"، **مجلة جامعة طيبة للآداب والعلوم الإنسانية**، م(4)، ع(7)(2014) ص286.

4- إدارة الموجودات(الأصول): يعمل هذا البعد على إدارة كل ما يتعلق بأصول المعلومات سواءا كانت طبيعية أو فكرية حيث يتم فيه تحديد ملكية كل أصل وكذا توثيقه لصيانة أصول المنظمة مع الاستخدام الأمثل للمعلومات (تصنيف المعلومة حسب قيمتها وحساسيتها)، مع تقديم الحماية الملائمة لمصادرها[1].

5- أمن الموارد البشرية: يهدف هذا الفصل إلى التقليل من المخاطر الناجمة عن الأخطاء البشرية وتقوم إدارة الموارد البشرية بتقييم أداء العاملين في المنظمة بصورة أكثر فاعلية بتحديد مسؤولياتهم وبأنهم مناسبون للأدوار المقدمة لهم بالإضافة إلى توفير قدر كافي من الوعي والتدريب في إطار المسؤوليات الأمنية المحددة لكل العاملين ضمن مواقعهم في التنظيم.

[1]- سعيد بن محمود الزهراني، "المواصفة القياسية ISO27001"، **مجلة عالم الجودة**، ع(3) (أوت 2011)، ص11.

6-الأمن الطبيعي والبيئي: يساهم هذا البعد في تأمين المناطق المادية (تسهيلات معالجة المعلومات، تأمين وسائل حفظ المعلومات، مناطق الشحن والتسليم)، وبيئة العمل داخل المنظمة في إدارة أمن المعلومات بصورة أمنة(حماية المعدات وأجهزة المنظمة من أية أخطار)، لأن كل عنصر يقع ضمن نطاق المنظمة من التسهيلات والعاملين والزبائن يؤدي دورا مهما في نجاح عملية حماية أمن المنظمة.

7-إدارة العمليات والاتصالات: يقوم هذا الفصل بوضع إجراءات تشغيلية لجميع مرافق تجهيز ومعالجة المعلومات، ووضع ضوابط لرصد وتوثيق خدمات المعلومات الآتية من المنظمات الخارجية، وتوفير الحماية من البرامج الخبيثة مع وضع سياسات تحذر من استخدام البرامج الغير مصرح بها مع ضرورة امتلاك نسخ احتياطية منها وكما تقوم بإدارة العمليات اليومية بصورة آمنة للاستخدام الأمثل لوسائل تشغيل الشبكات و البيانات.

8-السيطرة على الدخول: إن التحكم في عمليات وصول أو دخول العاملين للنظام يعتبر أمر ضروري ورئيسي في حماية معلومات المنظمة وتفادي اختراق الشبكات والبرامج ويكون ذلك بإتباع إجراءات رسمية لتسجيل المستخدمين وطرق آمنة لاختيار كلمات المرور والحفاظ على سريتها مع استخدام أسلوب دقيق وآمن لتوثيق هوية المستخدمين لتسهيل الوصول إلى نظم التشغيل على الأفراد الذين تم اختيارهم وفقا لطبيعة وظائفهم.

9-تطوير أنظمة أمن المعلومات وصيانتها: يهدف هذا البعد إلى تأكيد الأمن في نظم المعلومات والعمل على توفير متطلبات المحافظة عليها وصيانتها وذلك بتفادي انتشار الخسائر والأخطاء ومنع سوء استخدام المعلومات مع ضمان حمايتها وصحتها وسلامتها من خلال إقامة برامج التشفير لضمان أمن ملفات النظام والحد من وجود ثغرات أمنية ومراقبة نقاط الضعف التقنية.

10-الإدارة العرضية: يساعد هذا البعد على مواجهة الحالات الطارئة بتحديد مواقع الضعف في إدارة امن المعلومات كما تقدم الحلول اللازمة من خلال بناء نظام اتصال فعال بين المستويات التنظيمية المختلفة إضافة إلى تحديد مختلف الإجراءات والمسؤوليات لمعرفة كيفية التعامل مع حوادث أمن المعلومات والاستفادة منها مستقبلا وتتضمن الإبلاغ عن حوادث أمن المعلومات وإدارتها[1].

11-إدارة استمرارية الأعمال: يسمح بوجود مرونة مناسبة تقوم على مواجهة حالات الكوارث الطبيعية وحالات الفشل والأنشطة التي تعرقل سير العمل في المنظمة، كما تساعد في حماية نظم المعلومات من الأعطال الرئيسية كما تضمن إعادة تشغيل النظام في الوقت المناسب.

[1]- الزهراني، **المرجع السابق.**

12-إدارة الالتزام والتوافق: يسعى هذا البعد إلى تجنب أي ثغرات أو اختراقات للقوانين والتشريعات المدنية أو الجنائية وكذا الأنظمة والالتزامات التعاقدية ومتطلبات السياسات الأمن التنظيمية وفعاليات مراجعة النظام ومختلف الإجراءات الأمنية.

المطلب الثالث: خطوات تطوير نظام امن المعلومات حسب المواصفة القياسية.

يقوم معيار ISO 27001 بحماية المعلومات وذلك حسب متطلبات معينة يجب على المؤسسة تلبيتها للحصول على هذه الشهادة، فنجد أن نظام أمن المعلومات يخضع لأربع مراحل (التخطيط، التنفيذ، التحقق، المعالجة) تساهم في تطوره واستمرارية عمله ونوضحها كما يلي[1]:

1) تكوين لجنة أمن المعلومات: تقوم هذه اللجنة بتحقيق عدة متطلبات وهي:

- السعي إلى تطوير السياسة العامة لأمن المعلومات واعتمادها.
- التأكد من تطابق أهداف أمن المعلومات بأهداف المنظمة.
- إدارة المصادر الخاصة بإدارة أمن المعلومات.
- إعطاء تقييم شامل ونتائج صحيحة حول المخاطر ومدى تأثيرها على العمل.
- تطوير أساليب معالجة المخاطر.
- حسن إدارة و تنفيذ خطط معالجة المخاطر.
- ضمان تحقيق التطور لنظام إدارة أمن المعلومات في المؤسسة.
- التعامل مع الأزمات والأحداث بصورة أمنية وضمان السلامة الأمنية للمعلومات والبيانات داخل المؤسسة عند حدوث أي اختراق.

2) أعضاء اللجنة:

تطالب اللجنة بالدعم المباشر من الإدارة العليا وذلك لتفعيل نظام امن المعلومات، كما يستوجب أن يترأسها مدير تنفيذي حيث تتكون اللجنة على أعضاء أصحاب قرار في المنظمة لهم علاقة وطيدة بإدارة المعلومات والأعمال ومثال ذلك: عضو من الشؤون الإدارية والمالية، عضو من تقنية المعلومات وعضو من أمن المعلومات، عضو من إدارة شؤون الموظفين وإدارة الجودة، حيث تعتمد المنظمة ككل لها، ويستحسن أن يعين مدير لنظام إدارة أمن المعلومات من أعضاء هذه اللجنة.

3) اختيار نطاق العمل والأهداف:

تقوم هذه المرحلة على اختيار نطاق العمل بناءا على أهداف وأعمال المنظمة فمثلا تريد إدارة تقنية المعلومات للحصول على شهادة ISO 27001 في مركز البيانات حيث

[1]- شهادة الأمن و السلامة ISO27001، **مرجع سابق الذكر.**

تحتوى هذه الأخيرة على آليات معتبرة والتي بدورها تحتوي على جميع معلومات المنظمة وهنا يتبين أن حماية مصادر المعلومات في النطاق يدعم حماية عمل المنظمة.

4) كتابة السياسة:

بعد الانتهاء من تحديد النطاق يستلزم المبادرة في رسم سياسة عامة لأمن المعلومات في النطاق والداعمة لحماية المعلومات وتبين التزام الإدارة العليا بأمن المعلومات وقد يتم اعتمادها من أعلى جهة في المنظمة[1].

5) تطوير منهج تقييم المخاطر:

يقوم على مجموعة من الخطوات الأساسية التي تبين طريقة تحديد وتحليل وتفسير وكذا تقييم المخاطر لمصادر المعلومات في نطاق العمل بحيث يتم فيه معرفة أصول وقيمة المعلومات إضافة إلي معرفة مختلف الثغرات والتهديدات المحتمل حدوثها ومدى تأثيرها على سلامة وسرية المعلومات، فالفهم السليم لسير العمل داخل المنظمة من أفضل الوسائل التي تؤدى إلي معرفة أصول المعلومة وإظهار المخاطر المتوقعة لكل مصدر معلومات والذي يبين طرق الحماية التي تتناسب مع طبيعة المنظمة والتي يتم اختيار هذه الطرق من قائمة يوفرها المعيار كملحق له، فهذا المنهج يسعى إلي إيجاد طريقة ملائمة لحماية المعلومة والتقليل من المخاطر والسيطرة عليها[2].

6) التعامل مع المخاطر:

بعد الانتهاء من الخطوة السابقة أي بعد اختيار طرق الحماية يتم تسجيل وثيقة تتضمن جميع المخاطر التي تم تحليلها وتقييمها وكيفية التعامل معها ويتم الاختيار من قائمة طرق الحماية الواردة وتوضيح الطرق التي لم يتم التطرق إليها واستخدامها والسبب الذي أدى إلي عدم استخدامها كالأسباب المادية أو أسباب بيئية وتقنية...الخ، بحيث لابد من رفع هذه الوثيقة للجنة أمن المعلومات لمراجعة ما جاء فيها و متابعتها وكذا اعتمادها[3].

7) خطة تنفيذ الضوابط الأمنية:

واعتمادا على الوثيقة السابقة يتم وضع خطة تنفيذية تقوم على أساس تقييم وتحليل الخطر الذي استنتج مسبقا وتحديد طرق الحماية اللازمة بالإضافة إلى إعطاء طريق التنفيذ

---

[1]- بوفاس، طلحي، **نفس المرجع السابق**، ص8.
[2]- شهادة الأمن والسلامة، **مرجع سابق الذكر.**
[3]- بوفاس، طلحي، **مرجع سابق الذكر**، ص9.

وتاريخها والمهام والمسؤوليات الموكلة حيث نوضح أن طرق الحماية ليست بالضرورة أن تكون فقط تقنية وإنما يمكن أن تكون أيضا تنظيمية أو إجرائية.

8) التوعية الأمنية:

في هذه الخطوة يتم وضع برنامج لتوعية الموظفين بضرورة أمن المعلومات في نطاق عملهم، حيث يقوم هذا البرنامج على تقديم دورات تدريبية وتوعيتهم على تجسيد الأمن داخل المنظمة مع تقديم توضيح مفصل حول مختلف السياسات والإجراءات المتخذة بشأن أمن المعلومات وعلى أي جديد طرأ على هذا المفهوم مع التحقق من مدى توافق وتوازن أعمالهم مع ما جاء في الإجراءات.

9) إجراءات المراقبة والتطوير لنظام أمن المعلومات[1]:

تتسم عملية المراقبة على عدة خطوات تبين مدى مصداقية هذه السياسات وكذا إنشاء لجنة تقوم بتقييم هذه الإجراءات إذ تحتوي هذه الأخيرة على:

- مراجعة الأحداث الأمنية والعمل على معرفة المشكلة الرئيسية والتعامل معها.
- مراجعة سياسة أمن المعلومات بشكل دوري وتقديم مختلف التقارير الخاصة بالتحليل والتقييم للمخاطر.
- مراقبة ما تم تطبيقه من طرق للحماية والتي تم تبنيها من ملحق المعيار.
- مراجعة ملفات التدقيق الداخلي والخارجي للمؤسسة.
- رفع هذه التقارير للجنة أمن المعلومات والمسؤول عن نظام أمن المعلومات لاستخدامها كمدخلات لتطوير النظام وهذا التطور يشمل كافة هياكل النظام والمستجدات التي تطرأ عليه.

10) المحافظة على نظام أمن المعلومات:

إذ يتم هنا تطبيق كل ما تم التوصل إليه وتعديل ما يجب تعديله أي تصحيح الأخطاء الواردة والمستخلصة من الأحداث الأمنية والتقييم الداخلي والخارجي ومحاولة منع حدوثها في المستقبل وتعزيز هذا التواصل مع تبادل المعلومات فيما يتعلق بكيفية المحافظة على أمن المعلومات.

11) التدقيق الداخلي:

حيث يتشكل من فريق يقوم بمراجعة السياسات والإجراءات والسعي إلى تطبيقها على أرض الواقع ويستحسن أن يكون هذا الفريق منفصل أو مستقل عن الفريق الخاص بتطوير نظام أمن المعلومات لضمان سير العمل ونجاحه.

[1]- أسس ومبادئ نظام أمن المعلومات ISO27001، في: **http://www.qms.org.sa/qms/certificates-ar/iso-27001**، 2017/08/20.

