المؤتمر الدولي الثاني للذكاء الاقتصادي حول:

"اليقظة الاستراتيجية و نظم المعلومات في المؤسسة الإقتصادية "

أيام 30/29 أفريل 2014 جامعة باجي مختار / عنابة

الورقة البحثية المشارك بها ضمن المحور الخامس في إطار فعاليات الملتقى بعنوان:

نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية

من إعـداد الباحثان:

الاسم واللقب: د. الشريف بوفاس ، أستاذ إدارة الأعمال، رئيس قسم علوم التسيير

الاسم واللقب: أ.فاطمة الزهراء طلحي، أستاذة إدارة الأعمال

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

جامعة محمد الشريف مساعدية سوق أهراس الجزائر

البريد الإلكتروني: achraf1boufas@yahoo.fr

البريد الإلكتروني: fatmazohratalhi@yahoo.fr

الهاتف:0670013216

الهاتف: 0771334029

الملخص:

يلعب أمن المعلومات دورا مهما في حماية أصول المؤسسة، و قد أصبح يشكل هاجسا كبيرا في كل من الحكومة وقطاع الأعمال. لذلك ظهرت الحاجة إلى وضع مجموعة من المعايير التي يمكن من خلالها تحقيق مستوى ملائم من الأمن.

تعد ISO 27001 مواصفة متقدمة يمكن من خلالها تلبية متطلبات المؤسسة من خلال إقامة نظام إدارة حماية المعلومات، يصلح لكافة المنظمات سواء كانت صناعية أو خدمية، فضلا عن تطبيق، تشغيل، مراقبة، و مراجعة النظام ككل، كذلك يمكن اعتباره مدخلا للتحسين المستمر لنظام توثيق وإدارة المعلومات.

جاءت هذه الورقة البحثية لتوضيح مفهوم المواصفة الدولية ISO 27001 و تبيان دورها في إتاحة الفرص والقدرات والقابليات أكثر في التعامل مع المعلومات والبيانات التي تتسم بالتزايد و التعقد الكبيرين في منظمات الأعمال الإنتاجية منها والخدمية، مع محاولة إسقاطها على واقع الحال و إمكانية الإستفادة منها في بناء نظم لإدارة و حماية المعلومات في المؤسسات الجزائرية.

الكلمات المفتاحية: المواصفة الدولية ISO 27001، أمن المعلومات، نظم إدارة و حماية المعلومات.

Abstract:

Information security plays an important role in protecting the assets of the institution, and has become a major concern in both the government and the business sector. Therefore there is a need to develop a set of criteria by which to achieve an appropriate level of security.

The ISO 27001 specification developed by which to meet the requirements of the institution through the establishment of a management information protection, fit for all organizations, whether industrial or service, as well as the application, operation, monitoring, and review the system as a whole , as well as can be regarded as an input for continuous improvement of the documentation system and management information.

Came this paper to illustrate the concept of international standard ISO 27001 and demonstrate its role in providing opportunities, capacities and capabilities more in dealing with information and data that are complexity of big business organizations productive ones and service , with an attempt to overthrow the reality of the situation and its potential in building systems for the management and protection of information in the Algerian institutions .

***Keywords*:** International Standard ISO 27001, the information security, systems management and protection of information.

نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية

د/ بوفاس الشريف، جامعة محمد الشريف مساعدية سوق أهراس

أ/ طلحي فاطمة الزهراء، جامعة محمد الشريف مساعدية سوق أهراس

مقدمة:

إن التطور الهائل في مجال الإعلام الآلي و تقنيات المعلومات الناتج عن الثورة التقنية، والطفرة الكبيرة التي حدثت في وسائل الاتصالات، وشبكات المعلومات والدخول في عصر العولمة والإنترنت، صاحبه ظهور مخاطر ومهددات جديدة في الساحة الوطنية و العالمية والمتعلقة بأمن المعلومات مما يستدعي أخذ كافة الوسائل المتاحة والممكنة لأمن نظم المعلومات و حمايتها، باعتبارها مجموعة من الإجراءات والتدابير الوقائية التي تستخدم للحماية من جرائم الحاسوب والإنترنت، ومهددات استخدام التقنية التي قد تطال إما سرية المعلومات ،أو سلامتها، أو توفرها ،أو قد ترتبط بأجهزة الحاسوب نفسها كأن تطالها السرقة ،أو في استخدام أجهزة الحاسوب وشبكات المعلومات كوسيط في إرتكاب الجرائم. لهذا قامت منظمة المقاييس الدولية ISO بتطوير سلسلة جديدة متخصصة بحماية المعلومات وهي ISO27001:2005 والتي يطلق عليها نظم إدارة حماية المعلومات (المتطلبات)، إذ تزود المواصفة ISO 27001 المنظمة بنموذج مشترك لتطبيق وتشغيل وتحسين نظم إدارة حماية المعلومات.

مشكلة البحث:

تكمن في دراسة الإطار النظري لأمن المعلومات و المواصفة القياسية ISO 27001 :2005 و مدى إدراك المؤسسات الجزائرية لأهميتها و استعدادها للتوافق مع هذا المعيار الدولي و الاستفادة من مزايا التطبيق.

فرضية البحث:

ينطلق البحث من فرضية مفادها أن معظم المؤسسات الجزائرية تعاني من نقص شديد في التحكم في المفاهيم المتعلقة بأمن المعلومات و المواصفة القياسية ISO 27001 :2005 ، ممّا يتطلب التحسيس و بذل مجهودات أكبر لرفع التحديات بغية بناء نظم لإدارة حماية المعلومات و الاستفادة من مزايا التطبيق.

هيكلة البحث:

للإجابة عن الإشكالية السابقة نقترح المحاور التالية:

المحور الأول: أمن المعلومات

المحور الثاني: المواصفة الدولية ISO 27001

المحور الثالث: أمن المعلومات و ضرورة الاتجاه إلى المواصفة القياسية ISO 27001 :2005 في المؤسسات الجزائرية

أولا/ أمن المعلومات:

1- مفهوم أمن المعلومات:

يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين بالاطلاع عليها أو استخدامها [1].

إن مصطلح أمن المعلومات هو تعبير واسع يغطى مجموعة كبيرة و مرتبة من النشاطات في المؤسسة، وهو يتضمن كل المنتجات و العمليات التي تتم بهدف منع وصول الأفراد غير المصرح لهم بتعديل البيانات، حذف المعلومات[2].

أمن المعلومات من الزاوية الأكاديمية هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها، ومن الزاوية التقنية هو الوسائل والأدوات والإجراءات اللاّزم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن الزاوية القانونية فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الإعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (جرائم الكمبيوتر والإنترنت) [3].

