المعايير الدولية لإدارة أمن المعلومات

International Information Security Management Standards

هدى بن محمد*
كلية العلوم الاقتصادية، جامعة البليدة 2، الجزائر
haouchineyoucef1@gmail.com

ابتسام طوبال
كلية العلوم الاقتصادية، جامعة البليدة 2، الجزائر
haouchineyoucef1@gmail.com

نجاة كورتل
كلية العلوم الاقتصادية، جامعة البليدة 2، الجزائر
haouchineyoucef1@gmail.com

تاريخ الاستلام: 2020/12/27 **تاريخ القبول للنشر**: 2023/06/23 **تاريخ النشر**: 2023/07/01

ملخص

يهدف هذا البحث إلى التعرف على أمن المعلومات، وتسليط الضوء على مختلف المعايير الدولية المقبولة من أغلب الدول والمنظمات لإدارة أمن المعلومات، ونخص بالذكر معيار ISO / IEC 27001، ذلك لأن المنظمات الحائزة على هذه المعايير ستعزز من مكانتها على المستوى المحلي والإقليمي، وسيشكل حصولها على هذه المعايير دافعا قويا للاستمرار في تطوير خدماتها ومنتجاتها وفق أعلى وأفضل المعايير والأنظمة الدولية للرفع من ثقة المواطنين والعملاء والمستثمرين في كافة الأنشطة والعمليات التي تقوم بها.

* المؤلف المراسل.

ISSN: 1112-4938, EISSN: 2600-6456

– **الكلمات المفتاحية**: أمن المعلومات – عائلة معايير ISO / IEC 27000– معيار ISO / IEC 27001.

Abstract:

This research aims to identify information security and highlight several international standards accepted by most countries and organizations for information security management, particularly the ISO / IEC 27001 standard, because organizations that have these standards will improve their position at the local and regional levels. Obtaining these standards will be a significant motivator for continuing to enhance its services and products in accordance with the highest and best international standards and processes in order to increase citizens', customers', and investors' confidence in all of its activities and operations.

***Key words**:* information security - ISO / IEC 27000 family of standards - ISO / IEC 27001 standard.

مقدمة

عرفت تكنولوجيا المعلومات والاتصالات تطورات متسارعة في الآونة الأخيرة، وقد أحدثت معها تغيرات كبيرة في مختلف المجالات التي استغلتها أحسن استغلال، وعليه أصبحت أداة رئيسية لا غنى عنها لتحقيق نهضة الأمم وتطورها، وهذا نظرا للمزايا الكبيرة التي توفرها كالسرعة والدقة في أداء العمل، وتقليص المسافات، وتخفيض التكاليف وغيرها.

إلا أن استخدام تكنولوجيا المعلومات والاتصالات تجوبه العديد من المخاطر والتهديدات التي تمس أمن معلومات المنظمات كالقرصنة والتجسس وتخريب المعلومات

وغيرها، مما قد يؤثر على بقائها واستمراريتها خاصة بعدما أصبحت المعلومة تلعب دورا جوهريا في نشاط هذه المنظمات، مما استوجب عليها الاهتمام أكثر بإدارة أمن معلوماتها.

وبما أن المنظمات لا يمكن أن تضمن الحماية الكلية لمعلوماتها، فهي بحاجة إلى الاستعانة بمجموعة من المقاييس أو المعايير الدولية التي توفر أعلى مستويات الجودة وبأفضل الطرق والممارسات المتخصصة في إدارة أمن المعلومات المتعارف عليها دوليا، والتي يمكن من خلالها تحقيق مستوى ملائم من الأمن.

تعد عائلة المعايير ISO / IEC 27000 من الأساليب والتدابير وأفضل الممارسات المعترف بها دوليًا في مجال أمن المعلومات، وهي مخصصة لأي نوع من الشركات مهما كان حجمها أو قطاع نشاطها أو بلدها المنشأ. تهدف هذه المعايير إلى وصف الأهداف التي يجب تحقيقها من حيث الأمن المعلوماتي، ويعتبر معيار ISO / IEC 27001 من أهم هذه المعايير حيث يختص بأنظمة إدارة أمن المعلومات المصممة لحماية سرية ونزاهة البيانات وتوافرها.