يتبين من خلال هذه الخطوات أن تفعيل نظام أمن المعلومات وتطبيقه يتوقف على مشاركة مختلف جهات المنظمة والتعاون المتبادل لإظهار ضرورة المحافظة على سلامة هذا المفهوم وتطويره بمختلف الوسائل والإمكانيات[1].

المبحث الثاني: الجهود الجزائرية في مجال أمن المعلومات.

تكمن الجهود الجزائرية في وضع تشريعات قانونية تنص على الحماية الشاملة لمختلف أنظمتها وكذا تنظيم المعاملات الإدارية بشكل سليم، فهذه القوانين مست جميع المجالات لذا تم إصدار قوانين متعلقة بالجريمة الإلكترونية وأهم العقوبات التي تصيب مرتكبي هذه الجرائم كما قامت بإصدار قانون بشأن التوقيع والتصديق الالكترونيين.

المطلب الأول: مفهوم الجريمة الالكترونية.

انتشر موضوع الجريمة الالكترونية بشكل واسع حيث لقي صعوبة في تحديد تعريفا شاملا وجامعا لها، فنجد أن الباحثين قد استنتجوا أن الجريمة تعرف حسب الموقف وكذا حسب اهتمام كل فئة حيث تعددت جوانب هذه التعريفات فهناك من عرفها من الجانب الفني والتقني والبعض الأخر عرفها من الجانب القانوني[2].

تعرف الجريمة الالكترونية حسب الجانب التقني والفني على أنها عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي.

أما الجانب القانوني فيعرفها بأنها مجموعة من الأفعال والأنشطة المعاقب عليها قانونيا والتي تربط بين الفعل الإجرامي والثورة التكنولوجية أي أنها نشاط جنائي تتمثل في الاعتداء على برامج الحاسب الآلي بغية تحقيق الأرباح.

يتضح لنا أن الجريمة الالكترونية هي ممارسة أفعال غير قانونية والتي تلحق الضرر بالأشخاص حيث تتم باستخدام جميع الوسائل المتاحة وتكون بطريقة مباشرة أو غير مباشرة والجريمة الالكترونية من بين أحدث الجرائم المنتشرة والتي تهدد أمن الدولة بشكل عام وأمن الأفراد بشكل خاص.

المطلب الثاني: أنواع الجرائم الالكترونية.

---

[1]- بوفاس، **نفس المرجع السابق.**

[2]- فضيلة عاقلي، "الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري"، **http://jilrc.com/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9%D8%A7%...**، .2017/10/04

تعددت أنواع الجرائم الالكترونية حيث يصعب حصرها بسهولة لذا تم تصنيفها حسب الفئات وحسب الأسلوب المتبع في الجريمة، حيث سنقوم بجمع الجرائم التي تم التطرق إليها في أغلب التشريعات وهي كالتالي[1]:

- جريمة الدخول غير المشروع والتي تعني دخول الشخص إلى شبكة الانترنيت دون قبول الجهة المعنية بذلك وهذا الفعل ارتكب عمدا عن طريق خرق الحواجز والتدابير الأمنية بغية الحصول على معلومات الحاسب.
- إتلاف أجهزة المعلومات وتخريبها إضافة إلى حذف جميع المعلومات الموجودة فيها.
- صناعة الفيروسات ونشرها لتدمير برامج المعلومات.
- تغيير مواصفات وخصائص تقنية المعلومات التي تعتبر انتهاك لحقوق الملكية الفكرية.
- سرقة الأجهزة المادية ومكوناتها مع إتلاف المعلومات الهامة.
- الإخلال بالنظام عن طريق نشر مواقع ترويج أفكار وبرامج مخالفة للنظام العام والآداب والانتهاك للمعتقدات الدينية.
- جريمة الاعتداء على الملكية الفكرية وذلك بإصدار المصنفات الفكرية أو الأدبية وكذا الأبحاث المتاحة على شبكة المعلوماتية ونسخها دون أن تنسب إلى صاحبها الأصلي مما يلحق الضرر بالمؤلف وضياع حقوق الملكية الفكرية.

تبقي هذه الجرائم منتشرة بكثرة نظرا لسوء استخدام تقنية المعلومات وقصور الحماية القانونية لهذا النوع من الجرائم وعدم التشدد في مواجهتها مما تزداد في الانتشار وتتطور بتطور التكنولوجية مما يؤثر سلبا على الأداء الفكري والمؤسساتي.

المطلب الثالث: واقع الجريمة الالكترونية في الجزائر.

سابقا لم تكن الجريمة الالكترونية تشمل الجزائر ولكن مع حلول سنة 2005 سجلت الجزائر أول جريمة الكترونية، وفي عام 2009 ومع تزايد انتشار الانترنيت تزايد عدد المشتركين والناشطين فيها والتي أسفرت عن اعتقال 88 شخصا متهما بالجريمة الالكترونية حيث استمرت بالتقدم وتتمثل المخالفات المسجلة في:

- الاطلاع الغير شرعي على البيانات والمعلومات قصد إتلافها.
- القرصنة على المواقع الرسمية والخاصة.
- الدعاية المغرضة والإرهاب.
- سرقة المعلومات والتعدي على الحياة الشخصية للأفراد.

فنجد أن الجريمة الالكترونية تستهدف عدة مجالات ونشاطات وكذا جميع القطاعات حيث تتفاوت نسب الجريمة من قطاع لآخر فمثلا نجد أن الإدارة العامة والشركات الصناعية

[1]- فضيلة عاقلي، **نفس المرجع السابق.**

نسبة تعرضها للجرائم والتعديات الالكترونية تصل إلى60%، أما الشركات الخاصة تستهدف بنسبة 20% وفيما يخص الشركات الأجنبية فنسبة تعرضها للجريمة يقدر ب 11% وأخيرا تعود نسبة 6% للأشخاص العاديين[1].

أمام الفراغ القانوني في مجال الجريمة الالكترونية تم إصدار القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم لقانون العقوبات والذي ينص على الحماية الجزائية للأنظمة المعلوماتية من أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وفي سنة 2009 تم سن قانون الجريمة الالكترونية رقم 09-04 المؤرخ في 05 أوت 2009 والذي يتضمن القاعدة الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2].

- **مضمون قانون 09-04:**

يهدف قانون 09-04 المؤرخ في 5 أوت 2009 إلى "وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3]، حيث يتضمن على مادة مقسمة إلى ستة فصول وجاء فيها ما يلي:

ينص الفصل الأول على أحكام عامة والتي تبين الهدف من القانون وتبرز المفاهيم والمصطلحات المتعلقة بالجريمة الالكترونية مع الإحاطة بمجالات تطبيق أحكامها.

أما الفصل الثاني فينص على مراقبة مختلف الاتصالات الالكترونية مع وضع أحكام خاصة بمراقبة هذه الاتصالات، كما اهتمت هذه القواعد بخطورة التهديدات المحتملة وأهمية المصالح المحمية.

بينما ركز الفصل الثالث على القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجريمة الالكترونية تماشيا مع المعايير العالمية المعمول بها والأخذ بعين الاعتبار ما جاء في قانون الإجراءات الجزائية من مبادئ عامة،و فيما يخص الفصل الرابع فقد تطرق إلى خدمات والتزامات العاملين في مجال الاتصال خصوصا المتعلقة بحفظ المعطيات والتي تؤدى إلى دعم السلطات العمومية ومساعدتها في مواجهة الجرائم، أما الفصل الخامس فقد أشار إلى ضرورة إنشاء هيئة وطنية للوقاية من الإجرام وتحديد مسؤولياتها، وفي الأخير نجد أن الفصل السادس تناول التعاون والمساعدة القضائية الدولية في إضفاء قواعد تنص

---

[1]- سليم مزيود، "الجرائم المعلوماتية واقعها في الجزائر و آليات مكافحتها"، **المجلة الجزائرية للاقتصاد و المالية**، ع(1) (أفريل 2014)، ص 103.

[2]- عبد الله حاج سعيد،" تقييم نظام الحكومة الالكترونية في الجزائر"، **مجلة دولية علمية محكمة**، ع(02) (أكتوبر 2015).

[3]- الجمهورية الجزائرية الديمقراطية الشعبية، **الجريدة الرسمية العدد47**، القانون رقم 09-04 المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، ص 5.

على توفير الحماية لمجال تكنولوجيا الإعلام والاتصال والقضاء على مثل هذه الجرائم المخلة بالأمن العام والخاص[1].

المبحث الثالث: التشريعات الجزائرية المتعلقة بالتوقيع والتصديق الالكترونيين.

يتمتع كل من التوقيع الالكتروني والتصديق الالكتروني بمكانة وأهمية بارزة حيث ظهرت قوانين وتشريعات تعترف به، ومن ضمنها القانون الجزائري الذي جاء بنصوص واضحة حيث يعتبر القانون رقم 05-10 المؤرخ في 20 جوان 2005 أول قانون يتناول قضية التوقيع الالكتروني المعدل والمتمم للقانون المدني كما تم مؤخرا إصدار قانون 15-04 المؤرخ في 1 فيفري 2015 الذي يحدد القواعد العامة للتوقيع والتصديق الالكترونيين.

المطلب الأول: مفهوم التوقيع الالكتروني وأشكاله.

أولا: تعريف التوقيع الالكتروني.

يعرف التوقيع الالكتروني حسب المادة 2 من الفقرة الأولى من قانون 15-04 بأنه" بيانات الكترونية في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق"[2]، في حين نصت المادة 7 على أن تتوفر متطلبات خاصة بالتوقيع الالكتروني وهي:

- أن يتم إنشاء هذا التوقيع على أساس شهادة التصديق الالكتروني.
- ترتبط هذه الوثيقة بالموقع فقط و تملك قدرة تحديد الهوية.
- أن تكون مرتبطة بالبيانات الخاصة به.
- مصممة بواسطة آلية مؤمنة للتأكد من التوقيع و معرفة الموقع الحقيقي.

ثانيا: أشكال التوقيع الالكتروني.

تتعدد أشكال وصور التوقيع الالكتروني لما له من تقنيات مختلفة للتشغيل حيث يظهر لنا أن لكل شكل تقنية مختلفة تستخدم في إحداث توقيع إلكتروني، فهناك تقنية تعتمد على منظومة الأرقام أو الحروف أو الإشارات، ومنها من يعتمد على الخواص الفيزيائية والسلوكية للأشخاص وتتمثل هذه الصور فيما يلي[3]:

1. **التوقيع البيومتري:** يعتمد نظام التوقيع الالكتروني على صفات خاصة بكل شخص والتي تميزه عن غيره كبصمة الأصبع أو العين، نبرة الصوت وغيرها من الصفات الجسدية

---

[1]- سليم مزيود، **نفس المرجع السابق**، ص 104.

[2]- الجمهورية الجزائرية الديمقراطية الشعبية، **الجريدة الرسمية العدد 6**، القانون رقم 15-04 المؤرخ في 1 فيفري 2015، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الالكترونيين، ص7.

[3]- حنان براهمي، **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية**، أطروحة دكتوراه (جامعة بسكرة: كلية الحقوق والعلوم السياسية، 2015/2014)،ص ص 145-149.

والسلوكية، بحيث يتم تخزين هذه الصفات على الحاسب عن طريق التشفير حيث يعاد تفكيك هذا الأخير للتحقق من صحة التوقيع كما يحدد النظام الشخص الذي يملك المعطيات البيومترية التي تم إدخالها ليقارنها مع تلك المخزنة في النظام لتحديد هوية الشخص.
لكن رغم الأساليب المتخذة في هذا التوقيع وامتيازه بالدقة والأمانة إلا انه يبقى عرضة للتزوير فهذه الآليات يمكن تزويرها من خلال إعادة تسجيل ونسخ بصمة الصوت والأصبع أو مطابقة الشفاه بطريقة طلائها بمادة معينة ووضع عدسات لاصقة ليبين التشابه بالشخص المراد وهذه الأمور تؤدى إلى ضياع مصداقية التوقيع.

2. **التوقيع بالقلم الالكتروني:** يتم هذا التوقيع عن طريق استخدام الشخص لقلم الكتروني ليوقع على شاشة الحاسب الآلي ليتم تخزين إمضائه في الكمبيوتر بعدما تم تصويره وإدخاله إليه بالماسح الضوئي كما يتم حمايته برقم سري لاستعماله وقت الحاجة.
3. **التوقيع بالرقم السري:** يرتبط هذا النوع من التوقيع ببطاقات الممغنطة التي تصدر عن البنوك والمؤسسات المالية كوسيلة دفع أو سحب وتحتوي هذه البطاقة على أرقام سرية خاصة بالشخص يستخدمها أثناء إدخال البطاقة في الجهاز الصرف الآلي، حيث يمتاز هذا النوع بالأمان لصعوبة الحصول على الرقم السري للبطاقة إذ لا يعلمه إلا صاحب البطاقة ويتم إرساله بطريقة رسمية، وفي حال ضياع البطاقة يتوجب على الشخص إبلاغ البنك والسلطات المسؤولة لإيقاف عمل البطاقة[1].
4. **التوقيع الرقمي:** يعتبر هذا النوع من أهم صور التوقيع الالكتروني فهو يتمتع بدرجة عالية من الأمان في استخدامه وتطبيقه حيث يقوم بتحديد الوثيقة التي تم توقيعها بصورة لا تحتمل التغيير، فهو عبارة عن رقم سري ينشئه صاحبه باستخدام برنامج الحاسب الآلي لينشأ دالة رقمية لرسالة الكترونية يجري تشفيره بإحدى طرق المفتاح العام والخاص فيحول الوثيقة الالكترونية من صورة مقروءة إلى صورة غير مفهومة ولا مقروءة ولا يمكن لأي شخص إعادة هذه المعادلة الرياضية بالشكل المقروء إلا ملك التشفير.