2- عناصر أمن المعلومات:

إن أغراض أبحاث واستراتيجيات ووسائل أمن المعلومات سواء من الناحية التقنية أو الأدائية، وكذا هدف التدابير التشريعية في هذا الحقل هو ضمان توفر العناصر التالية لأيّة معلومات يراد توفير الحماية الكافية لها: [4]

- **السرية أو الموثوقية**: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك .

- **التكاملية وسلامة المحتوى** : التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به، وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع .

- **استمرارية توفر المعلومات أو الخدمة** : التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها .

- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به** : و المقصود هو ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين .

3- تحديد المسؤوليات والواجبات الأمنية:

قبل تحديد نوع الحماية ودرجتها، يجب اتخاذ الإجراءات والخطوات الكفيلة التي تمكن من فرض الحماية المطلوبة متمثلة في تحديد المسؤوليات والواجبات. [5]

إن الإدارة العليا هي المسؤولة من توفير الأمن والحماية للمنشأة وهذه المسؤوليات تتدرج من مستوى إداري إلى آخر.

أ. مسؤولية قمة الهرم الإداري: هي وضع الإطار العام لسياسات أمن المؤسسة والإقرار بالمسؤولية عن حمايتها.

ب. مسؤولية إدارة أمن نظم المعلومات: تقع مسؤولية وضع السياسات الأمنية وتطبيقها على عاتق إدارة متخصصة مناط بها تطبيق رغبة الإدارة العليا في حماية المؤسسة وأصولها.

ج. مسؤولية مالك البيانات والمعلومات: تؤول ملكية المعلومات و نظم المعلومات و أصولها إلى جهات أو أفراد داخل المؤسسة، ويكون المالك هو المسؤول المباشر عن كل ما يتعلق بتأمين المصادر تحت ملكيته مثل تحديد نوع الحماية المطلوبة وتحديد الصلاحيات الممنوحة للمستخدمين ...الخ.

د. مسؤولية خدمة البيانات والمعلومات: وتتم عادة من موظفي التقنية والمسؤولية تقع على إدارة النظم وصيانة المعلومات وتحديثها وعمل النسخ الوقائي.

هـ. مسؤولية المستخدمين: هم الأشخاص الذين يقومون باستخدام البيانات بشكل روتيني من خلال الصلاحيات الممنوحة لهم

لأداء العمل بصورة لا تشكل تهديدًا لأمن نظم ومعلومات المؤسسة، وتقع حدود مسؤوليتهم في الاستخدام الشرعي للنظام في حدود صلاحياتهم.

4- مناطق أمن المعلومات و مستوياتها:

تصنف المعلومات من الناحية الأمنية إما كمعلومات سرية، خاصة، حساسة أو عامة.

تقع مسؤولية التصنيف على مالك المعلومات وغالبًا ما تقع على الإدارة العليا، و على المؤسسة وضع محددات التصنيف حتى تتمكن من وضع درجات سرية وحساسية المعلومات.

لتقييم وتصنيف مدى سرية وحساسية المعلومات بالمؤسسة ولتحديد نوع ودرجة الحماية الأمنية، فإن المحددات التي يمكن استخدامها هي: (6)

- فائدة المعلومات.
- أهمية وقيمة المعلومات.
- عمر المعلومات.
- حجم الخسائر التي قد تلحق بالمؤسسة عند كشف المعلومات.
- حجم الخسائر التي قد تلحق بالمؤسسة عند حدوث تعديل أو تلف بالمعلومات.
- القوانين واللوائح والمسؤوليات الخاصة بحماية المعلومات.
- من المصرح له باستخدام المعلومات؟
- من الذي سيقوم بصيانة المعلومات؟
- أين ستحفظ المعلومات؟
- من الذي يمكنه إعادة إصدار المعلومات؟
- أي نوع من المعلومات يحتاج إلى تصنيف خاص؟

تجدر الإشارة إلى أن تكلفة الحماية غالبا ما تكون عالية جدا، وعليه فان الإدارات العليا صاحبة القرار لها الخيار في حماية أنظمتها ومعلوماتها من حيث التكلفة و الإستفادة منها ودرجة المخاطر، أو أن تتحمل المخاطر إذا ما رأت في ذلك مصلحة للمؤسسة، إذ لا يعقل حماية ما قيمته عشرة دولارات بتكلفة قدرها ألف دولار. ولتحقيق الأهداف الأمنية في ظل التهديدات، لابد لأي

مؤسسة من اتخاذ الخطوات والإجراءات الكفيلة بحماية المؤسسة. ولا يتأتى ذلك إلاّ بإنشاء إدارة مختصة لأمن النظم والمعلومات، تطوير السياسات والمعايير والإجراءات مع الإلتزام التام بتطبيق وتنفيذ السياسات والإجراءات الأمنية.

1.4. مناطق أمن المعلومات: يمكن تحديدها في: [7]

أ. **أمن الاتصالات:** ويراد بأمن الاتصالات حماية المعلومات خلال عملية تبادل البيانات من نظام إلى آخر.

ب. **أمن الكمبيوتر:** ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها كحماية نظام التشغيل، و حماية برامج التطبيقات، وحماية برامج إدارة البيانات، وحماية قواعد البيانات بأنواعها المختلفة.

ولا يتحقق أمن المعلومات دون توفير الحماية المتكاملة لهذين القطاعين عبر معايير أمنية تكفل توفير هذه الحماية، ومن خلال مستويات أمن متعددة ومختلفة من حيث الطبيعة.

2.4. أنماط ومستويات أمن المعلومات:

إن إستراتيجية أمن المعلومات أو سياسة أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المؤسسة، وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها[8].

تتمثل أهم مستويات أمن المعلومات في: [9]

أ. **الحماية المادية** : وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول إلى الأجهزة الحساسة.

ب. **الحماية الشخصية** : وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن، إلى جانب الوعي بمسائل الأمن ومخاطر الاعتداء على المعلومات.

ج. **الحماية الإدارية** : ويراد بها سيطرة جهة الإدارة على إدارة نظم المعلومات وقواعدها، مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق باخلالات الأمن، ومسائل الإشراف والمتابعة لأنشطة الرقابة، إضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالاشتراكات الخارجية.

د. **الحماية الإعلامية– المعرفية** : كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة عند اتخاذ القرار بعدم استخدامها.

3.4. اتجاهات المخاطر والاعتداءات في بيئة المعلومات:

تطال المخاطر والاعتداءات في بيئة المعلومات أربعة مواطن أساسية هي مكونات تقنية المعلومات كما يلي: [10]

أ. **الأجهزة:** وهي كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها .

ب. **البرامج:** وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة فيه.

ج. المعطيات: إنها الدم الحي للأنظمة، وما سيكون محلا لجرائم الكمبيوتر، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم. والمعطيات قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين خارجه.