ومما سبق نطرح الإشكالية التالية:

ما هي المعايير الدولية المعتمدة في إدارة أمن المعلومات؟

وعليه فإننا نهدف من خلال هذه الورقة البحثية إلى ما يلي:

- التعرف على ماهية أمن المعلومات.
- التعرف على عائلة المعايير ISO/IEC 27000.
- تسليط الضوء على ماهية معيار ISO / IEC 27001.

تكمن أهمية هذا البحث في تمكين المنظمات من التعرف على أفضل الممارسات الدولية المتعلقة بأمن المعلومات، خاصة بعد تزايد الأخطار والتهديدات التي تمس أمن معلوماتها،

والعمل على تطبيق المعايير الدولية في هذا المجال نظرا للفوائد الكبيرة التي يمكن أن تجنيها من وراء ذلك.

ومن أجل معالجة إشكالية البحث سوف نستخدم المنهج الوصفي للتعرف على أمن المعلومات، والمعايير الدولية المعتمدة في هذا المجال.

وقد تناولت العديد من الدراسات إدارة أمن المعلومات والمعايير الدولية الخاصة بها، ومن بين هذه الدراسات نذكر ما يلي:

- دراسية Joffre Velasco وآخرون حول فوائد تطبيق نظام إدارة أمن المعلومات في الصناعة التحويلية في الإكوادور وفقا لمعيار ISO 27001، حيث هدفت هذه الدراسة إلى اقتراح مبادئ توجيهية تسهل تنفيذ نظام إدارة أمن المعلومات وفقًا لمعيار ISO 27001، مع الأخذ في الاعتبار أن الإدارة السليمة للمعلومات تمثل في الوقت الحاضر رصيدًا لا يقدر بثمن لأي منظمة[1].
- دراسة Candiwan حول تحليل تطبيق معيار ISO 27001 في الشركات والمؤسسات الصغيرة والمتوسطة في إندونيسيا، حيث هدفت هذه الدراسة إلى التعرف إلى أي مدى يتم تنفيذ معيار ISO27001 في الشركات والمؤسسات الصغيرة والمتوسطة في إندونيسيا. وتوصلت الدراسة أن تنفيذ متطلبات معيار ISO 27001 في الشركات هو أكثر من المؤسسات الصغيرة والمتوسطة[2].
- دراسة Vladislav V. Fomin وآخرون حول أسباب قلة تبني معيار ISO 27001، حيث هدفت هذه الدراسة إلى استكشاف أسباب تدني تبني هذا المعيار بالمقارنة مع اثنين من معايير نظام الإدارة الأخرى المطبقة على نطاق واسع وهي معيار ISO 9001 لإدارة الجودة ومعيار ISO 14001 للإدارة البيئية، وخلصت

الدراسة إلى أن معيار ISO 27001 تلقى اهتماما ISO / IEC أقل بكثير من الأوساط الأكاديمية ، كما تم قياسه من خلال الرقم من المنشورات العلمية حول هذا الموضوع. واختتمت الدراسة بجملة من الدوافع والعوائق المحتملة لتبني هذا المعيار[3].

وعليه سوف نقسم بحثنا إلى ثلاثة محاور أساسية تتمثل فيما يلي:

المحور الأول: ماهية أمن المعلومات

المحور الثاني: عائلة المعايير ISO/IEC 27000

المحور الثالث: ماهية معيار ISO / IEC 27001

المحور الأول: ماهية أمن المعلومات

تواجه المنظمات في خضم التطورات الكبيرة في تكنولوجيا المعلومات والاتصالات مخاطر وتهديدات عديدة، مما ألزم عليها الاهتمام أكثر بأمن معلوماتها، الذي أصبح يلعب دورا مهما في حماية أصول هذه المنظمات.

1- تعريف أمن المعلومات: يقصد بأمن المعلومات حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة. ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات وهي الكنز الثمين الذي يجب على المنشأة الحفاظ عليه[4].