التشفير: عبارة عن تغيير في شكل البيانات عن طريق تحويلها إلى رموز وإشارات لضمان الحماية للبيانات من التغيير والتعديل أو الحذف لذا اعتمد هذا التوقيع على التشفير والذي ينقسم إلى نوعين:

1- التشفير المتماثل والذي يقوم على فكرة الرقم السري المتبادل بين طرفين ويعمل في بيئة منعزلة وأن الرقم السري معروف لدى صاحبه والجهاز فقط.
2- التشفير الغير متماثل والذي يعتمد على مفتاحين غير متماثلين مفتاح عام وآخر خاص[2].

[1]- حنان، **نفس المرجع السابق، الصفحة نفسها.**
[2]- طيموش عزولة، فريدة علاوات، **التوقيع الالكتروني في ظل القانون رقم 15-04**، مذكرة ماستر(جامعة بجاية: كلية الحقوق و العلوم السياسية،2016/2015)، ص11.

المفتاح الخاص يكون معروف من قبل جهة واحدة فقط وقد عرفه المشرع الجزائري في نص المادة 2 من الفقرة 8 من قانون 15-04 بأنه" عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء توقيع الكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي[1].

أما المفتاح العام فيكون معروف من أكثر من شخص ويستطيع المفتاح العام فك شفرة الرسالة التي تم تشفيرها بواسطة المفتاح الخاص، حيث عرف المشرع الجزائري في نص المادة 2 من الفقرة 9 من قانون 15-04 المفتاح العام بأنه" عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الالكتروني وتدرج في شهادة التصديق الالكتروني"[2].

المطلب الثاني: شروط وخصائص التوقيع الالكتروني.

أولا: شروط التوقيع الالكتروني.

اعتبر التوقيع الالكتروني شكلا جديدا من أشكال التوقيع، فهو مطابق للتوقيع التقليدي من حيث القيمة القانونية، لذا استلزم علينا دراسة الشروط الواجب توفيرها في هذا التوقيع ليكون ذات فائدة لكافة تعاملاته ونلخصها كالتالي:

1- ارتباط التوقيع بالموقع دون غيره:

لابد أن يكون لصاحب التوقيع الالكتروني بيانات وشفرة خاصة به تكون مختلفة عن باقي الموقعين، حيث يبين التوقيع عن هوية الشخص ويبرز رغبته في العقود التي تبرم عن طريق التوقيع فيتم الاعتراف به كعلامة مميزة للموقع سواء ذكر الاسم أم لم يذكر ويستحسن إدراج الاسم في آخر التوقيع أو الحرف الأول من إسمه، لذا لا يمكن أن يصدر توقيع واحد لشخصين فالتوقيع الالكتروني يحدد المعلومات الأساسية للشخص الموقع ومركزه كما يقوم على الخصائص الذاتية لكل شخص.

2- التعبير عن رغبة الموقع:

يقوم هذا الشرط على إبراز رضا الموقع وإقراره على قبول ما نصت عليه الملفات بطريقة التوقيع مهما كان شكل هذا الأخير، ويتم الاعتراف بتحقق هذا الشرط إذا توفر استخدام الأرقام السرية لبطاقات الائتمان في أجهزة الحاسب الآلي والذي يعبر عن إرادة

[1]- الجمهورية الجزائرية الديمقراطية الشعبية، **الجريدة الرسمية العدد6**، الصفحة نفسها.
[2]- ج ج د ش، المرجع نفسه.

الشخص بالتصرف، ويتماشى هذا الشرط مع كل أشكال التوقيعات الالكترونية الأخرى لأن التكنولوجيا طغت على مختلف الخدمات وأصبح تعترف بها قانونيا حيث يأخذ هذا التوقيع كدليل يوضح إرادة الشخص نفسه دون أدنى شك خاصة مع تقنيات التشفير والإجراءات الأمنية المتخذة حيال ذلك[1].

3- سلامة الوثيقة الوقعة من التغيير:

للتحقق من سلامة محتوى السندات من أي تعديل وتغيير التي قد تطرأ عليها فإن شهادة الموثق ضرورية لذلك ليتم التأكد من صحة التوقيع الرقمي كما يؤكد على أن التوقيع منسوب للشخص نفسه إضافة إلى صحة البيانات الموقع عليها وصدورها من موقعها فتصبح بذلك بيانات موثقة لا يمكن إنكارها، فهذه الخاصية تعتمد على تقنية التشفير ذات مفتاحين يقوم المرسل بتشفير الرسالة بمفتاح عام ليتم اختصارها إلى خانات رقمية ثم يشفر المرسل رسالته بمفتاح خاص الذي يحول النص المشفر إلى الوضع الأصلي التي تتم قراءته بشكل واضح ومفهوم.

ثانيا: خصائص التوقيع الالكتروني.

يتم التوقيع الالكتروني عن طريق عدة أجهزة ووسائل الكترونية من حاسب آلي وانترنيت حيث يمكن الاطلاع على وثائق العقد وإفراغه في محررات إلكترونية وكذا إجراء التوقيع الالكتروني عليه.

- يشترط في التوقيع الالكتروني أن تأخذ صورة معينة وتكون ذو طابع منفرد ليتم تحديد هوية الشخص الموقع و إظهار رغبته في إقرار العمل القانوني.
- وظيفة التوقيع الالكتروني هو ربط المحرر الالكتروني بالتوقيع والحفاظ على مضمون المحرر وتأمينه من التعديل (الحذف أو الإضافة).
- التوقيع الالكتروني يحدد شخصية الموقع و يميزه عن غيره.
- يضمن التوقيع الخصوصية والسرية للموقع ويسهل عمل مستخدمي الانترنيت والعاملين في إمكانية تحديد هوية الموقع.

يمتاز التوقيع الالكتروني بالدقة والوضوح في انجاز المعاملات كما يبسط الإجراءات ويسهل تقديم الخدمات للمواطنين على أحسن وجه إضافة إلى امتيازه بالسرية والشفافية والمعالجة الفورية للطلبات[2].

المطلب الثالث: مفهوم التصديق الالكتروني وشروط ممارسته.

أولا: مفهوم التصديق الالكتروني.

---

[1]- سهيلة طمين، **الشكلية في عقود التجارة الالكترونية**، رسالة ماجستير(جامعة تيزي وزو:كلية الحقوق،2011)،ص ص 52-54.

[2]- طيموش، علاوات، **مرجع سابق الذكر**، ص 17.

مع بروز العقود والسندات الالكترونية عبر الانترنيت أصبح من الضروري ممارسة نشاط التصديق الالكتروني على مختلف البيانات والمعلومات التي تتضمنها هذه العقود وكذا تحديد الأطراف المتداخلة في العقد لسلامة وأمن المعاملات، وللقيام بتأدية خدمات التصديق لابد من وجود هيئة مختصة تملك كفاءة تقنية وقانونية تتماشى مع الأوضاع وكذا التطور الذي لحق بتكنولوجيا المعلومات.

يعرف التصديق الالكتروني على أنه مجموعة من الإجراءات التي تسمح بتسيير الشهادات الالكترونية وإصدارها أو إبطالها، حيث تستخدم هذه الشهادة للتحقق من التوقيعات الالكترونية وتضمن عدة جوانب لتبادل المعلومات: السرية، التوثيق، النزاهة وعدم الاستنكار التي تؤدي إلى زيادة الثقة[1].

التصديق الالكتروني(التوثيق الالكتروني): يعد الموثق الالكتروني بمثابة طرف ثالث محايد (شركات أو أفراد) حيث تقوم بمهام الوسيط بين المتعاملين لإتمام المعاملات الالكترونية وتتمثل مهامهم في تحديد هوية المعاملين وأهليتهم القانونية للتحقق من سلامة المعاملات وجديتها[2].

يظهر لنا أن التصديق الالكتروني نشاطه قائم على متابعة طريقة سير المعاملات الالكترونية ومدى مصداقيتها حيث وضع المشرع الجزائري أهم الخدمات التي يقوم بها التصديق ويحدد هوية الموقع وتطابق هذا التوقيع مع الشخص نفسه.

ثانيا: شروط ممارسة نشاط التصديق الالكتروني.

لقد حدد المشرع الجزائري في المواد من 33إلى 40 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الالكترونيين الشروط الملائمة لتأدية خدمات التصديق والتي يستوجب على الشخص الراغب في تأدية هذه الخدمة والنشاط التقيد بهذه الشروط:

- أن يكون خاضعا للقانون الجزائري وتمتعه بالجنسية الجزائرية.
- امتلاكه لميزانية مالية معتبرة.
- التمتع بمؤهلات وخبرة في ميدان تكنولوجيا المعلومات والاتصال.
- أن لا يكون ذات سوابق عدلية والتي تنفي تأدية خدمة التصديق الالكتروني ومعارضة للقيم والشروط[3].
- أما فيما يخص الترخيص الممنوح للراغبين في مواصلة تأدية خدمة التصديق الالكتروني، نص المشرع الجزائري على وجوب حصوله على شهادة تأهيل لمدة سنة كاملة " تمنح

---

[1]-ندا معيزي، **النظام القانوني للتصديق الالكتروني**، مذكرة ماستر(جامعة ورقلة: كلية الحقوق و العلوم السياسية،2015)، ص6.

[2]- ناجي الزهراء،" التجربة التشريعية في تنظيم المعاملات الالكترونية المدنية و التجارية"، **المؤتمر العلمي المغاربي الأول حول المعلوماتية و القانون المنعقد في الفترة من 28 إلى 29 أكتوبر 2009**، ص13.

[3]- مصطفى هنشور وسيمة، **النظام القانوني للتجارة الالكترونية في التشريع الجزائري و المقارن**، رسالة دكتوراه، (جامعة مستغانم: كلية الحقوق و العلوم السياسية، 2016)، ص276.

شهادة التأهيل قبل الحصول على الترخيص لمدة سنة واحدة (1)، قابلة للتجديد مرة واحدة و تمنح لكل شخص طبيعي أو معنوي لتهيئة كل الوسائل اللازمة لتأدية خدمات التصديق الالكتروني"[1].

- بعد حصول الشخص على الترخيص لمدة 5 سنوات ترفق معه وثيقة دفتر الشروط الذي يحدد كيفية تقديم خدماته المتعلقة بالتصديق إضافة إلى توقيع شهادة التصديق الخاصة بمؤدى الخدمة من طرف السلطة الاقتصادية للتصديق.

المطلب الرابع: التزامات مؤدي خدمات التصديق الالكتروني.

أثناء امتثال مزود خدمات التصديق الالكتروني لقائمة الشروط التي وجب عليه تطبيقها، يستلزم عليه القيام بمجموعة من الالتزامات التابعة لهذه الخدمات وهي كالتالي[2]:

1- الالتزام بالتأكد من صحة البيانات:

يجب على مؤدى الخدمات الالكترونية التأكد من صحة البيانات الممنوحة للأشخاص الذين تم تصدير الشهادة لهم والتحقق من الصفات المميزة التي برزت في الشهادة حيث يعتبر هذا الالتزام أكثر دقة بالنسبة لمقدم خدمات التصديق الالكتروني لذا يحتاج إلى طاقم وظيفي ذات خبرة وكفاءة عالية في إنجاز مثل هذه الأعمال وإظهار صحة البيانات وأهلية الشخص، حيث يترتب على هذا النوع من الالتزام صعوبة كبيرة لما له من آثار سلبية على التجارة الالكترونية ووقوع أخطاء وحدوث خلل في المعطيات مما يؤدى إلى التعويض من طرف مقدم خدمات التصديق الالكتروني في حالة تقديم بيانات غير صحيحة، بحيث نجد تعدد تصنيفات خاصة بهذا الالتزام وهي كالتالي:

- التزامات مزاولة النشاط: أي متابعة ومواصلة النشاط الممنوح لمقدم خدمات التصديق الالكتروني دون توقف أو إحالته لشخص آخر دون الموافقة عليه من قبل الجهة المختصة والتي منحت الترخيص بالعمل.

- التزامات تفحص صحة البيانات: وتتمثل في مراجعة جميع البيانات وبيان صحتها من قبل الشخص الذي تم تأهيله لممارسة مهام مقدم خدمات التصديق الالكتروني ومنحه الشهادة. وهذا الجانب يعتبر العنصر المهم والدقيق لإتمام المهام الضرورية.