د. الاتصالات: وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا، وتتيح فرصة اختراق النظم عبرها كما أنها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي. ومحور الخطر هو الإنسان، سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام، فإدراك هذا الشخص حدود صلاحياته، وإدراكه آليات التعامل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، مسائل رئيسة يعنى بها نظام الأمن الشامل، تحديدا في بيئة العمل المرتكزة على نظم الكمبيوتر وقواعد البيانات.

5. نظم إدارة أمن المعلومات:

إن التطور السريع في عالم جرائم الحاسوب سابق لوسائل وبرامج الحماية، لذا لابد من تخصيص جهة محددة لإدارة هذه التغيرات ومواكبتها وسد الثغرات بمسؤولية، لذا كان ضروريا أن تنشأ دائرة تعنى بإدارة الأمن ومهيأة بكوادر مؤهلة وذوي خبرة، على أن تتمتع هذه الإدارة باستقلالية تامة وأن توضع في الهيكل التنظيمي في موضع يجعلها تعمل بفاعلية ودون مؤثرات وضغوط من الإدارات الأخرى، وتستمد هذه الإدارة قوتها من قناعة ودعم الإدارة العليا للمؤسسة لها.

إن إدارة أمن المعلومات مناطة بعدة مهام تشمل:

- تطوير السياسات والمعايير والإجراءات الأمنية وتطبيقها.
- المشاركة في تطوير وتقييم و اعتماد جميع النظم.
- مراجعة وتقييم النظم القائمة وتصحيح أوضاعها.
- تحديد الفجوة الأمنية وتحليلها.
- جلب وتركيب البرامج الخاصة بالحماية.
- التحكم في مستخدمي النظم ومنح صلاحيات تراخيص الاستخدام.
- مراجعة التقارير الرقابية.
- تقديم الاستشارات الأمنية.
- مراقبة أجهزة ونظم الحماية وتنفيذ الإجراءات المناسبة في حالة التجاوزات والاختراقات.

ثانيا/ المواصفة الدولية ISO 27001:

1- تعريف المواصفة:

تحدد المواصفة الدولية ISO 27001: 2005 متطلبات إنشاء و تطبيق و تشغيل مراقبة و إعادة النظر في صيانة وتحسين نظام موثق لإدارة أمن و سرية المعلومات من خلال الإطار العام لإدارة مخاطر العمل داخل المؤسسات. كما تحدد المواصفة متطلبات تطبيق ضوابط لأمن و سرية المعلومات بما يتناسب مع احتياجات المؤسسات أو بعض إدارتها أو جهات تابعة لها. [11] من الممكن أن تطبق هذه المواصفة بأية جهة مهما كان نشاطها أو مجال عملها حيث تم تصميمها لتضمن انتقاء و تطبيق الضوابط الأمنية الملائمة التي تحمي الأصول المعلوماتية بأية مؤسسة، و لكن أهم الجهات المستفيدة هي البنوك و شركات الاستثمار و مقدمي الحلول التقنية و

المنتجات الذكية و الشركات الصناعية و الشركات التي تمتلك أسرارا تجارية كبرى و الجهات الاستشارية و شركات المحاماة...إلخ.إضافة إلى الجهات الحكومية و المنشآت العسكرية و الأمنية التابعة لها.

تزود مواصفة ISO27001 إدارات المنظمات الصناعية والخدمية بتوجيهات لتطبيق نظم إدارة حماية المعلومات ،فضلا عن حصولها على شهادة الطرف الثالث الدولية لإثبات سيطرة المنظمة على حماية معلوماتها والتي تشغل طبقا لمتطلبات المعايير الدولية، بالإضافة الى مراقبة وإدامة نظام إدارة حماية المعلومات من قبل منظمة ISO، وبهذا يجب أن يخاطب نظام إدارة حماية المعلومات كل أطوار الهيكل التنظيمي، السياسات، خطط النشاط، المسؤوليات، الممارسات، الإجراءات، العمليات وأخيرا مصادر المعلومات. [12]

هو عبارة عن تطوير، تنفيذ، تشغيل،مراقبة،مراجعة،محافظة، وتحسين نظام أمن معلومات موثق في المنظمة يهدف إلى إدارة فعالة ومستمرة للمخاطر توفر حماية مناسبة للمعلومات حسب أهميتها.

ومعيار الإيزو 27001 عبارة عن معيار متكامل لبناء نظام أمن معلومات فعال قابل للتطوير المستمر ويخضع للتقييم من جهة مخولة بذلك مرتين خلال السنة ويعطي الحصول عليه مزيد من الثقة بالجهة الحاصلة على الشهادة من ناحية حمايتها لمعلوماتها ومعلومات عملائها. [13]

2- مميزات تطبيق المواصفة القياسية 2005: ISO 27001 بشأن أمن وسرية المعلومات:

يمكن أن نشير إلى بعض ميزات تطبيق المواصفة كما يلي: [14]

- المطابقة مع المتطلبات الرقابية للحفاظ على أمن وسرية البيانات.
- تصميم أفضل الضوابط الداخلية وأكثرها اقتصاديا بما يتناسب مع بيئة الأعمال وحجم النشاط.
- إنشاء السياسات والإجراءات الموثقة على أساس تقييم المخاطر ووضع نظم لمعالجة المخاطر المتوقعة.
- تخفيف تكاليف إعادة إنشاء قواعد بيانات وأنظمة آلية فيما إ ذا تعرضت للفقدان أو الاختراق.
- توحيد السياسات والإجراءات لكافة الوحدات التنظيمية في التعامل بشأن إدارة أمن وسرية المعلومات.
- تبوء موقع ريادي متقدم في ظل بيئة المنافسة في السوق.
- رفع درجة الوعي لدى الموظفين داخل كيان الأعمال بمفهوم إدارة أمن وسرية المعلومات.
- زيادة فاعلية وكفاءة تشغيل وإدارة نظم المعلومات، مما يوفر الوقت والموارد، وذلك من خلال تفعيل هندسة العمليات.
- ضمان استمرارية العمل في حالات الأزمات.
- اعتماد الضوابط الأمنية المناسبة والكافية لحماية المعلومات، وزيادة الثقة لدى كافة الأطراف المتعاملة مع كيان الأعمال.