يعرف أمن المعلومات من زوايا عديدة أهمها[5]:

- من منظور أكاديمي: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.
- من منظور تقني: هو الوسائل والأدوات والإجراءات اللازم توفرها الضمان حماية المعلومات من الأخطار الداخلية والخارجية.
- من منظور قانوني: هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء 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 والانترنت).

وعليه يمكن تعريف أمن المعلومات بأنه العمل على توفير مختلف المتطلبات اللازمة من وسائل وأدوات وإجراءات لضمان حماية المعلومات من الأخطار التي تواجهها.

2- أهمية أمن المعلومات: تنبع أهمية المعلومات من أنها تستخدم من قبل الجميع بلا استثناء، كما أنها هدف للاختراق من جانب الجميع كذلك وأيضا بلا استثناء، وفي بعض الأحيان تكون المعلومات هي الفيصل بين النصر والهزيمة في الحروب، وأحيانا تكون هي الفيصل بين المكسب والخسارة للشركات وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان.

في هذا العصر بالذات انقلبت الآية ولم تعد مشكلة الناس الحصول على المعلومات، وإنما أصبحت مشكلتهم هي هذا الفيض الهائل من المعلومات كيف نفرق بين الغث منها والثمين. ومن ثم كيف نحمي هذه المعلومات من الأخطار التي تهددها[6].

3- عناصر أمن المعلومات: لا بد من ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها[7]:

- **السرية والموثوقية Confidentiality:** وتعني التأكد من أن المعلومات لا تكشف ولا تطلع عليها من قبل أشخاص غير مخولين بذلك.
- **التكاملية وسلامة المحتوى Integrity:** 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 Availability:** التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات، وتقديم الخدمة لمواقع معلوماتية، وإن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** ويقصد به 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.

وقد تم وضع ثلاثة عناصر بنفس الكيفية مع تغيير المسميات وهي[8]:

- **الخصوصية Privacy:** كي تتم المحافظة على خصوصية الرسالة الإلكترونية، يجب ألا يتمكن من الاطلاع عليها إلا الأطراف المعنية المسموح لها بذلك. وللحفاظ على الخصوصية، لا بد من التحكم بعملية الدخول، وأكثر طرق التحكم

انتشارا هي: استخدام كلمات المرور، الجدران النارية، إضافة إلى شهادات الترخيص مثل BBB الأمريكية.

- **سلامة المحتوى Integrety:** لا بد من حماية عمليتي نقل المعلومات وتخزينها، وذلك لمنع أي تغيير للمحتوى بشكل متعمد أو غير متعمد. وتكمن أهمية ذلك في الحفاظ على محتوى مفيد وموثوق به. وفي الغالب، تكون الأخطاء البشرية وعمليات العبث المقصود هي السبب في تلف أو تشويه البيانات. وينتج عن ذلك أن تصبح البيانات عديمة الجدوى، وغير آمنة للاستخدام. ولتلافي تشويه أو تلف البيانات، يمكن استخدام تقنيات مثل: البصمة الإلكترونية للرسالة، والتشفير.
- **التحقق من هوية الأطراف الأخرى Peer Authentication:** يجب التأكد من هوية الأطراف المعنية بعملية تبادل البيانات، إذ يجب على كلا الطرفين معرفة هوية الآخر لتجنب أي شكل من أشكال الخداع (مثل عمليات التزوير وانتحال الشخصيات). وهناك بعض الحلول والإجراءات للتحقق من هوية الأطراف المتصلة مثل: كلمات المرور، التوقيعات الرقمية، والشهادات الرقمية.

4- متطلبات أمن المعلومات: يتطلب الأمر لحماية أمن المعلومات الإشارة إلى أهمية نشر الوعي بين العاملين في المنشأة بالأخطار التي تهدد أمن المعلومات، ومن متطلبات أمن المعلومات[9]:

- وضع سياسة محددة لأمن المعلومات.
- دعم الإدارة العليا لسياسات وخطط وبرامج أمن المعلومات.
- تحديد أشخاص محددين كمسؤولين عن أمن المعلومات.
- تحديد طرق الحماية اللازم توافرها في أنظمة تشغيل المعلومات.