- التزامات حماية المعلومات وتأمينها: يقوم مؤدى خدمات التصديق الالكتروني بوضع متطلبات فنية وتقنية مؤمنة تكون متطابقة مع شروط التوقيع الالكتروني، لذا وجب توفر إمكانيات مادية ومعنوية (أجهزة، مختصين) ليبرز الطرق والأساليب التي ينتهجها للقيام بعمله لضمان التأمين للمعلومات وكذا صحة البيانات المتحصل عليها.

2- الالتزام بإصدار شهادة التصديق الالكترونية:

[1]- الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية العدد6، **المرجع سابق الذكر**،ص12.

[2]- معيزي، **المرجع سابق الذكر**، ص 10.

يقوم مؤدى الخدمات الالكترونية بإصدار الشهادة وفقا للشروط التي ينبغي توفرها حيث يؤكد من خلال هذه الشهادة صحة التوقيع الالكتروني الذي تتضمنه وتطابقه مع الشخص نفسه، كما يحدد هوية الشخص واستجابته للشروط القانونية، حيث يظهر لنا أن دور شهادة التصديق الالكتروني يتشابه مع دور بطاقة التعريف الوطنية لأنها تبين علاقة الشخص بالوثيقة التي يحملها من خلال إظهار صحة التوقيع والصورة الموضوعة على مستوى الوثيقة.

فنجد أن المشرع الجزائري عرف الشهادة الالكترونية حسب المرسوم التنفيذي رقم 15-04 على أنها الوثيقة التي تأتي على شكل إلكتروني لتثبت العلاقة الموجودة بين بيانات فحص التوقيع الالكتروني والشخص الموقع، إذ تنص على ضرورة تقيد الشخص وخضوعه للالتزامات التي تحددها الوثيقة[1].

كما يفرض على موظف الخدمات الالكترونية الالتزام بالسرية عند أداء مهامه والحفاظ على سرية المعلومات الشخصية للأشخاص.

نستنتج أن هذه الالتزامات تقوم على تحديد المسؤوليات المترتبة على مقدم الخدمات الالكترونية إذ تبين الطرق الواجب تطبيقها عند تنفيذ مهامه وأن القانون والتشريعات ينص على ضرورة التقيد بها لأن أي خلل ينجم عنه أو يلحق الضرر بصاحب الشهادة فالقانون المدني يلزم مؤدي الخدمة على تقديم تعويض لسوء الخدمة.

خلاصة الفصل:

لقد بين هذا الفصل مختلف القوانين والتشريعات التي اعتمدت عليها الجهود الدولية والجزائرية في مجال نظام أمن المعلومات وبيان الالتزامات التي ينبغي التقيد بها بغية تحقيق وبث الثقة والأمان للمؤسسات والإدارات في تسيير شؤونها وأعمالها بمواكبة التطور السريع في مجال تكنولوجيا المعلومات حيث تعرض إلى كيفية إجراء المعاملات الالكترونية التي تقوم أساسا على عنصري الإثبات والتوثيق لمختلف الوثائق والشهادات الصادرة وتحديد كافة المسؤوليات.

نجد أن كافة الإجراءات الصادرة عن هذه الجهات تكمن في توفير الأمن للمعاملات الالكترونية وسلامة مضامينها بغية القضاء على كافة الجرائم الالكترونية.

[1]- هنشور وسيمة، **نفس المرجع السابق الذكر**، 277.

الفصل الثالث

نظام أمن المعلومات في بلدية سوق الاثنين بولاية تيزي وزو 2014-2017

تمهيد:

بعدما تم التعرض إلى الإطار المفاهيمي والجهود المبذولة لموضوع نظام أمن المعلومات في الإدارة والدور الفعال الذي يمكن أن يلعبه أمن المعلومات في الرفع من فعالية نظام المعلومات، سيتم في هذا الفصل محاولة الاطلاع على واقع نظام امن المعلومات في الإدارة العامة المتمثلة في بلدية سوق الاثنين بتبني أسلوب دراسة الحالة كأحد الأساليب الهامة التي يستخدمها المنهج الوصفي التحليلي الذي تم اعتماده في هذه الدراسة، حيث تم اختيار مؤسسة محلية قصد معرفة الأساليب الأمنية التي تنتهجها هذه المؤسسة لضمان سلامة نظام معلوماتها.

لذا قسم هذا الفصل إلى ثلاث مباحث هي:

المبحث الأول: التعريف ببلدية سوق الاثنين بولاية تيزي وزو.

المبحث الثاني: واقع نظام أمن المعلومات ببلدية سوق الاثنين.

المبحث الثالث: المعوقات التي تواجه نظام أمن المعلومات وأهم الحلول المقترحة.

المبحث الأول: التعريف ببلدية سوق الاثنين بولاية تيزي وزو.

يتمثل مجتمع الدراسة في منظمة تابعة للجماعات المحلية ألا وهي بلدية سوق الاثنين (S.E.T) التي أطلق عليها هذا الاسم نسبة إلى السوق الأسبوعي المقام بالمنطقة كل يوم اثنين.

المطلب الأول: التعريف ببلدية سوق الاثنين(S.E.T):

1- نشأة و هيكلة المؤسسة (بلدية سوق الاثنين):

مر تأسيس المنطقة على ثلاث مراحل، الأولى العهد الفرنسي SAS من 1957 إلى 31 ديسمبر 1963 ثم انضمت إلى بلدية معاتقة من 1 جانفي 1964 إلى غاية 31 ديسمبر 1984 وانبثقت عنها إثر التقسيم الإداري الأخير لسنة 1984. إذ تضم هذه البلدية على ثمانية قرى تربطها بشبكة طرق تقدر مساحتها حوالي 14 كيلومتر مربع (كلم^2).

تقع بلدية سوق الاثنين على بعد 25 كلم جنوب مقر ولاية تيزي وزو، يحدها من الجنوب بلديتي مشطراس وتيزي نتلاثة، ومن الشرق بني دوالة، من الغرب معاتقة وتيزي وزو، من الشمال بني زمنزار، إذ قدر عدد سكان البلدية حسب إحصاء سنة 2008 ب14534، حيث يتواجد 14412، بالمركز و122 نسمة يعيشون في المناطق المجاورة، كما تتواجد في البلدية مؤسسات تعليمية على مستوى الأطوار الدراسية الثلاثة، إذ تم فتح ثمانية مدارس ابتدائية موزعة على مختلف قرى البلدية، أما فيما يخص المدارس المتوسطة تتوفر البلدية على متوسطتين، إضافة إلى وجود ثانوية واحدة على مستوى مقرها كما قامت هذه البلدية بتوفير أربع حافلات مخصصة للنقل المدرسي للتلاميذ[1].

هيأت البلدية عيادة متعددة الاختصاصات تتوفر على أربع قاعات للعلاج للتكفل بالصحة السكانية، وقاعتين للرعاية بصحة الأم والطفل إضافة إلى قاعة الاستعجالات ووجود سيارتين للإسعافات لنقل المرضى. كما يوجد في البلدية مركز البريد والمواصلات يهتم بالخدمات البريدية للسكان.

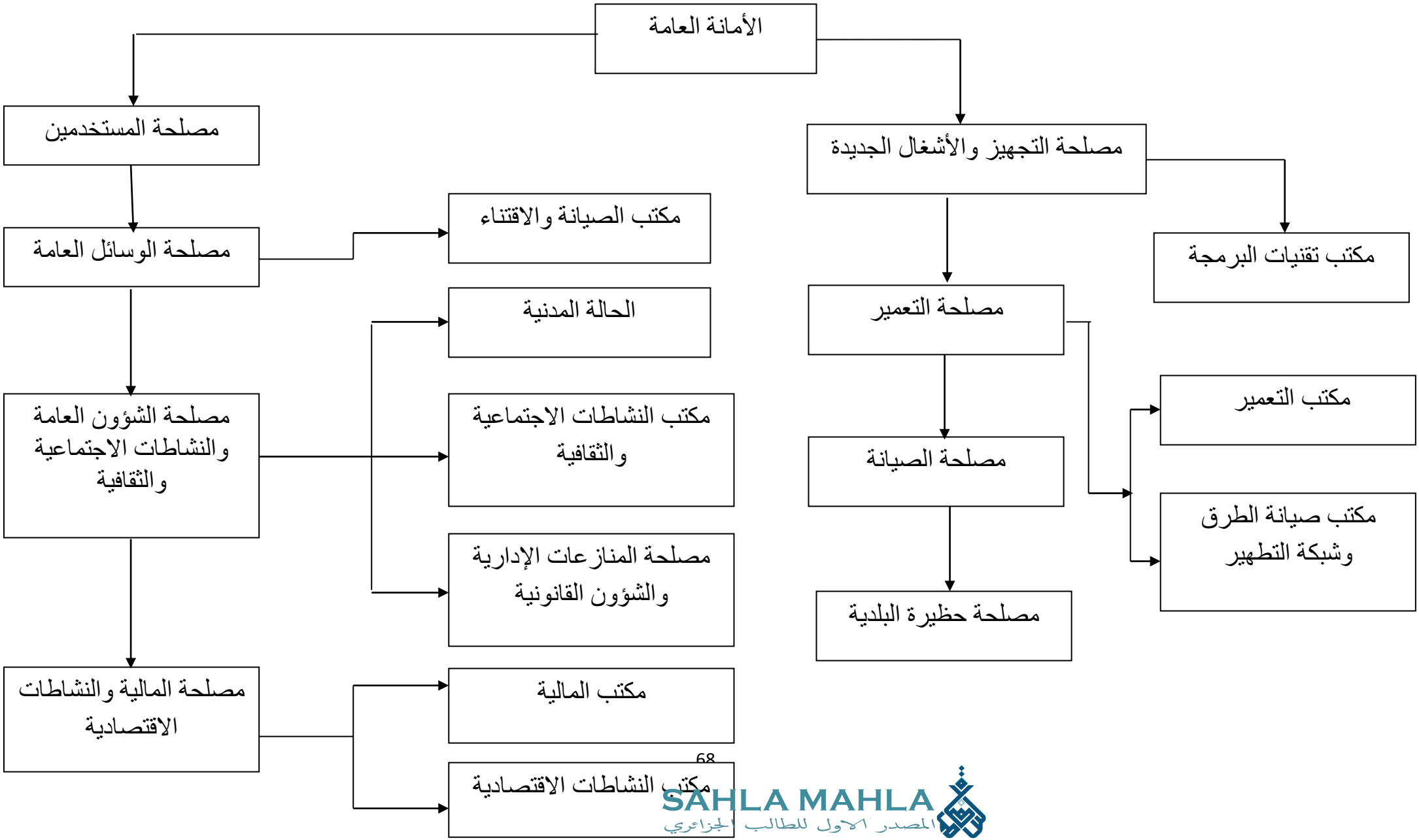
تهتم البلدية بالجانب الرياضي حيث تشمل مرافق ونوادي رياضية مخصصة للشباب والمتواجدة في سوق الاثنين (المركز) إذ تنشط هذه الجمعيات بهدف تحقيق التنمية، وتمتلك البلدية مؤهلات وإمكانيات فلاحية فهي منطقة مناسبة لتربية المواشي والفلاحة الريفية وكذا تربية النحل، كما فتحت البلدية دار الشباب تنشط فيها ثلاثة جمعيات ثقافية (الجمعية الثقافية ثاذويرث لقرية تعرقوبت، الجمعية الثقافية ثغري ألمزي لقرية نات عمار، الجمعية الثقافية ثيغيلت ناغ)، حيث تسهر هذه الجمعيات على إحياء ذكرى اندلاع الثورة التحريرية المجيدة والمصادفة للفاتح نوفمبر كما تقوم بمسابقات ثقافية علمية وأدبية للاحتفال بعيد الطفولة[2].

يتكون الهيكل التنظيمي لبلدية سوق الاثنين من الأمانة العامة والتي تشرف على ثمانية مصالح تقوم بوظائف متنوعة وتتمثل هذه المصالح في مصلحة المستخدمين، مصلحة

[1]- مستخرج من **سجل البلدية**، في 2017/9/7، ص 45.
[2]- **نفس المرجع السابق**، الصفحة نفسها.

التجهيز والأشغال الجديدة، مصلحة الوسائل العامة، مصلحة الشؤون العامة والنشاطات الاجتماعية والثقافية، مصلحة المالية والنشاطات الاقتصادية، مصلحة التعمير، مصلحة الصيانة، مصلحة حظيرة البلدية، حيث تكون كل مصلحة مسؤولة عن متابعة أعمال ونشاط مكتب معين والشكل رقم (1-3) يبين الهيكل التنظيمي للبلدية.

الشكل رقم(1-3): الهيكل التنظيمي لبلدية سوق الاثنين.