إضافة إلى ذلك فمن أهم فوائد الشهادة هو وضع معالم أمن المعلومات في المؤسسة، و بناء نظام متكامل يعتمد على عمليات مستمرة يؤدي تطبيقها إلى الحماية المرجوة و التطور المستمر بناء على منهجية معتمدة، كما تعد الشهادة مؤشرا بالتزام المؤسسة على جميع مستوياتها بحماية المعلومات، و زيادة الثقة بالمؤسسة. [15]

3- خطوات تطوير نظام أمن المعلومات بناء على المعيار العالمي والحصول على شهادة الإيزو 27001:

ينقسم تطوير نظام أمن المعلومات إلى أربع مراحل مستمرة وهي التخطيط – التنفيذ– التأكد والمراجعة – التنفيذ و نوضح ذلك كما يلي: [16]

1.3– تكوين لجنة أمن المعلومات: وتعنى هذه اللجنة بـ:

- تطوير السياسة العامة لأمن المعلومات واعتمادها.
- تطوير أهداف أمن المعلومات والتأكد من توافقها مع أهداف المؤسسة.
- إدارة المصادر الخاصة بإدارة نظام أمن المعلومات.
- مراجعة نتائج تقارير تقييم المخاطر ومدى تأثيرها على العمل.
- تطوير خطط معالجة المخاطر.
- إدارة تنفيذ خطط معالجة المخاطر.
- التأكد من تطور نظام إدارة أمن المعلومات في المنظمة.
- التأكد من أن التعامل مع الأحداث الأمنية (مثل الوقوع تحت هجمات الكترونية، انتشار الفيروسات،...)يتم بشكل جيد.

2.3– أعضاء اللجنة: تحتاج اللجنة أن تدعم من الإدارة العليا بشكل مباشر وذلك لتفعيل نظام أمن المعلومات كما ينصح بأن يترأسها المدير التنفيذي أو من ينوبه كما يجب أن تحتوي اللجنة على أعضاء أصحاب قرار في المؤسسة ولهم علاقة مباشرة بإدارة المعلومات والأعمال ومثال ذلك: عضو من التشغيل، عضو من الشؤون الإدارية والمالية، عضو من إدارة شؤون الموظفين، عضو من إدارة الجودة، عضو من تقنية المعلومات، عضو من أمن المعلومات، عضو من إدارة المبنى، ونحوه ويعتمد ذلك على كل المنظمة والهيكل التنظيمي لها كما نشير إلى ضرورة تعيين مدير لنظام أمن المعلومات ويكون احد أعضاء هذه اللجنة.

3.3 – اختيار نطاق العمل والأهداف: يتم في هذه المرحلة تحديد النطاق الذي سيتم حصول الشهادة عليه على أن يكون اختيار النطاق بناء على أهداف وخدمات وأعمال المنظمة. فمثلا قد ترغب إدارة تقنية المعلومات بالحصول على شهادة الايزو 27001 على مركز البيانات والذي يحتوي على الخوادم ونحوها والتي بدورها تحتوي على جميع معلومات المنظمة (وهنا كان حماية المعلومات في النطاق يدعم حماية عمل المنظمة). ومن ما يميز هذا المعيار أنه يكفي لتحديد النطاق أن يكون حماية مصادر المعلومات في نطاق العمل يساعد في تحقيق أو دعم نطاق عمل المنظمة ولا يلزم الحصول على الشهادة على المنظمة ككل. وللتوضيح بالمثال قد تقوم شركة مصنعة للسيارات باختيار أن يكون المعلومات المتمحورة حول التصاميم الجديدة لمنتجاتها هو نطاق الشهادة ونلاحظ أن هناك معلومة نحتاج لحمايتها ونعني مواصفات وتصاميم السيارات وأيضا حماية هذه المعلومة يدعم أهداف المنظمة.

4.3–كتابة السياسة: بعد تحديد النطاق يلزم كتابة السياسة العامة لأمن المعلومات في النطاق، والتي تتضمن خطوط عريضة تضمن الالتزام بحماية المعلومات وتوضح التزام الإدارة العليا بأمن المعلومات، وقد يتم اعتمادها من أعلى جهة في المنظمة (بناء على اعتمادها من لجنة أمن المعلومات).

5.3– تطوير منهج تقييم المخاطر: والذي سيتم إتباعه خلال تحليل وتقييم المخاطر لمصادر المعلومات في نطاق العمل. ويحتوي ذلك على خطوات توضح عملية تحديد وتحليل المخاطر بحيث يتم معرفة أصول المعلومات (الكترونية، ورقية، أدوات أو أجهزة وأشخاص أيضا)، قيمة هذه الأصول، ومن ثم معرفة ما هي التهديدات والثغرات المحتملة ومدى تأثيرها على المعلومة سواء من ناحية التأثير على السرية أو سلامة المعلومة (تغييرها ونحوه) أو تأثيرها على توفر المعلومة. ويعتبر فهم سير العمل في نطاق العمل من أفضل

الوسائل لمعرفة ما هي الأصول ومعرفة مدى أهمية كل أصل. ومن هنا نحصل على المخاطر المحتملة على كل مصدر معلومات. ومن ثم يتم العمل على توفير الحماية اللازمة لأصول المعلومات وذلك باختيار طرق الحماية التي تتناسب مع طبيعة المنظمة وذلك باختيار طرق الحماية من قائمة يوفرها المعيار كملحق له. ولا يلزم اختيار جميع الطرق بل ما يلزم لحماية المعلومة واحتواء الخطر.

ويكون ناتج هذه المرحلة: تقرير تقييم وتحليل المخاطر، تقرير التعامل مع المخاطر وتقليلها بعد اختيار طرق الحماية اللازمة ويتضمن حساب المخاطر بعد تطبيق طرق الحماية للتأكد من مدى فاعليتها.

6.3– التعامل مع المخاطر: بناء على الخطوة السابقة وبعد اختيار طرق الحماية يتم كتابة وثيقة تحتوي على جميع المخاطر التي تم تحليلها وتقييمها وطرق التعامل معها والاختيار من قائمة طرق الحماية الواردة في الملحق ويتم توضيح ما هي الطرق التي لم يتم استخدامها وتوضيح سبب ذلك (ومن أمثلة أسباب عدم التطبيق: أسباب مادية، بيئية، وقتية، تقنية، وغيرها). ويتم رفع هذه الوثيقة إلى لجنة أمن المعلومات لمراجعة ما جاء فيها واعتمادها والتوجيه بتطبيق ما ورد فيها.

7.3 – خطة تنفيذ الضوابط الأمنية: بعد اعتماد الوثيقة السابقة يتم تطوير خطة تنفيذية لتطبيق ما ورد في المرحلة السابقة. وتحتوي الخطة على خطر تم تحليله وتقييمه، يتم تحديد طرق الحماية التي سيتم تنفيذها وتاريخ التنفيذ والمهام والمسؤوليات. كما نشير إلى أن طرق الحماية ليست بالضرورة أن تكون تقنية بل من الممكن أن تكون إجرائية، تنظيمية، أو تقنية.