- تحديد آليات المراقبة والتفتيش على نظم المعلومات.
- حفظ وسائط التخزين.
- تحديد وسائل وطرق لتشفير المعلومات.
- تأمين استمرارية عمل نظم المعلومات وإتاحتها.

5- عقبات أمن المعلومات: هناك عقبات تقف في طريق توفير المستوى المناسب لتدابير الحماية الأمنية للمعلومات منها[10]:

- نقص الأفراد المدربين والذين يبدون اهتماما بمشكلة أمن وسلامة البيانات.
- نقص التمويل والوقت والأهم من ذلك الوعي والمساندة من جانب الإدارة والجهات المستفيدة من المعلومات.
- سوء التقدير لمدى تعقد النظم والتطبيقات والاستعجال لبلوا حالة التشغيل الأمر الذي يؤدي إلى قلة الاهتمام أو إغفال تدابير السلامة الضرورية.

المحور الثاني: عائلة المعايير ISO/IEC 27000

هناك العديد من المعايير الدولية لإدارة أمن المعلومات، من أهمها عائلة المعايير ISO/IEC 27000 التي وضعتها المنظمة الدولية للمعايير.

1- تعريف عائلة المعايير ISO / IEC 27000 : هي مجموعة من الأساليب والتدابير وأفضل الممارسات المعترف بها دوليًا في مجال أمن المعلومات. وهي مخصصة لأي نوع من الشركات مهما كان حجمها أو قطاع نشاطها أو بلد منشئها. تهدف هذه المعايير إلى وصف الأهداف التي يجب تحقيقها من حيث الأمن المعلوماتي، وليس بالطريقة الملموسة لتحقيقها؛ لأن هذا يعتمد عادة على السياق المحدد لأي منظمة.

على المستوى الدولي تعتبر اللجنة الفرعية 27 للجنة المشتركة بين منظمة الإيزو ISO واللجنة الدولية الإلكتروتقنية IEC رقم 1 ، اختصار ISO / IEC JTC 1 / SC 27 اللجنة التي تتعامل مع إدارة ونشر معاييرها الرائدة في مجال أمن المعلومات وذلك من قبل خبراء المتطوعين.

تتكون عائلة المعايير ISO/IEC 27000 من مجموعة من المعايير، حيث يتم حجز المعايير من 27000 إلى 27010 للتوثيق العام لنظام إدارة أمن المعلومات ISMS، في حين تم تخصيص المعايير من 27011 إلى 27019 لمواصفات نظام إدارة أمن المعلومات لقطاعات اقتصادية محددة (مثل ISO / IEC 27015 للقطاع المالي، ISO / IEC 27011 لقطاع الاتصالات)[11].

يعتبر معيار ISO / IEC 27001 الذي يحدد متطلبات أنظمة إدارة أمن المعلومات، المعيار الأكثر شهرة في هذه العائلة[12].

يمكن تصنيف معايير الإيزو إلى معايير للمتطلبات أو معايير الأدوات، إذ تحدد معايير المتطلبات ما يجب فعله، ولكن ليس كيفية القيام به بينما تصف معايير الأداة كيفية القيام بذلك. وفي عائلة المعايير ISO/IEC 27000، تعتبر المعايير ISO/IEC 27001 و ISO/IEC 27006 فقط هي معايير المتطلبات[13].