يبلغ عدد الموظفين الناشطين في هذه البلدية 154 موظف حكومي، حيث ينقسم هذا العدد إلى ثلاث مجموعات، المجموعة الأولى هم الموظفون الحاصلين على هذه الوظيفة بعقد دوام دائم وعددهم 63 موظف، أما المجموعة الثانية فهم الموظفين العاملين بعقد لمدة محددة (أي تكون لوقت كلي أو لوقت جزئي) وعددهم 76 موظف، أما المجموعة الأخيرة فيكون عقد لمدة غير محددة وعددهم 16 موظف[1].

المطلب الثاني: مجالات نشاط المؤسسة وأهدافها.

أ- مجالات نشاط البلدية:

تقوم البلدية بعدة نشاطات اقتصادية واجتماعية والثقافية، إذ تقدر ميزانية البلدية حوالي 265000000 مليون دينار جزائري حيث قامت بإعداد مشاريع مستقبلية مبنية على تخطيط مسبق بإعداد ورسم السياسة اللازمة لإتمام هذه المشاريع المتنوعة من بينها[2]:

- مشروع بناء سكن اجتماعي على مستوى مقر البلدية.
- إقامة مكتبة عامة في مقر البلدية.
- إعادة ترميم وتأهيل لدار الشباب.
- هم في صدد بناء مقر جديد للبريد والمواصلات.

كما تقوم بعدة نشاطات أخرى:

- إعادة تشكيل شبكة الطرق تعبيد مختلف طرق قرى المنطقة.
- القيام بترميم أرصفة البلدية و جميع الأشغال المتعلقة بالصرف الصحي وتنظيفها.
- التكفل بإعادة الطلاء لمختلف الأماكن العمومية
- دعم القرى المشاركة في حملة نظافة ماديا تحت اسم" أجمل وأنظف قرية" والموزعة على مختلف بلديات ولاية تيزي وزو.

تقوم بإعادة ترميم مختلف المدارس الموجودة بالمنطقة والتكفل بمختلف الأشغال الموجودة فيها من إعادة الطلاء لمختلف الأقسام والتكفل بميزانية المطاعم المدرسية.

كما يتم على مستوى البلدية استخراج مختلف الوثائق الخاصة بالحالة المدنية من[3]:

- بطاقة الإقامة.
- شهادة الميلاد، عقد الزواج، شهادة الوفاة.
- البطاقة العائلية للحالة المدنية.
- شهادة الميلادS12.

[1]- مقابلة مع السيد محمد شبلي، **أمين عام لبلدية سوق الاثنين**، عدد العاملين في البلدية و أهم نشاطاتها، في بلدية سوق الاثنين، 2017/09/9.
[2]- **المرجع نفسه.**
[3]- **نفس المرجع السابق.**

- تجديد الدفتر العائلي...الخ.

إن الوثائق الخاصة بالحالة المدنية أصبحت محوسبة ويتم إنتاجها واستخراجها عن طريق السجل الوطني الآلي للحالة المدنية، وفي حالة الانهيار المؤقت (انقطاع التيار الكهربائي، فشل النظام، غياب الاتصال بالانترنيت) يحق للمواطن الحصول على وثيقة الحالة المدنية المكتوبة بخط اليد.

يمكن إصدار وثائق الحالة المدنية في أي بلدية أو مرفق متصل بالسجل الوطني للحالة المدنية بصورة مستقلة عن بلدية الولادة.

انخفاض عدد وثائق الحالة المدنية إلي 14 وثيقة كما تم تحسين محتوياتها، إضافة إلى تمديد مدة صلاحية هذه الوثائق فمثلا شهادة الميلاد أصبحت صالحة للاستخدام 10 سنوات، أما شهادة الميلاد الخاصة بعقد الزواج فهي صالحة لمدة 3 أشهر.

يعفى المواطن من الانتقال إلى المحاكم لتصحيح الأخطاء المرتكبة في وثيقة الحالة المدنية الخاصة به بل البلدية هي التي تتكفل بها وذلك باتخاذها جميع الخطوات اللازمة.

ب- أهداف البلدية:

- ✓ التحقق من التقدم المحرز في رقمنة سجلات الأحوال المدنية.
- ✓ التحقق ما إذا كان السجل الوطني للحالة المدنية يعمل على مستوى المرفقات المشتركة.
- ✓ التحقق ما إذا كانت الخدمات مقدمة في حالة انقطاع التيار الكهربائي أو انقطاع الشبكة التي تربط السجل الوطني الآلي بالبلديات وغيرها.

المطلب الثالث: تقديم المصلحة المرتبطة بموضوع الدراسة[1].

- مصلحة جواز السفر وبطاقة التعريف البيومترية: تتكون هذه المصلحة من خمسة مكاتب موزعة لاستكمال ومتابعة الوثائق الخاصة بهذه المصلحة حيث ينشط فيها 6 موظفين كل حسب شهادته إذ تشرف عليهم ومراقبة نشاطهم مهندسة الإعلام الآلي كما تتوفر المصلحة على أجهزة حواسيب ذات جودة عالية من النوع الجيد hp: ثمانية أجهزة كمبيوتر، أربعة أجهزة طباعة، جهاز سكانير، آلة تصوير، مع توفر أجهزة إضافية في حالة حدوث عطل بالنسبة للأجهزة المستخدمة لضمان عدم توقف العمل.

- تتم عملية معالجة جواز السفر البيومترية الالكترونية عن طريق الخطوات التالية:

1- الخطوة الأولى: التدقيق (Vérification).

[1]- المقابلة مع السيدة فريزة مرجان، **مهندسة الإعلام الآلي**، التعريف بمصلحة جواز السفر، في بلدية سوق الاثنين، 2017/09/12.

- التحقق من مكونات المستندات المقدمة.
- إدخال 99% من المعلومات الديمغرافية في الصفحة 2 من جواز السفر(الاسم، اللقب، تاريخ الميلاد) و توليد تلقائيا رقم الهوية الوطنية(NIN).
- تفحص الصورة وs12 من مقدم الطلب.
- طباعة الإيصال الخاص بالملف.
- ضمان الامتثال للصورة المسجلة.
- إنشاء ملف التطبيق(مجلد جديد، ملف التجديد).

2- الخطوة الثانية: التدوين (saisie).

إدخال المعلومات المتبقية وإرسال الملف إلى جهة التصديق.

3- الشهادات (certification).

- التأكد من أن بيانات الضبط تتوافق مع الوثائق الواردة في الملف الذي قدمه مقدم الطلب للحصول على جواز السفر.
- التحقق النهائي من الملف ونقل هذا الأخير إلى وظيفة التجنيد.

4- التجنيد (Enrôlement):

- التدقيق النهائي من البيانات المدخلة (يعرض النظام جميع المعلومات التي سيتم طباعتها على جواز السفر).
- التحقق من صحة البيانات من قبل مقدم الطلب لجواز السفر إلزامي.
- ضمان التنظيف والتشغيل السليم لكافة المعدات.
- تشغيل إشارة الطوارئ من فشل المعدات.

5- الإصدار أو التسليم (délivrance):

- تسجيل جوازات السفر الالكترونية البيومترية.
- إصدار جوازات السفر الالكترونية البيومترية.
- التحقق من المعلومات المطبوعة على جواز السفر.
- تصحيح المعلومات غير صحيحة عبر البرمجيات.
- إعادة جوازات السفر ذات أخطاء طباعة.

- طباعة نماذج العودة وإرسالها إلى مديرية الأوراق المالية والوثائق المضمونة (DTDS) مصحوبة بجوازات سفر عائدة.

المبحث الثاني: واقع نظام امن المعلومات في بلدية سوق الاثنين.

المطلب الأول: هياكل أنظمة أمن المعلومات.

في هذا المبحث سيتم عرض نتائج دراسة الحالة (المقابلة والملاحظة) التي قمنا بها في المؤسسة ومناقشتها، وذلك من خلال وصف عملية تطبيق نظام أمن المعلومات داخل المؤسسة ومحاولة تقييمه واختبار صحة الفرضيات المقترحة للدراسة بناءا على النتائج المتوصل إليها.

- بناءا على المقابلة والملاحظة تم جمع المعلومات المتعلقة بنظام المعلومات الخاص بالبلدية حيث يتكون من: الأجهزة والمعدات، البرمجيات والعنصر البشري وكذا وجود قاعدة بيانات والشبكات.

1- الأجهزة والمعدات: تمتلك البلدية أجهزة من النوع الجيد والممتاز، حيث سنعرض مختلف أنواع الأجهزة المستخدمة. ويتمركز مكان هذه الأجهزة في مكتب موجود في الطابق العلوي في البلدية ويمنع دخول أي من الموظفين فهذا المكتب مخصص لمهندس الإعلام الآلي.
يتكون نظام المعلومات من عدة أجهزة ذات جودة عالية وهي مصنفة كالتالي:

الجدول رقم (3-1): مكونات نظام المعلومات.

الأجهزة	العلامة(النوع)	العدد
خادم: serveur ثماني النواة	BULL	3
الموجه: Routeur	CISCO	2
Rouleurs	CISCO	2
Modem مودم:	HP	1
مولد كهربائي	condor	3
مخزن الطاقة	CISCO	1
مكيف الهواء	Condor	17
أجهزة طباعة	Hp	20
جهاز سكانير	Hp	1
آلة تصوير	Samsung	1

جهاز كمبيوتر	Hp	20

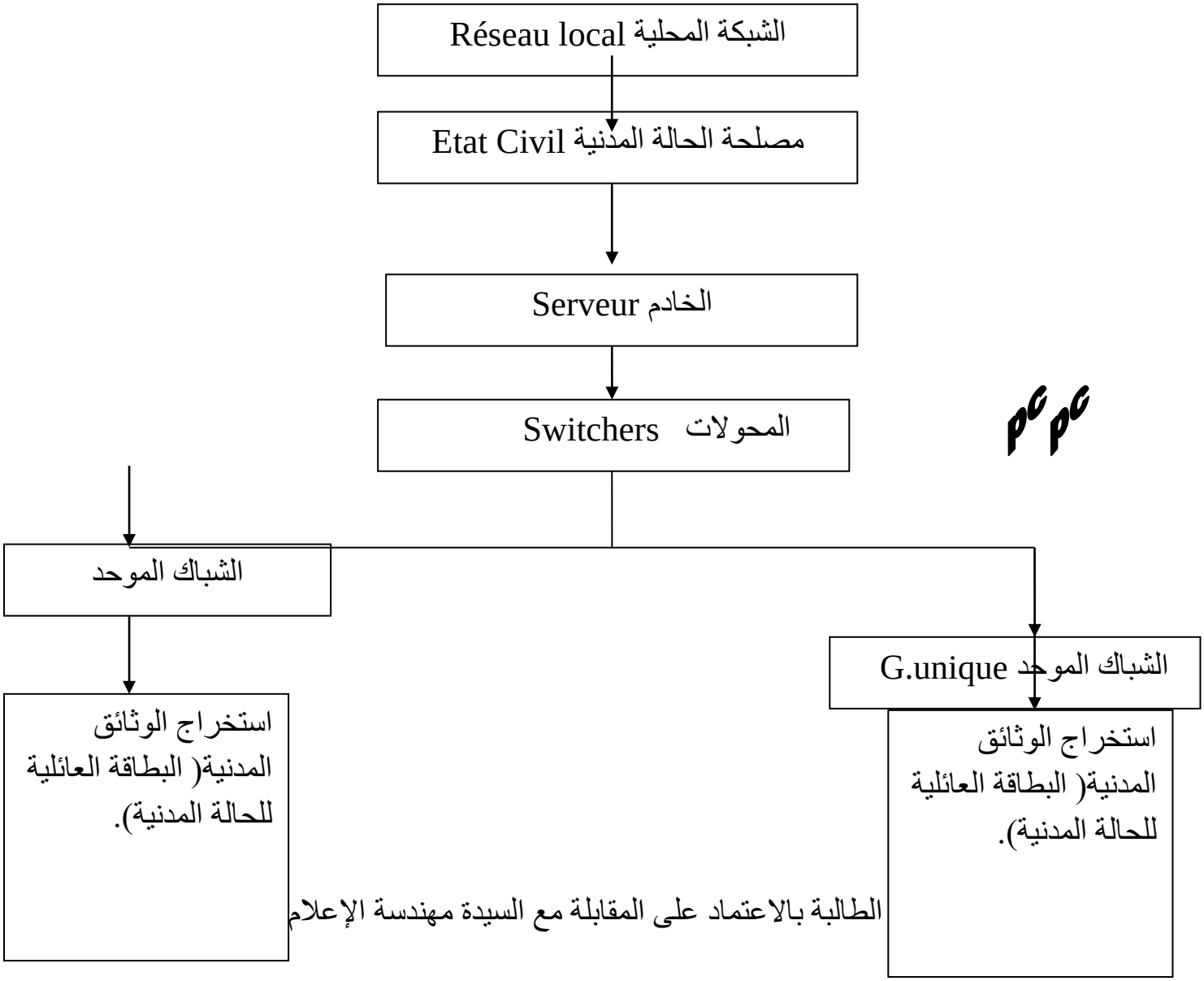
المصدر: من إعداد الطالبة بالاعتماد على المقابلة مع السيدة مهندسة الإعلام الآلي للبلدية.
يبين هذا الجدول الأجهزة الموجودة على مستوى المكتب المخصص لمهندس الإعلام الآلي وهذا المكتب يعتبر الركيزة الأساسية لتشغيل مختلف المعدات المنتشرة في مختلف مصالح البلدية. فهذا المكتب يجب أن تتوفر فيه مختلف وسائل الحماية المادية كما يبقي مكيف الهواء فيه على درجة 18°، وتكون هذه الأجهزة ذات جودة وكفاءة عاليتين وبكمية كافية. إضافة إلى الأجهزة الموزعة في مكاتب البلدية.