8.3– التوعية الأمنية: يتم بعد ذلك عمل برنامج توعية أمنية للموظفين داخل نطاق العمل (والذي تم تحديده في الخطوة الأولى) وقد يشمل البرنامج على: عروض تقديمية توعوية، دورات تدريبية أو تعليم. ويحتوي البرنامج أيضا على توضيح لسياسات وإجراءات أمن المعلومات والتي تم تطويرها كجزء من المرحلة السابقة وتعريف الموظفين في نطاق العمل عن أي إجراءات جديدة والتأكد من توافق أعمالهم مع ما تمت كتابته في الإجراءات.

9.3– إجراءات المراقبة والتطوير المستمر لنظام أمن المعلومات: وتحتوي على:

- مراجعة الأحداث الأمنية والعمل على معرفة السبب الرئيسي والتعامل معه.
- مراجعة سياسة أمن المعلومات بشكل دوري والهدف من النظام. مراجعة تقارير تحليل وتقييم المخاطر ومستوى الخطر المقبول والمتبقي.
- مراجعة ما تم تطبيقه من طرق الحماية التي تم اختيارها من ملحق المعيار.
- مراجعة تقارير التدقيق الداخلي والخارجي. و رفع تقارير نتائج المراجعات للجنة أمن المعلومات و المسؤول عن نظام أمن المعلومات لاستخدامها كمدخلات لتطوير النظام بشكل عام. بحيث قد يشمل التطوير على: تطوير الهيكل التنظيمي، تطوير التقنية، معرفة التهديدات المستقبلية وبناء الخطط الملائمة للتعامل معها، فهم الأنظمة والقوانين الجديدة المتعلقة بنطاق العمل أو بالمنظمة ككل والتي بدورها ستؤثر على نطاق العمل وأمن المعلومات.

10.3 – المحافظة على نظام أمن المعلومات وتطبيق التطوير المقترح: ويتم هنا تطبيق ما توصل إليه في الخطوة السابقة واتخاذ ما يلزم لتصحيح بعض الأخطاء والتي تم استخلاصها من الأحداث الأمنية والتقييم الداخلي والخارجي ومحاولة منع حدوثها بالمستقبل. كما نشير إلى ضرورة تفعيل التواصل وتبادل المعلومات فيما يخص المحافظة على أمن المعلومات مع جميع المشاركين في نطاق العمل.

11.3 – التدقيق الداخلي: ويفضل أن يقوم بهذه المرحلة فريق مستقل عن الفريق الذي قام بتطوير نظام أمن المعلومات. يقوم فريق التدقيق بمراجعة السياسات والإجراءات ويتأكد من تطبيقها على أرض الواقع.

4. خطوات الحصول على الشهادة:

عند اكتمال جميع الخطوات السابقة يتم مراسلة الجهات المخولة بعمل تقييم نظام امن المعلومات والمعتمدة من المنظمة العالمية ISO وعند الإنفاق تنقسم مرحلة تقييم نظام أمن المعلومات إلى مرحلتين:

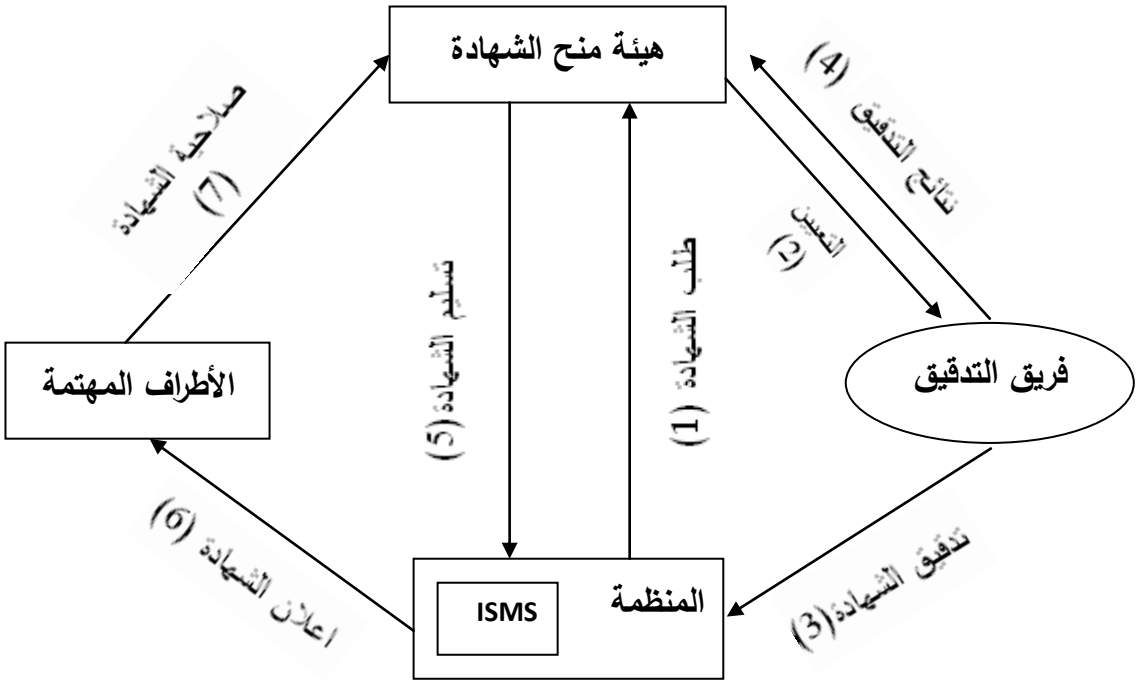
1.4– المرحلة الأولى مراجعة ما تم عمله من وثائق ومتطلبات: ومنها:

- وثيقة توضح الهدف من نظام امن المعلومات وتوضح نطاق العمل.
- سياسة أمن المعلومات.
- منهج تحليل وتقييم المخاطر.
- تقارير تقييم المخاطر.
- خطة تنفيذ تطبيق ما تم اختياره من أدوات.
- إجراءات التعامل مع الأحداث الأمنية.
- إجراءات الإكتشاف والتطوير.
- تقارير التقييم الداخلي.
- تعبئة نموذج التطابق مع المعيار والذي يشتمل على قائمة بالمخاطر و ما تم اختياره و استبعاده من أدوات التحكم بأمن المعلومات والمذكورة في الملحق كما يتوجب توضيح أسباب استبعاد أي من أدوات التحكم.