2- نبذة تاريخية عن ظهور عائلة المعايير ISO/IEC 27000: بدأت بوادر ظهور عائلة المعايير ISO/IEC 27000 في ثمانينات القرن العشرين وهي ماضية في التطور والنمو تبعا للتطورات الحاصلة في المجال، حيث نشرت شركة Shell في 1980 وثيقة داخلية تبرز سياسة أمن معلوماتها[14]، ويمكن إبراز أهم مراحل ظهور عائلة المعايير ISO/IEC 27000 فيما يلي:

- في عام 1995، نشر المعهد البريطاني للمعايير BS 7799 الذي يضفي الطابع الرسمي لسوق المملكة المتحدة مجموعة من أفضل الممارسات في مجال أمن المعلومات.
- في عام 1998، نشر المعهد البريطاني للمعايير الجزء الثاني من BS 7799-2 لتنفيذ شهادة تطبيق أحكام BS 7799 التي تم ترقيمها BS 7799-1 في هذه المناسبة.
- في عام 1999، نشر المعهد البريطاني للمعايير طبعة ثانية من BS 7799-1 من أجل تقديمها إلى منظمة الإيزو.
- في عام 2000، أصبح المعيار البريطاني BS 7799-1 المعيار ISO 17799، الذي يدل على الممارسات لإدارة أمن المعلومات.
- في عام 2002، نشر المعهد البريطاني للمعايير نسخة محسنة من BS 7799-2 لتنسيقها مع أنظمة إدارة الجودة والبيئة (ISO 9001 و ISO 14001).
- في أكتوبر 2005، تم تحديث المعيار ISO 17799 وفقا لسياسة مراجعة لمدة خمس سنوات من منظمة الإيزو.
- في عام 2005، أصبح معيار BS 7799-2 المعيار ISO 27001.
- في فبراير 2007، يقوم معيار ISO 27006 ، استناداً إلى معيار ISO 17021 ، بإكمال النظام من خلال توفير متطلبات هيئات التدقيق وإصدار الشهادات الخاصة بـISMS ؛
- في الأول من يوليو 2007، أصبح المعيار ISO 17799 المعيار ISO 27002 دون تغيير المحتوى.

- في يونيو 2008، حل المعيار ISO 27005 محل المعيار BS 7799-2 لوصف إدارة المخاطر لأمن المعلومات.

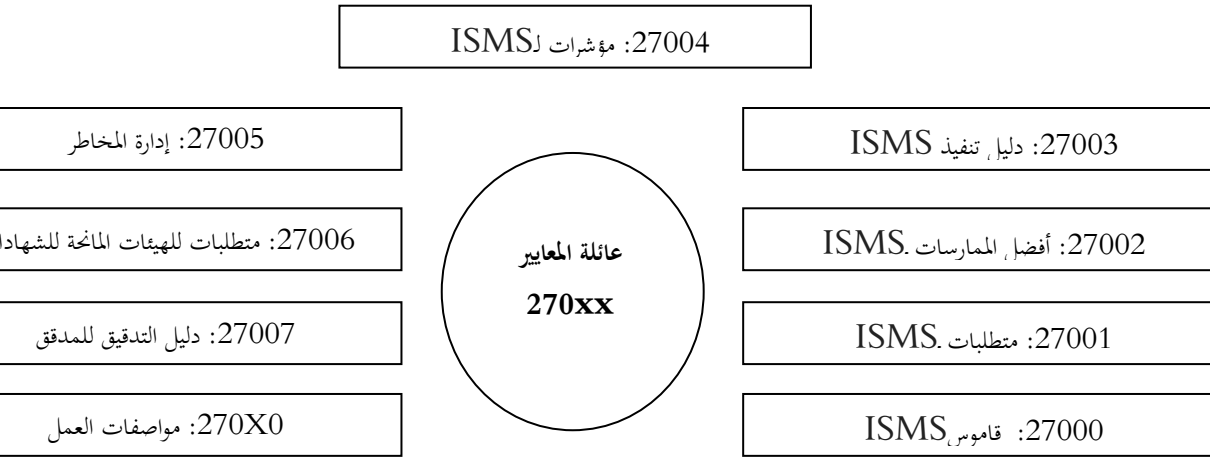
إضافة إلى ذلك[15]:

- في 2008 تم نشر المعيار ISO/IEC 27799.
- في 2009 تم نشر المعايير ISO/IEC 27000 ، ISO/IEC 27003، ISO/IEC 27004 و ISO/IEC 27033-1.
- في 2010 تم نشر المعيارين ISO/IEC 27003 و ISO/IEC 27033-3.
- في 2011 تم نشر المعايير ISO/IEC 27007 ، ISO/IEC 27008، ISO/IEC 27031، ISO/IEC 27034-1، ISO/IEC 27035، كما تم مراجعة ISO/IEC 27006
- في 2012 تم نشر المعايير ISO/IEC 27010 ، ISO/IEC 27032 و ISO/IEC 27033-2.
- في 2013 تم مراجعة المعيار ISO/IEC 27001 والمعيار ISO/IEC 27002.