2- الشبكات: تحتوي البلدية على نوعين من الشبكات هما الشبكة المحلية (Réseau Local) والشبكة الوطنية (Réseau National).

2-1- الشبكة المحلية Réseau local: يستخدم هذا النوع من الشبكات للربط بين مصالح البلدية أي في مجمع متقارب إذ تبلغ سرعة نقلها (100 Mbit/s)، حيث ينقسم عمل هذه الشبكة إلى مصلحتين تابعتين لها وهي مصلحة الحالة المدنية وكذا مصلحة جواز السفر البيومترية، فنجد بأن الشبكة المحلية هي المشرفة والمراقبة لمختلف الخدمات والنشاطات التي تقوم بها هذه المصلحتين.

أ- مصلحة الحالة المدنية Etat Civil: هذه المصلحة تنجز مهامها في إطار متابعة من طرف الشبكة المحلية إذ تتوفر فيها خدمات متنوعة والشكل التالي يوضح طريقة عمل الشبكة المحلية:

الشكل رقم (2-3): كيفية عمل مصلحة الحالة المدنية.

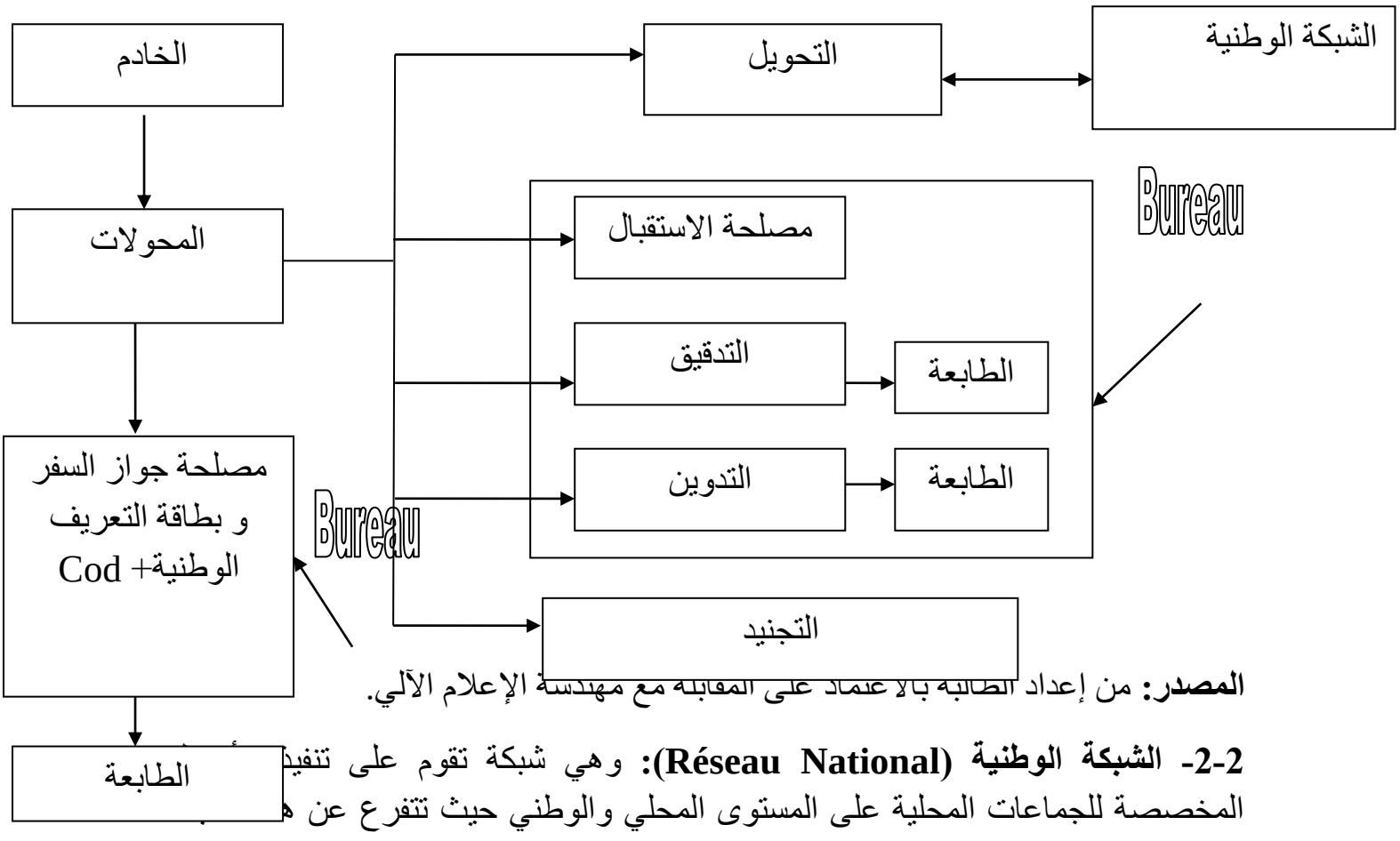


الطالبة بالاعتماد على المقابلة مع السيدة مهندسة الإعلام

يوضح الشكل التالي طريقة عمل الشبكة المحلية حيث يتبين لنا أن مصلحة الحالة المدنية التابعة لها تقوم بإنتاج الوثائق المدنية عن طريق الاتصال المباشر بالشبكات المحلية حيث يتم العمل بطريقة متسلسلة بين الأجهزة فمثلا جهاز الخادم يقوم بإرسال الوثائق المدنية من الشبكة المحلية إلى محولات لتمر إلى حواسب الحالة المدنية ليتم استخراجها للمواطنين الراغبين بها .

ب- مصلحة جواز السفر البيومترية: هي مصلحة متواجدة في الشبكة المحلية للبلدية إذ تقوم هذه الأخيرة بخدمات متنوعة ويتم استخراج هذه الوثائق بانتهاج الطريقة التالية التابعة للشبكة المحلية.

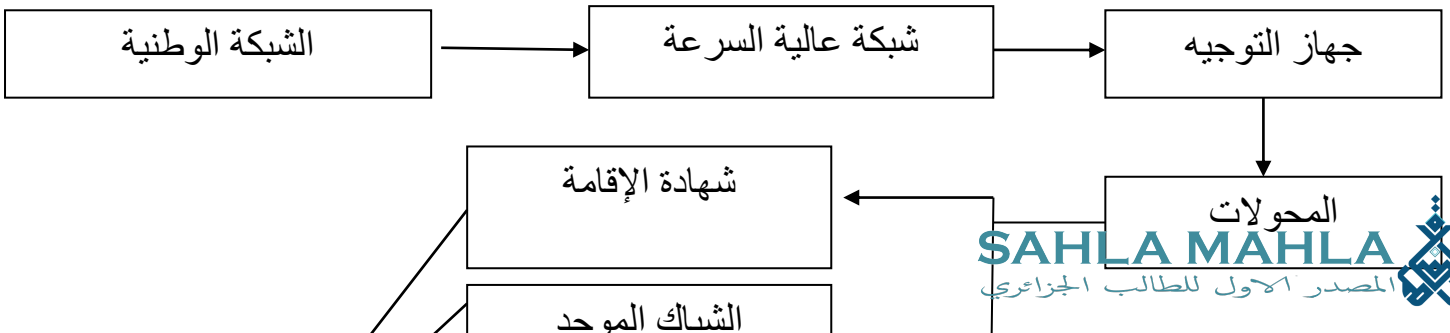
الشكل رقم(3-3): طريقة عمل مصلحة جواز السفر.



المصدر: من إعداد الطالبة بالاعتماد على المقابلة مع مهندسة الإعلام الآلي.

2-2- الشبكة الوطنية (Réseau National): وهي شبكة تقوم على تنفيذ [illegible] المخصصة للجماعات المحلية على المستوى المحلي والوطني حيث تتفرع عن ه[illegible] إلى شبكة تقوم بتنفيذ مهامها وهي شبكة عالية السرعة (Réseau Haut Débit) والتي تنشط على كافة مصالح البلدية إذ تتوزع خدماتها كالتالي:

الشكل(3-3): طريقة عمل شبكة عالية السرعة



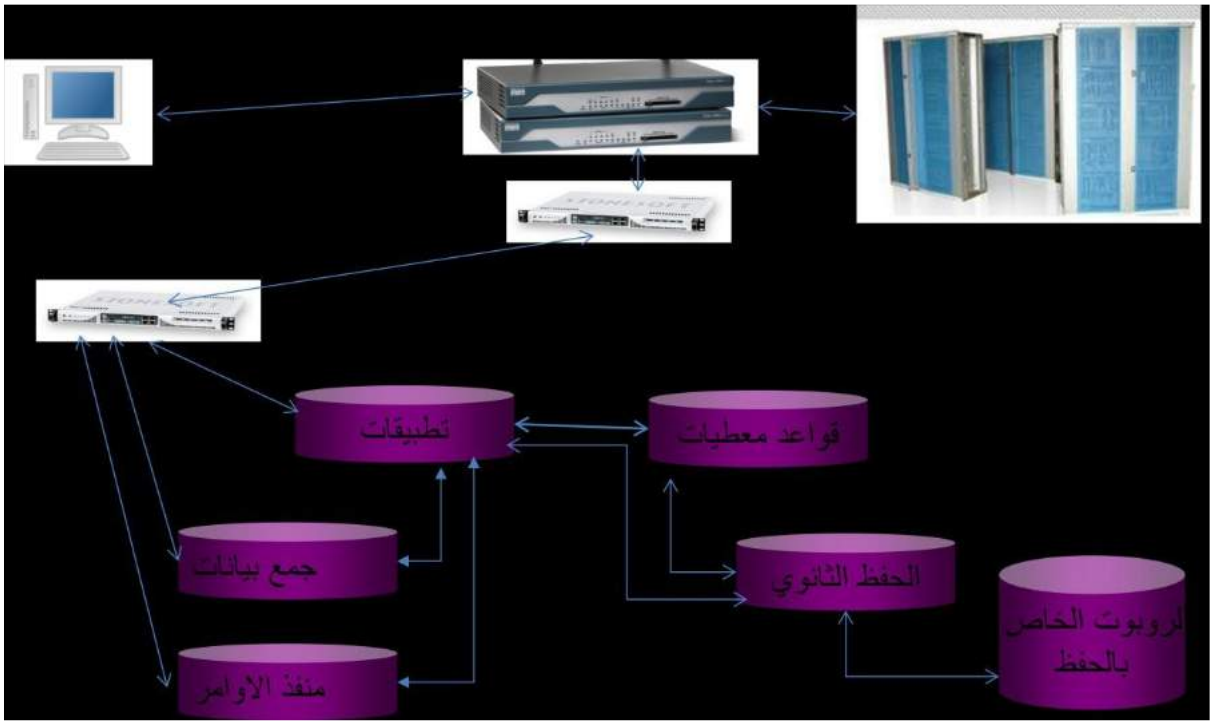
المصدر: من إعداد الطالبة بالاعتماد على المقابلة مع مهندسة الإعلام الآلي.

يوضح هذا الشكل الطريقة المتبعة لانجاز الخدمات على مستوى البلدية حيث تستقبل الوثائق الخاصة على الشباك الوطني وهذا الجهاز لديه نوعين من البطاقات الأولى خاصة بالشباك الوطني والثانية خاصة بالشباك المحلي حيث يمنع استخدام ويفي wifi أثناء العمل.

3- طريقة سير الأوامر والأعمال في نظام المعلومات بالبلدية:

يمثل الشكل الموالي طريقة نقل المعلومات والبيانات من الجهة المرسلة إلي الجهة المستقبلة حيث تستقبل كل البيانات المرسلة من طرف الجهة المركزية إلى البلدية حيث تقوم هذه الأخيرة بتوزيع معلومات النظام إلى باقي مصالح البلدية وأما المعلومات السرية فيتم حفظها.

الشكل (4-3) طريقة سير الأوامر داخل نظام المعلومات.



المصدر: نموذج مقدم من طرف مهندسة الإعلام للبلدية.

تقوم مهندسة الإعلام الآلي بمحاورة نظام المعلومات عن طريق الشبكات المتوفرة لديها، ثم تنتقل البيانات إلى الموجهات وقبل وصول هذه البيانات إلى الخادمات تمر أولا عبر الجدار الناري الذي يقوم بدور الحماية فتدخل البيانات إلى الخادم على شكل معطيات ليتم إنشاء لكل أمر نظام معلومات ويكون هذا الأمر موازي لأجهزة الاتصالات ويتم تنفيذه عبر الشبكة.