2.4 – المرحلة الثانية زيارة الموقع ومراجعة نطاق العمل وتطبيقه على ارض الواقع: حيث يقوم المراجع بالتأكد من تطبيق ما ورد في ما تم تقديمه من وثائق في المرحلة الأولى، وذلك بمقابلة الأشخاص المعنيين وزيارة ميدانية للمكاتب المشمولة في النطاق ومراجعة ما ذكر في الوثائق ومدى تطبيقة، ومن ثم يقوم بتقديم التقرير. ويحتوي التقرير على التوصيات التي يرى المراجع أنها قد تؤدي إلى تحسين أداء نظام أمن المعلومات ويحتوي على حالات عدم المطابقة وهي عبارة عن بعض متطلبات المعيار الأساسية والتي لم يتم إعدادها (مثل منهجية تقييم المخاطر أو إجراءات التصحيح والتقييم المستمر) أو إجراءات مكتوبة لم يتم تطبيقها. وبعد تقديم التقرير للمؤسسة يجب العمل على إجراءات تصحيحية وخطة للتنفيذ ويتم إرسالها للمراجع. وبعد مراجعتها يرفع المراجع تقريرا نهائيا لمنظمة الإيزو بالموافقة على منح شهادة المطابقة للمعيار العالمي الإيزو 27001.

الشكل التالي يوضح آلية المعالجات للحصول على شهادة ISO27001 :

الشكل رقم 01 آلية المعالجات للحصول على شهادة ISO27001



المصدر: علي عبد الستار عبد الجبار الحافظ، أحمد هاني محمد النعيمي: " دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (نموذج مقترح)"

5. **الخطوط العريضة لمحتويات الملحق A:**

1.5 – سياسة أمن المعلومات: مجموعة من القوانين والمعايير التي تتم كتابتها واعتمادها ومن ثم تطبيقها لحماية المعلومات في نطاق العمل الذي تم اختياره. ومثال ذلك: " تعتبر معلومات المنظمة أحد أصول المنظمة وتعد حمايتها أمر أساسي لاستمرارية العمل. وتعد المحافظة على صحة وسرية وسلامة المعلومات أمورا حتمية لتحقيق أهداف المنظمة التنظيمية والقانونية والتعاقدية. وبناء عليه سيتم اتخاذ جميع ما يوفر الحماية اللازمة لهذه الأصول سواء من الإستخدام الغير مصرح به أو التعديل أو الكشف عنها سواء كانت المحاولات عرضيه أو متعمدة. يلتزم جميع الموظفين والمتعاقدين والأطراف العاملة داخل المنظمة بحماية المعلومات وتنفيذ سياسات وإجراءات أمن المعلومات."

2.5 – تنظيم أمن المعلومات: ويهدف إلى التأكد من إدارة أمن المعلومات في المنظمة، وتوضيح المهام والمسؤوليات ذات العلاقة سواء داخل المنظمة من إدارات أو خارجها من جهات تتعامل معهما. ويعتبر وجود تنظيم واضح لأمن المعلومات في المنظمة مؤشر هام للالتزام في حماية المعلومات وهو أحد متطلبات المعيار العالمي. ويعد وجود لجنة أمن المعلومات أحد مؤشرات تنظيم أمن المعلومات.

3.5 – إدارة الأصول: يعرف الأصل على أنه أي شيء له قيمة للمنظمة، وتهدف إدارة الأصول إلى توفير حماية تتناسب وأهمية الأصول بحيث يتم أولا معرفة وتحديد جميع الأصول المادية (من أجهزة وخوادم وقواعد بيانات وموارد بشرية ونحوها)، أو غير المادية مثل سمعة المنظمة، ومعرفة مدى قيمة هذه الأصول، ويتم بعد ذلك التخطيط لحمايتها وتوفير الحلول المناسبة.

4.5– أمن الموارد البشرية (الموظفين، المتعاقدين، ...): ويعني به تحديد المسؤوليات والمهام للموظفين والمتعاقدين ونوحهم والإعتناء باختيارهم بما يتوافق مع المعلومات التي سيتعامل معها كل فرد بناء على سياسات أمن المعلومات. ومثال ذلك أنه عند الحاجة لتوظيف مدير قواعد بيانات على سبيل المثال (وبناء على أن قواعد البيانات للمنظمة تحتوي على جميع المعلومات الحساسة) يجب أن يتم أولا الاختيار بعناية ويتم بعد ذلك عمل التحقق من خلو سجله العملي من أي سوابق غير متلائمة مع الوظيفة التي سيعمل عليها، وعند التوظيف يتم تعريفه بالمهام والمسؤوليات وتوقيعه (كأي موظف) على وثيقة عدم إفشاء المعلومات والمحافظة عليها. بمعنى أن المعيار يعنى بعملية إدارة الموظفين كعملية متكاملة ابتداء من اختيار الموظف، قبل التوظيف،عند التوظيف، خلال التوظيف وممارسة الوظيفة ومن ثم عند إنهاء الخدمة. ويتم خلال التوظيف العناية برفع مستوى الوعي الأمني للموظفين عن طريق تقديم الدورات التدريبية والتوعوية. ويعني الإهتمام بإنهاء الخدمة أن يتم أولا التأكد من إنهاء جميع الإجراءات بالشكل المناسب مثل التأكد من إيقاف جميع حسابات المستخدم الذي أنهى خدماته مباشرة واسترجاع جميع ما لدية من أصول.

5.5– الأمن المادي والبيئة المحيطة بالمعلومات: وهو حماية موارد وأصول المنظمة من الوصول والعبث بها وذلك بتوفير أدوات حماية مناسبة للمباني ومركز البيانات (الذي يحتوي على الأجهزة والخوادم) والمكاتب والأجهزة. كما يجب أن الأخذ بعين بالاعتبار هنا المخاطر الطبيعية مثل الأمطار والعواصف ونحوها. ومن أدوات الحماية توفير سياسات وإجراءات للدخول إلى المبنى والدخول إلى مركز البيانات ونقل وتحميل الأجهزة من مكان إلى آخر سواء داخل المبنى أو خارجة.

6.5 – إدارة الإتصالات والتشغيل: وتعنى هذه النقطة بإدارة الإتصالات وتشغيل تقنية المعلومات وأن يراعى هنا المحافظة على سرية المعلومات وتوفرها عند الحاجة، والمحافظة على سلامة محتواها من التغيير غير المصرح به. بحيث يتم تطوير إجراءات تشغيلية للتعامل مع تقنية المعلومات وخصوصا ما يتعلق بنطاق العمل الذي تم تحديده.

7.5– التحكم بالوصول الى المعلومات: يتم هنا تعريف المستخدمين والموارد (من معلومات وأنظمة وتطبيقات وموارد شبكية ونحوها) وطريقة الوصول إليها، والصلاحيات المخولة لكل مستخدم بناء على مبدأ المعرفة قدر الحاجة وتوزيع وفصل المهام. كما يجب العناية بالمراجعة الدورية للصلاحيات ومدى الحاجة لها.

8.5– التطوير والصيانة لأنظمة المعلومات: يعنى المعيار بأهمية توضيح متطلبات الأنظمة من النواحي الأمنية، والتأكد من معالجة المعلومات بطريقة تتناسب وأهميتها وسريتها وتحافظ على ملفات النظام.