3- مكونات عائلة المعايير ISO/IEC 27000: تتكون هذه المجموعة من معايير متطلبات ومعايير أدوات للحصول على مجموعة من المتطلبات والمعلومات وأفضل الممارسات لتحسين تأمين نظام معلومات لجميع أنواع المنظمات المتعلقة بأمن المعلومات، مثل البيانات المالية، ومعلومات الموظفين، وبيانات الطرف الثالث أو الملكية الفكرية.

ويمكن توضيح مكونات عائلة المعايير ISO/IEC 27000 من خلال الشكل التالي:

شكل رقم 01: عائلة المعايير ISO/IEC 27000



Source :

http://www.utc.fr/~mastermq/public/publications/qualite_et_management/MQ_M2/2017-2018/MIM_projets/qpo12_2018_gr08_secu_info/mim.pdf Vu le 12-08-2020.

من خلال الشكل السابق يمكن إدراج مكونات عائلة معايير 270X0 التالية، علما أن هذه المعايير هي في تجدد مستمر.

أ- **معيار ISO / IEC 27000**: تقدم ISO / IEC 27000: 2016 نظرة عامة على أنظمة إدارة أمن المعلومات. تحدد الوثيقة المصطلحات المتعلقة بها.

ISSN: 1112-4938, EISSN: 2600-6456

ب- معيار ISO / IEC 27001: تحدد المواصفة القياسية :ISO / IEC 27001 2013 متطلبات إنشاء نظام ISMS وتطبيقه وصيانته والتحسين المستمر له. كما يحدد إطارًا شاملاً للإدارة والرقابة لمعالجة مخاطر أمن المعلومات.

تغطي متطلبات ISO / IEC 27001: 2013 جميع أنواع المنظمات، بغض النظر عن نوعها وحجمها وطبيعتها.

ج- معيار ISO / IEC 27002: توفر ISO / IEC 27002: 2013 إرشادات حول المعايير التنظيمية لأمن المعلومات والممارسات الجيدة لإدارة أمن المعلومات.

تسمح هذه الوثيقة للمؤسسات باختيار الإجراءات الضرورية كجزء من عملية تنفيذ ISMS وفقًا لـ ISO / IEC 27001.

د- معيار ISO / IEC 27003: تدعم الوثيقة المفاهيم العامة لـ ISO / IEC 27001 ؛ يشجع على تنفيذ نهج العملية.

و- معيار ISO / IEC 27004: ISO / IEC 27004: 2016 عبارة عن مجموعة من الإرشادات التي تقدم إرشادات حول وضع برنامج للتدابير والضوابط وإضفاء الطابع الرسمي على المؤشرات لقياس كفاءة نظام إدارة أمن المعلومات (ISMS).

ه- معيار ISO / IEC 27005: تدعم هذه الوثيقة المفاهيم العامة في ISO / IEC 27001 ؛ وهي مصممة للمساعدة في تنفيذ أمن المعلومات على أساس نهج إدارة المخاطر.

المحور الثالث: ماهية معيار ISO / IEC 27001

يعتبر معيار ISO / IEC 27001 من أهم معايير عائلة المعايير ISO/IEC 27000، وهو يهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المنظمة. وعادة ما ينطبق على جميع أنواع المنظمات، بما في ذلك المؤسسات التجارية والوكالات الحكومية، وغيرها.