المطلب الثاني: السياسات الأمنية المنتهجة في البلدية.

تقوم سياسة أمن المعلومات في البلدية بالتركيز على عدة مستويات حيث تتجسد في العناصر الأساسية والمهمة والتي تدعو إلى الحماية المثلى لنظامها ويمكن شرحها كالتالي:

4-1- السياسة الأمنية الخاصة بالأفراد:

- ✓ يكون النظام ذو كفاءة عالية إذ تشرف على استخدامه مهندسة الإعلام الآلي حيث تستفيد هذه الأخيرة من دوريات تكوينية للإطلاع على كل جديد دخل حيز التطبيق بشأن الحفاظ على سلامة وأمن النظام وتكون هذه الدورات إضافية لاطلاع المستخدمين بهذه المستجدات.
- ✓ يتم توزيع البرنامج المخصص لكل مصلحة حيث تتوفر لدى كل عامل التكوين الخاص به أي يطلع على طريقة وكيفية استخدام النظام الخاص بمكتب عمله.
- ✓ كل عامل يستخدم نظام المعلومات بالبلدية يحصل على كلمة السر واسم مستعمل خاص به وكذا نموذج مخصصة له.
- ✓ كل نشاط أو عملية حدثت على مستوى النظام يسجل باسم العامل الذي قام بها.

4-2- السياسة الأمنية الخاصة بمكان العمل:

- ✓ مكان وجود خادمات قاعدة البيانات هو مكان مغلق ومحمي حيث يمنع دخول أي عامل أو موظف إلى هذا المكتب إلا المسؤولة عنه وهي مهندسة الإعلام الآلي.
- ✓ يتوفر المكتب على تكييف جيد وخاص لضمان سلامة الأجهزة مع وجود مولدات كهربائية لتجنب إطفاء أجهزة النظام مثل الخادم serveur أثناء حدوث انقطاع كهربائي.
- ✓ وجود مضادات الحرائق.

4-3- السياسة الأمنية الخاصة بالأجهزة:

- ✓ تستخدم البلدية أجهزة خوادم عالية الأداء وذات سرعة فائقة.
- ✓ تتوفر الأجهزة على ملحقات التبريد الملائمة وكذا تأمين الكهرباء في حالة الانقطاع.
- ✓ توجد حواسب نهائية لاستخدام النظام في مصالح متنوعة في البلدية حيث يكون أداء هذه الحواسب مقبول ومتقارب ومخزنات متوفرة و كافية.
- ✓ شبكة محلية تربط الخوادم عن طريق بروتوكول TCP/TP.
- ✓ أجهزة اتصال، هاتف، فاكس متوفرة وتستخدم في كثير من الأحيان.
- ✓ الطابعات متوفرة سواءا مركزية أو شخصية.
- ✓ وجود كمبيوتر خاص بالداخل والخارج أي يهتم بإعداد مختلف الوثائق ليتم إرسالها إلى المركز وهذا الجهاز مرتبط بالخادم وهو منعزل تماما عن الانترنيت.

- ✓ يمنع الموظفين من استخدام الأقراص الضاغطة الشخصية في أجهزة البلدية لمنع دخول فيروسات منها.

4-4- السياسة الأمنية الخاصة بالبرامج:

تهتم هذه السياسة بالتطبيق الجيد لسياسة أمن المعلومات على مستوى هذه البرامج الموجودة على الأجهزة المختلفة بالمؤسسة لضمان سلامة نظام معلوماتها، حيث تستخدم البلدية برنامج Windows 2008 بالنسبة للخادم بالإضافة إلى استخدام ويندوز7 في الحواسب الخاصة بالمصالح البلدية وينقسم إلى:

أ- السياسة الأمنية على الخوادم:

- ✓ يكون برنامج تسيير قواعد البيانات عالي الأداء وكذلك الحال لنظام التشغيل حيث يكون البرنامج الرئيسي عبارة عن مجموعة من الوحدات المترابطة ذات مفتاح خاص به.
- ✓ وجود نسخ احتياطية (يومية وشهرية)، فالنسخ الشهرية يتم في حوامل خارجية (الأقراص الضاغطة) وتحتفظ بها مهندسة الإعلام.
- ✓ استخدام مضاد الفيروسات Kaspersky ويكون متداخل مع الجدار الناري حيث يتم كل سنة إعادة برمجته وتأهيله، كما تقوم المشرفة على الإعلام الآلي بمراقبة كافة الملفات وتدقيقها ليتم حفظها في disque dure الخاصة بالمصلحة البيومترية والحالة المدنية.
- ✓ إنشاء حسابات خاصة لكل الموظفين حيث يكون لكل موظف اسم وكلمة مرور خاصة به إذ تقوم مهندسة الإعلام بمراقبة عملهم من مقر عملها دون التنقل من مصلحة إلى أخرى إلا لضرورة قصوى.
- ✓ في حالة حدوث أي خلل أو عطل للخادم الرئيسي تنتقل المراقبة آليا للخادم المرافق الخاص بقاعدة البيانات ليعوض الخادم المعطل.
- ✓ وجود برنامج مخصص للحماية حيث يقوم هذا الأخير بمعالجة الأعطال التي تصيب الأجهزة فيقوم بأخذ صور لإعادة النظام كما كان من قبل.

ب- السياسة الأمنية على مستوى حواسب الموظفين:

من أجل تنفيذ مهام البلدية على أكمل وأحسن وجه والحفاظ على نظام معلوماتها لابد من الموظفين والمستخدمين احترام الإجراءات الأمنية التالية والعمل بها:

- ✓ أنظمة لويندوز من نسخ مختلفة.
- ✓ مضاد الفيروسات مركزي مثبت على كافة الحواسيب.
- ✓ اتصال الانترنيت متوفر بشكل واحد وهي الشبكة ويمنع استخدام الويفي وتكون الانترنيت متمركزة فقط على بعض الحواسب.

- ✓ تكون البرامج مختلفة لأغراض متفرقة.
- ✓ يجب على الموظفين استخدام أدوات البريد الالكتروني من أجل العمل فقط.
- ✓ عدم ترك وسائل الحفظ الالكترونية (الأشرطة، والأقراص الصلبة وغيرها) في أماكن مفتوحة يسهل الوصول إليها.
- ✓ إيقاف البرنامج المستخدم وغلق الجهاز الخاص وعدم إيقافه عن طريق نزع السلك الكهربائي.

المبحث الثالث: المعوقات التي تواجه نظام أمن المعلومات والحلول المقترحة.

تناول هذا المبحث أهم المشاكل التي تعيق هذا الموضوع وأبرز السلبيات التي يتميز بها نظام امن المعلومات وكذا اختبار صحة الفرضيات، مع تقديم مجموعة من الحلول التي تصبو إلى نجاح السياسة الأمنية.

1- المعوقات التي تواجه نظام امن المعلومات:

من خلال تحليل نتائج المقابلة والملاحظة تمكنا من تحديد مختلف المعوقات التي يمكن أن تصيب النظام وتحول دون إنجاح السياسة الأمنية والتي تعرقل سير العمل الإداري وعدم استمرار يته، حيث تظهر هذه المعوقات في:

- ✓ عدم وجود مراقبة ومتابعة مستمرة بشأن اتخاذ الإجراءات الأمنية على مستوى البلدية(اللامبالاة).
- ✓ في حالة انقطاع التيار الكهربائي يتوقف الموظفين عن العمل رغم توفر المولدات الكهربائية وعدم احترامهم لمواقيت العمل.
- ✓ عدم وجود اتصال بين الطابعة المركزية والنظام ووجود تعطل في كثير من أجهزة البلدية.
- ✓ تنقل الموظفين بين المكاتب واستخدام أجهزة من طرف جميع الموظفين إذ يتم التداول على جهاز واحد من طرف هؤلاء الموظفين مما يزيد من نقص الخدمة المناسبة وكثرة الأخطاء في الشهادات المدنية.
- ✓ انعدام التكوين والكفاءة في صيانة الأجهزة المعطلة كآلات الطباعة مما يؤدى إلى تنقل التقنيين من أجل إصلاحها والذي يؤدي إلى توقف العمل لفترة معينة بسبب ذلك.
- ✓ نقص الخبرة وانعدام المسؤولية بين أصحاب العمل والموظفين.
- ✓ نقل الملفات الخاصة بالبلدية عبر الأقراص الصلبة أو ما يسمى فلاش ديسك بين الأجهزة التي ينجم عنها خلق فيروسات مختلفة والتي تؤدى إلى إتلاف الملفات أو النظام.
- ✓ عدم تجهيز مكتب الأجهزة كما يجب فمعظم الأسلاك التي تربط الأجهزة بعضها ببعض موزعة على الأرض بشكل عشوائي.

- ✓ استخدام لوحة مفاتيح كهربائية واحدة تخدم مكتب الأجهزة الالكترونية وجميع المكاتب المرتبطة بالمصلحتين مما يؤدى إلى خطر الحمولة الكهربائية الزائدة والتي تنجم عنها انقطاع الكهرباء بشكل مستمر أو نشوب حرائق ناتجة عن التيار الكهربائي.
- ✓ عدم التحقق من برمجة التثبت التلقائي لمضادات الفيروسات على مستوى كافة أجهزة البلدية من طرف الموظفين ونقص المعرفة بضروريات الحماية الواجبة توفيرها لمثل هذه الخدمات العامة.
- ✓ وجود مهندس واحد على مستوى البلدية والمكلف بمراقبة ومتابعة جميع مصالح البلدية مما يؤدى إلى تباطأ العمل نظرا لكثرة الاستخدامات للأجهزة أي عند حدوث مشاكل في المكاتب دفعة واحدة لا يمكنه مواجهة المشاكل وحده وضرورة وجود مساعد تقني يتولى مثل هذه الأمور العالقة.

المطلب الثاني: الحلول المقترحة.

من خلال دراستنا لموضوع نظام أمن المعلومات ومعرفة وجهات نظر العديد من الجهات والنتائج المتوصل إليها سنقترح بعض الحلول التي تضمن نسبة معتبرة من الأمن وهي:

- ❖ ضرورة توفير عنصر الرقابة الشاملة و الفعلية لمختلف مصالح البلدية.
- ❖ تكوين العمال وإعطائهم نظرة حول كيفية استخدام النظام والتزامهم بخطوات السياسة الأمنية وكذا التقيد بالقوانين السارية في المنظمة بخصوص هذا الموضوع.
- ❖ العمل على توفير بيئة ملائمة لحفظ الأجهزة الالكترونية وطريقة توصيلها وكذا حسن استخدامها ويكون فقط في نطاق العمل.
- ❖ إصدار تقارير ومذكرات تضم التوجيهات والنصائح التي ينبغي على المستخدم إتباعها و تطبيقها بخصوص نظام أمن المعلومات أثناء أداء وظائفه.
- ❖ الاستغلال الأمثل للبرامج الموجودة و ضرورة امتلاك الإدارة إستراتيجية واضحة في مجال نظام امن المعلومات.
- ❖ ضرورة وجود عمال الصيانة للأجهزة الكهربائية على المستوى الداخلي للبلدية.
- ❖ وجود حلول بديلة للمخاطر التي يتعرض لها النظام.
- ❖ تعميم مبدأ السرية على كافة ملفات ووثائق البلدية.
- ❖ تصنيف البيانات التي يمكن أن تتعرض للإتلاف والضرر، وتوفير الوسائل اللازمة للسيطرة على هذه الأضرار.
- ❖ توفير الآليات اللازمة لاسترجاع الملفات الضائعة والتي أتلفت.
- ❖ محاولة مواكبة جل المعوقات التي تهدد النظام والسعي للقضاء عليها.

خلاصة الفصل:

تضمن هذا الفصل الدراسة الميدانية والتي شملت بلدية سوق الاثنين التابعة لدائرة معاتقة وذلك من أجل معرفة أهمية نظام أمن المعلومات في تحديد مدى كفاءة وفعالية البلدية، حيث تم التطرق إلى الطريقة المستخدمة، وعرض أهم نتائجها والتي تضمنت نظام أمن المعلومات ونتائج كل من المقابلة والملاحظة والتي أضفت على إبراز الايجابيات التي تعود للنظام من سرعة التنفيذ وكذا سهولة مراقبة أعمال المصالح بالإضافة إلى أنه يساعد على اتخاذ القرارات والتدابير اللازمة لمواجهة أي خطر محدق من خلال استعمال ملحق النظام وتطبيقه.

كما يقوم باختبار صحة الفرضيات المبنية وكذا الإجابة على الإشكالية الرئيسية والتي تبين كفاءة و فعالية نظام أمن المعلومات في المؤسسة.