9.5 – إدارة الأحداث الأمنية: يتم هنا تعريف السياسات والإجراءات الخاصة بالتعامل مع الأحداث الأمنية وطريقة احتوائها ومنع أو التقليل من تأثيرها على المعلومات وسير العمل ودراسة مسبباتها لتجنبها في المستقبل.

10.5 – استمرارية الأعمال: يتم هنا تطوير الخطط الكفيلة بضمان استمرارية العمل حتى في حال حصول بعض المشاكل التقنية (مثل عطل في أحد الخوادم، انطفاء الكهرباء،تعطل أحد الموجهات أو حتى تغيب أحد الموظفين) واختبارها دوريا وتحسينها بما يتلائم ومتطلبات المؤسسة.

11.5– التطبيق والتوافق مع المتطلبات القانونية والتشريعية: يعنى المعيار هنا بالتأكد من أن المؤسسة مطبقة لجميع المتطلبات والتشريعات القانونية والتشريعية والمتعلقة بأمن المعلومات ومثال ذلك نظام مكافحة الجرائم الإلكترونية.

ثالثا/ أمن المعلومات و ضرورة الاتجاه إلى المواصفة القياسية ISO 27001 :2005 في المؤسسات الجزائرية:

1- أمن المعلومات والتشريعات بالجزائر:

تدرك الجزائر وعلى غرار ما يحدث في العالم ضرورة توفير الحماية القانونية للحريات والملكيات وحرية الإبداع الفكري والفني الذي يشكل حافزا رئيسيا للإبتكار والتجديد، وما نص المادة 54 من الدستور إلا تعبير صريح على إهتمام الجزائر بمثل هذا المجال وإدراكها العميق لما له من آثار إيجابية على الأفراد والمؤسسات "حرية الإبداع الفكري والفني والعلمي للمواطن مضمونة في إطار القانون، وحقوق التأليف محمية قانونا". ولقد مر التشريع الجزائري في إطار حماية الملكية الفكرية(الأدبية منها والفنية) بمرحلتين حيث يرى الأساتذة الباحثين على أنه يمكن إعتبار أن التشريع الجزائري يأخذ منعرجين هامين اليوم بعد إصدار الأمر رقم 03/05 و هو بداية نحو محاولة التشريع للبيئة الإلكترونية والذي يبقى نوعا ما محتشما مقارنة بما هو حاصل اليوم من تطورات في البيئة الإلكترونية من جهة وبالنظر إلى مختلف القوانين والنصوص التشريعية التي تسن في البيئة الرقمية. (17)

نظرا للتطور العلمي الهائل الذي مسّ جميع المجالات وبظهور الحاسب و اعتماد أغلبية دول العالم نصوص وقوانين تشريعية مست برامج الحاسب (**Logiciel**) ونظرا للعمل الذهني الذي يتطلب تكوينه.لكن الجزائر انتظرت إلى غاية سنة 2003 لإصدار الأمر رقم 05/03 الذي يتعلق بحق المؤلف والحقوق المجاورة والذي يساير في مجمله التطورات الحديثة الحاصلة في ميدان التشريع أو التقنيات الحديثة (التكنولوجيات الجديدة) على حد سواء، وبذلك توضع الجزائر ضمن قائمة الدول المسايرة لمتطلبات العصر وهذا من خلال المادتين:03 و41 على التوالي من هذا الأمر.حيث سمحت الأولى منه بإدخال برامج الحاسب في إطار المصنفات المحمية بموجب حق المؤلف، ونصت المادة 41 على "عدم الاستنساخ الخطي لكتاب كامل أو مصنف موسيقي في شكل خطي وعدم استنساخ قواعد البيانات في شكل رقمي وعدم استنساخ برامج الحاسب إلا في الحالات المنصوص عليها في المادة 52 من هذا الأمر".

2- ضرورة الاتجاه إلى المواصفة القياسية ISO 27001 :2005 في المؤسسات الجزائرية:

تعد المعايير الدولية سواء في التسيير أو مسار الإنتاج، ضرورة تفرضها المعطيات الدولية، إلى جانب أن المعايير تعتبر وسيلة للتنمية والابتكار داخل المؤسسة، وتعطي الثقة للمستهلك لبناء علاقات دائمة مع المؤسسة . و في الجزائر لا يزال هناك تغييب لهذا العنصر الهام في تطوير المؤسسات الوطنية، حيث لا تتجاوز عدد المؤسسات المؤهلة وفق معيار نظام إدارة الجودة في الجزائر (إيزو 9001) حوالي 1000 مؤسسة من أصل 300 ألف مؤسسة ناشطة في الاقتصاد الوطني. (18)

كما نشير أنه من خلال بحثنا في المواقع المتخصصة و المواقع الرسمية لم نجد مؤسسات جزائرية حاصلة على شهادة الإيزو 27001 : 2005 في حين أن أهم الشهادات التي توجهت إليها بعض المؤسسات الجزائرية الذي يعد قليلا جدا كانت تتمحور حول شهادة الإيزو 9001 لتطبيق أنظمة الجودة، الإيزو 14001 المتعلقة بأنظمة البيئة،الإيزو 22000 المتعلق بالسلامة الغذائية ، الإيزو 18001 المتعلق بالصحة و السلامة المهنية.

نشير إلى الدور المنوط بالمعهد الوطني للتقييس حيث تعتبر الجزائر عضوا في منظمة الإيزو منذ سنة 1976،حيث يعمل المعهد على إعداد المواصفات الوطنية بالتنسيق مع مختلف القطاعات، وينجز الدراسات والبحوث و التحقيقات العمومية مع تحديد الاحتياجات الوطنية في مجال التقييس، و السهر على تنفيذ البرنامج الوطني للتقييس، ضمان توزيع المعلومات المتعلقة بالتقييس ، وتمثيل الجزائر في الهيئات الدولية للتقييس و التي تكون الجزائر طرفا فيها. كما نثمن إعلان وزارة الصناعة و المؤسسات الصغيرة والمتوسطة وترقية

الاستثمار عن المسابقة الوطنية لمنح الجائزة الجزائرية للجودة قصد مكافأة مجهودات المؤسسات و الهيئات على النتائج المتحصل عليها في مجال تحسين و تطوير الجودة .

نشير إلى ضرورة استفادة المؤسسات الجزائرية من الخبرات و الاستشارات الخارجية، خاصة بالنسبة للمؤسسات الأجنبية التي لها فروع في الجزائر كالبنك العربي الذي يطبق نظاما لأمن و حماية المعلومات يتوافق مع الإيزو 27001: 2005 و هو من الحالات القليلة جدا التي وجدناها من خلال بحثنا في المواقع المتخصصة ذات الصلة بالموضوع.

3- نقطة البداية لأي منظمة أعمال ترغب في البدء بتطبيق المواصفة القياسية الإيزو 27001:2005:

يمكن الاستعانة بجهة استشارية متخصصة، حيث تتوافر لديها الخبرة العملية المتراكمة وفريق عمل من الخبراء المؤهلين والحاصلين على شهادات متخصصة ككبير مدققين للمواصفة القياسية 27001:2005 بشأن أمن وسرية المعلومات، تتيح لها تأهيل منظمات الأعمال المختلفة للاعتماد وفقا لهذه المواصفة. تقوم الجهات الخارجية المتخصصة في هذا المجال بمراحل العمل التالية: [19]

- المرحلة الأولى: تحليل الفجوة ما بين الوضع الحالي و متطلبات المواصفة القياسية إيزو 27001:2005 بشأن أمن و سرية المعلومات.
- المرحلة الثانية: توثيق النظام طبقا لمتطلبات المواصفة القياسية 27001:2005.
- المرحلة الثالثة: الإشراف على التنفيذ.
- المرحلة الرابعة: التدقيق الداخلي ومراجعة الإدارة.
- المرحلة الخامسة: التدريب على مبادئ المواصفة القياسية 27001:2005.
- المرحلة السادسة: المتابعة مع الجهة المانحة.
- المرحلة السابعة: صيانة النظام خلال فترة صلاحية الشهادة.

خلاصة و استنتاجات:

- يعتبر المعيار العالمي الايزو 27001 من المعايير العالمية المتميزة إن لم يكن الوحيد المعتمد والذي يتميز بمرونته بحيث يتوافق مع جميع المنظمات حكومية كانت أو خاصة، بحيث تقوم المؤسسة بدراسة المخاطر المتعلقة بمعلوماتها وفهمها ومن ثم بناء نظام أمن معلومات متكامل يقلل المخاطر وقابل للتطوير بناء على منهجية واضحة وموثقة.

- نستطيع القول أن المشرع الجزائري اليوم بدأ في مرحلة التركيز في مجال حقوق المؤلف في انتظار التركيز أكثر للتماشي مع متطلبات العصر الرقمي، و الجزائر تمتلك المقومات التقنية والتشريعية للدخول في عالم الرقمنة إذا ما تم إستغلال ذلك على أكمل وجه.
- إن جميع المنظمات والشركات الحكومية والخاصة لها معلومات مهمة تحاول الحفاظ عليها، لذلك فإن تطبيق المعيار العالمي لأمن المعلومات يعتبر أمرا ضروريا لمساعدة المنظمة على تحقيق أمن المعلومات، و ذلك أيضا لتسهيل العملية الإدارية داخل المنظمة.

- نقترح على المؤسسات في الجزائر ضرورة التركيز على المفاهيم الحديثة التي تسلط الضوء على كل ما له علاقة بدورة حياة المعلومات، والمواصفة (ISO 27001) إذ أن المنظمات اليوم أصبحت تتسم بتزايد هائل في المعلومات، الأمر الذي يتوجب معه توجيه الأنظار نحو المفاهيم و الأنظمة التي من شأنها أن تسهل وتنظم التعامل مع هذه الزيادات في المعلومات.
- يجب على المؤسسات الجزائرية ضرورة الربط الواقعي بين إدارة دورة حياة المعلومات ، والمواصفة (ISO 27001) ، إذ أن هذا الربط سيوفر وسائل فاعلة وناجحة للتعامل مع المعلومات ، فضلا عن أن حصول المنظمات على شهادة ISO في هذا المجال سوف يمكنها من الحصول على ميزة تنافسية، وإكسابها الطابع العالمي من خلال حصولها على شهادة دولية.
- لا يمكن الاستفادة من معايير أمن المعلومات العالمية المتاحة إلا إذا تم تنفيذها بشكل صحيح بمشاركة جميع الأطراف بالتعاون الكامل على جميع مستويات المؤسسة.
- يجب بذل جهود اكبر من المعهد الوطني للتقييس فيما يخص تحديد الاحتياجات الوطنية في مجال التقييس، و من ابرزها اليوم المواصفة القياسية العالمية لأمن و حماية المعلومات، و السهر على تنفيذ البرنامج الوطني للتقييس،و ضمان توزيع المعلومات المتعلقة بالتقييس.

الهوامش و المراجع:

1. "**أمن المعلومات**"، موقع الموسوعة الحرة، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://ar.wikipedia.org/wiki
2. أيمن عبد السلام: "**أمن المعلومات**"، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://coeia.ksu.edu.sa
3. عايض المري: "**أمن المعلومات: ماهيتها و عناصرها و استراتيجياتها**"، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://www.dralmarri.com
4. نفس المرجع، ص 02.
5. "**مقدمة عن سياسات و معايير أمن المعلومات** "،وزارة رئاسة مجلس الوزراء السوداني، المركز القومي للمعلومات – الإدارة الفنية، قسم الجودة و التطوير – وحدة المعايير،فيفري 2010، ص 08.
6. نفس المرجع، ص 09.
7. عايض المري، مرجع سابق، ص 16.
8. نفس المرجع، ص 23.
9. نفس المرجع، ص 24.
10. أيمن عبد السلام، مرجع سابق، ص 25.
11. نظام إدارة أمن و سرية المعلومات ISO 27001:2005، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://www.alhartany.com
12. علي عبد الستار عبد الجبار الحافظ، أحمد هاني محمد النعيمي: " دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (نموذج مقترح)"،
13. منصور عوض الحربي: " معيار الإيزو 27001" ، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://coeia.ksu.edu.sa
14. " المواصفة القياسية ايزو 27001 نظام إدارة أمن المعلومات" ، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://www.gckw.com/ISO-27001-AR.
15. نفس المرجع، ص 14.
16. فهد فايز المدرع: " **المعايير العالمية لأمن المعلومات**"، [على الخط] ، مقال متاح على الموقع الإلكتروني:
http://iehad.com/index.php

17.بن ضيف الله فؤاد: " **أمن المعلومات أحد السبل لحماية الملكية الفكرية**"،[على الخط] ، مقال متاح على الموقع الإلكتروني:

http://www.journal.cybrarians.org

18.محمد سيدمو: " توقيع **منتدى رؤساء المؤسسات بروتوكول اتفاق مع المعهد الجزائري للتقييس "إيانور**" ""،[على الخط] ، مقال متاح على الموقع الإلكتروني :

économie.http://www.elkhabar.com./ar/

19." **المواصفة القياسية الإيزو 27001 نظام إدارة أمن المعلومات**" ،[على الخط] ، مقال متاح على الموقع الإلكتروني :

http://www.gckw.com/ISO-27001-AR.