خاتمة

نستنتج من خلال دراستنا لموضوع نظام أمن المعلومات أن هناك العديد من المخاطر والمعوقات التي تعيق استمرارية النظام و حداثته، لذا قامت مختلف الجهات الوطنية والدولية برسم سياسة أمنية هادفة إلى التحسين المستمر لاستخدامات النظام والتي تدعو إلى تطبيق مجموعة من القوانين والتشريعات التي تحول دون انتشار هذه المخاطر وتسعى لتفادي قرصنة المعلومات و تزويرها، لذا وجب على جميع المنظمات انتهاج هذه السياسة منعا من ضياع المعلومات و التمسك بمصداقيتها.

يعد نظام أمن المعلومات من أكثر الأساليب انتشارا في زمن العولمة حيث أن المنظمات اليوم أصبحت تعتمد في تنفيذ سياستها وبرامجها على الأجهزة الالكترونية، مما دعي إلى تبني إستراتيجية محكمة والتي تقوم على حماية جميع موارد المنظمة سواء داخليا أو خارجيا، وهذا ما يساهم في ضمان استمرار فعالية نظام المؤسسة بتحقيق السرية التامة للمعلومات.

قائمة المراجع

قائمة المراجع

- المراجع باللغة العربية

أولا: الكتب

1- همشري، عمر أحمد. **الإدارة الحديثة للمكتبات ومراكز المعلومات**.عمان: دار صفاء للنشر والتوزيع، ط.2، 2010.

2- الطائي، محمد عبد حسين، الكيلاني ينال محمود. **إدارة أمن المعلومات**.عمان: دار الثقافة للنشر و التوزيع، 2015.

3- داود، حسن طاهر. **الحاسب وأمن المعلومات**. الرياض: مكتبة الملك فهد الوطنية، 2000.

4- الغثير، خالد بن سليمان، القحطني محمد بن عبد الله. **أمن المعلومات**. الرياض: فهرسة مكتبة الملك فهد الوطنية أثناء النشر، 2009.

5- الجنبيهي، منير محمد، الجنبيهي ممدوح محمد. **أمن المعلومات الاليكترونية**. الإسكندرية: دار الفكر الجامعي، 2005.

6- الصباغ، عماد، **نظم المعلومات ماهيتها ومكوناتها**. الدوحة: جامعة قطر،2000.

7- جمعة، النجار فايز، **نظم المعلومات الإدارية منظور إداري**. عمان: دار حامد للنشر والتوزيع، ط.2، 2010.

8- البداينة، ذياب، **الأمن وحرب المعلومات**. عمان: دار الشروق، 2002.

9- المدادحة، أحمد نافع، الذيابات عدنان عبد الكريم، **اقتصاديات المعلومات والمعرفة**. عمان: مكتبة المجتمع العربي للنشر والتوزيع، 2014.

10- ربحي، عليان مصطفى، **اقتصاديات المعلومات**. عمان: دار صفاء للنشر والتوزيع، 2010.

11- النوايسة، عوض غالب، **مصادر المعلومات في المكتبات ومراكز المعلومات**. عمان: دار صفاء للنشر والتوزيع، ط.2، 2015.

12- قنديلجي، عامر إبراهيم، النجار حسن رضا، **علم المعلومات والنظم والتقنيات**. عمان: دار المسيرة للنشر والتوزيع والطباعة، 2015.

13- المدادحة، أحمد نافع، **نظم المعلومات المحوسبة ودورها في مجال المكتبات**. عمان: مكتبة المجتمع العربي للنشر والتوزيع، 2014.

ثانيا: المجلات.

14- زغنوف، عبد الغاني." المعلومة وأهميتها في المجتمع المعلوماتي"، **مجلة البحوث والدراسات الإنسانية**، سبتمبر2014.

15- معوج، عبد الحكيم. "أمن نظام المعلومات وأهميته في ظل تطورات تكنولوجيا المعلومات والاتصالات"، **مجلة فكر ومجتمع**، الجزائر، طاكسيج كوم، 2015.
16- النجار، فايز الجمعة. "نظم المعلومات وأثرها في مستويات الإبداع"، **مجلة جامعة دمشق للعلوم الاقتصادية و القانونية**، م.26، ع.2 (2010).
17- إسماعيل جبوري، ندى." حماية أمن أنظمة المعلومات"، **مجلة تكريت للعلوم الإدارية والاقتصادية**، م.7، ع.21 (2011).
18- عبد الستار عبد الجبار الحافظ، على. " دور ISO27001:2005 في تعزيز مفهوم إدارة دورة حياة المعلومات (نموذج مقترح)"، **مجلة تكريت للعلوم الاقتصادية والإدارية**، م.6، ع.17 (2010).
19- عبادة العربي، أحمد." معيار المنظمة الدولية للتوحيد القياسي ايزو 27002 (ISO/IEC 27002) لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية، **مجلة جامعة طيبة للآداب والعلوم الإنسانية**، م.4، ع.7 (2014).
20- الزهراني، سعيد بن محمود." المواصفة القياسية ISO27001، **مجلة عالم الجودة**، ع.3 (أوت 2011).
21- مزيود، سليم."الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"، **المجلة الجزائرية للاقتصاد والمالية**، ع.1 (أفريل 2014).
22- عبد الله حاج، سعيد." تقييم نظام الحكومة الالكترونية في الجزائر"، **مجلة دولية علمية محكمة**، ع.2 (أكتوبر 2015).

ثالثا: الوثائق الرسمية.

23- الجمهورية الجزائرية الديمقراطية الشعبية،الجريدة الرسمية العدد 47، **القانون رقم 04-09** المؤرخ في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
24- الجمهورية الجزائرية الديمقراطية الشعبية، الجريدة الرسمية العدد 6، **القانون رقم 15-04** المؤرخ في 1 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.

رابعا: الدوريات أو المؤتمرات الدولية.

25- بوفاس الشريف، طلحي فاطمة الزهراء، "نحو بناء نظم لإدارة حماية المعلومات في المؤسسات الجزائرية"، **المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقظة الإستراتيجية ونظم المعلومات في المؤسسة الاقتصادية**، أيام 30/29 أفريل 2014، جامعة باجي مختار عنابة.

26- ناجي الزهراء،" التجربة التشريعية في تنظيم المعاملات الالكترونية المدنية والتجارية"، **المؤتمر العلمي المغاربي الأول حول المعلوماتية و القانون المنعقد في الفترة من 28 إلى 29 أكتوبر 2009.**

خامسا: الرسائل الجامعية الغير منشورة.

27- رجم، خالد، **"أثر نظام معلومات الموارد البشرية علي أداء العاملين، دراسة حالة مؤسسة شي علي بسطيف خلال 2011"**، رسالة ماجستير، جامعة ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير،2011.

28- مناصرية، إسماعيل،" **دور نظام المعلومات الإدارية في الرفع من فعالية عملية اتخاذ القرارات الإدارية"**،رسالة ماجستير، جامعة مسيلة: كلية العلوم التجارية وعلوم التسيير، 2014.

29- مرمي، مراد، **"أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة الجزائرية**، شركة chi ali profiplax بسطيف"، رسالة ماجستير، جامعة سطيف: قسم العلوم الاقتصادية، 2010.

30- جمعون، محمد ، مناعي مونير، **"أهمية نظام المعلومات التسويقي في اتخاذ القرارات التسويقية"**، رسالة ماستر، جامعة البويرة، كلية العلوم الاقتصادية والتجارية، 2014.

31- قاعود، عدنان محمد، " **دراسة وتقييم نظام المعلومات المحاسبية الالكترونية في الشركات الفلسطينية"**، رسالة ماجستير، جامعة غزة: كلية التجارة، 2007.

32- الشيخ، ياسين، **"أمن نظم المعلومات الرقابة"**، رسالة ماجستير، جامعة دمشق:المعهد العالي للتنمية الإدارية، 2010.

33- زكرياء ،أحمد عمار،" **حماية الشبكات الرئيسية من الاختراق والبرامج الضارة"**، رسالة ماجستير، بغداد: كلية الدراسات العليا، 2011.

34- براهمي، حنان، " **جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية"**، أطروحة دكتوراه، جامعة بسكرة: كلية الحقوق والعلوم السياسية، 2015/2014.

35- عزولة، طيموش، فريدة علاوات، **"التوقيع الالكتروني في ظل القانون رقم 15-04"**، مذكرة ماستر، جامعة بجاية: كلية الحقوق والعلوم السياسية، 2015 /2016.

36- طمين، سهيلة، **"الشكلية في عقود التجارة الالكترونية"**، رسالة ماجستير، جامعة تيزي وزو: كلية الحقوق، 2011.

37 – معيزي، ندا، **"النظام القانوني للتصديق الالكتروني"**، مذكرة ماستر، جامعة ورقلة: كلية الحقوق والعلوم السياسية، 2015.

38- هنشور وسيمة، مصطفى، " **النظام القانوني للتجارة الالكترونية في التشريع الجزائري والمقارن"**، رسالة دكتوراه، جامعة مستغانم: كلية الحقوق والعلوم السياسية، 2016.

سادسا: المواقع الالكترونية.

39- "نظم إدارة الجودة"، في: **http¡//www.gcKw.com/ISO-FAQS-AR.asp ? SPID=67.**

40- منتديات اليسير للمكتبات وتقنية المعلومات، "المعايير العالمية لأمن المعلومات"، في: **http://www.alyaseer.net/Vb/Shouwthread.php ?t=25671.**

41- أبو حجر، سامح رفعت، محمد عبد العزيز، أمنية. "دور آليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر أمن المعلومات للحد من التلاعب المالي الالكتروني في الوحدات الالكترونية"، في:

http://www.Kantakji.com/media/175569/%D8%AF/%D9%88%D8%B1% D8% A2%D9%84%D9%....

42- شهادة الأمن والسلامة ISO 27001، في:

http://www.iehad.com/index.php/2011-10-03.12-05-36/2012-06-21-22-31-37.html..

43- الهادي محمد، محمد. " توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية" في: **http://www.cybrarians.info/journal/n...o-Secuirty.htm.**

44- أسس ومبادئ نظام امن المعلومات ISO27001، في:

http://www.qms.org.sa/qms/certificates-ar/iso-27001

45- عاقلي، فضيلة. "الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري"، في:

http://jilrc.com/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9%D8%A7%...

المراجع باللغة الفرنسية:

46- balle, Francis. **dictionnaire des medias,** paris : Larousse, 1998.

الفهـــــــــرس

الفصل الثالث: واقع نظام أمن المعلومات في بلدية سوق الاثنين ولاية تيزي وزو.

فهرس الجداول

فهرس الأشكال

ملخص الدراسة:

تعد المعلومة الغاية التي تبرهن صحة إثبات الفرضيات ولهذا فان قابلية استخدامها في الميدان يتطلب التحقق من قدرتها لتجاوز مختلف أساليب عرقلة استخدامها وعليها انشأ نظام المعلومات فنجد أن خصائص ومكونات نظام المعلومات تؤدي دور فعال في صيانة المعلومة ذلك بإعطاء تغذية سليمة للبيانات المتعلقة بالمعلومة المراد الحفاظ عليها عن طريق فرض رقابة شاملة لمنع انحراف هذه الأخيرة عن هدفها، ويختلف نظام المعلومات باختلاف ميادين استخدامه والبيئة التي تحيط بها فيتعلق النظام المعلوماتي بطبيعة المعلومات المراد تناولها وما تحمله من خصائص وميزات وأيضا مصادر استخلاصها التي يجب التقيد بها قبل الشروع في معالجتها ولهذا ليس من السهل إدماج المعلومات بنظام يليق بها إلا بدراسة معمقة لها عن طريق مكونات النظام المعلوماتي التي تعمل على التوافق بين المعلومات وبيئتها، وعند ظهور موجة التسارع لكسب المعلومات والاحتفاظ بها انبثقت في الأفق الرغبة الملحة للمدراء ذوي الشركات والمؤسسات العمومية لإيجاد وسائل لحماية المعلومات من القرصنة الخارجية ولهذا استخدمت الإدارة في مختلف المؤسسات نظام امن المعلومات لتفادي الوقوع في معضلة الاختلاس الالكتروني للبيانات التي تمتلكها هذه الأخيرة بحيث يعمل امن نظام المعلومات بأبعاد تجعله يلم بكافة المجالات التي تأتي منها المعلومة ونظرا لضمانه السرية في التخزين والإرسال فهو المعتمد من قبل المؤسسات، ومما سهل من عمل وحماية المعلومات الجهود الدولية الرامية بنظمها الأمنية للحفاظ على سلامة المعلومة وذلك وفقا لمتطلبات المؤسسة عن طريق نظام ISO الذي برمج لخدمة والتنسيق بين المؤسسات وفقا للمعايير الدولية، كما أن الجزائر أعطت أهمية خاصة لتأمين المعلومات في مؤسساتها الإدارية وذلك بسياسة القوانين الميدانية لمخترقي المواقع الإدارية والتنويه بالجريمة الالكترونية بمختلف أشكالها كطريقة لفساد عمل الإدارة.