1- مفهوم معيار ISO / IEC 27001:

1-1- تعريف معيار ISO / IEC 27001 (تكنولوجيا المعلومات- تقنيات الأمن- نظم إدارة أمن المعلومات- المتطلبات):

معيار ISO 27001 ، أو رسميًا واسمه ISO / IEC 27001: 2005، هو معيار دولي نشرته منظمة الإيزو في أكتوبر 2005. ثم تم تعديله في 2013 ليصبح ISO / IEC 27001: 2013.

تم إعداد هذا المعيار الدولي لتوفير نموذج لإنشاء نظام إدارة أمن المعلومات (ISMS) وتطبيقه وتشغيله ومراقبته ومراجعته وصيانته وتحسينه[16].

ويشير نظام إدارة أمن المعلومات إلى المنهجية النظامية التي بموجبها تضمن المنظمة أمن المعلومات الحساسة. تم تصميم نظام إدارة أمن المعلومات وفقًا لعمليات إدارة المخاطر، ويشمل الأشخاص والعمليات وأنظمة تكنولوجيا المعلومات. يمكن أن يكون هذا الحل مفيدًا للمؤسسات من جميع القطاعات والأحجام الذين يقدرون سرية معلوماتهم[17].

يستند إنشاء سياسات نظام إدارة أمن المعلومات على نهج إدارة المخاطر. يبدأ تعريف السياسات بفهم بيئة العمل وتقييم الموارد والعمليات، من أجل تحديد مخاطر أمن المعلومات التي قد تحدث.

بعد تحديد المخاطر، تقوم الشركة بتقييم كل من المخاطر، وتقييم التأثير المحتمل، ووضع استراتيجيات في إدارة المخاطر بمشاركة مكثفة من الإدارة بالإضافة إلى الموظفين. وبما أن البيئة وعمليات الأعمال تختلف من منظمة إلى أخرى، فإن المخاطر المحددة والإستراتيجية التي تم تطويرها ستختلف أيضًا.

بمعنى أن معيار ISO / IEC 27001 يوفر المتطلبات والمواصفات لتطبيق نظام إدارة أمن المعلومات، ولكن نظام إدارة أمن المعلومات مصمم خصيصًا لكل مطوري ISO / IEC 27001.[18]

يمكن لأي منظمة تنفيذ ISO / IEC 27001، سواء كانت ربحية أو غير ربحية، خاصة أو عمومية، صغيرة أو كبيرة.

وقد كتبه أفضل الخبراء في العالم في مجال أمن المعلومات، ويوفر منهجية لتنفيذ إدارة أمن المعلومات في المنظمة. كما أنه يمكن الشركات من أن تصبح معتمدة، مما يعني أن هيئة مستقلة لإصدار الشهادات قد أكدت أن إحدى المنظمات قامت بتنفيذ أمن المعلومات المتوافق مع ISO / IEC 27001.[19]

1-2- مميزات تطبيق معيار ISO / IEC 27001: يمكن أن نشير إلى بعض مميزات تطبيق المعيار كما يلي[20]:

- 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 لمعاجلة المخاطر المتوقعة.
- تخفيف تكاليف إعادة إنشاء قواعد بيانات والأنظمة الآلية فيما إذا تعرضت للفقدان أو الاختراق.
- توحيد السياسات والإجراءات لكافة الوحدات التنظيمية في التعامل بشأن إدارة أمن وسرية المعلومات.
- تبوّء 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.

1-3- أسباب تطبيق معيار ISO / IEC 27001: أصبحت انتهاكات البيانات والهجمات السيبرانية -للأسف- من الحوادث العادية، إذ إن ملايين الأمريكيين كانوا ضحايا لهذه الانتهاكات والهجمات، فالولايات المتحدة وحدها تمثل 47 ٪ من انتهاكات البيانات في

العالم في عام 2017. ومع التكلفة العالمية لخروقات البيانات التي تم تحديدها بـ 2.1 تريليون يورو بحلول عام 2019، لم تعد المنظمات قادرة على تجاهل هذا التهديد.

يمكن لإدارة المخاطر أن تساعد في تخفيف الانتهاكات، إذ يحدد المعيار ISO / IEC 27001 منهجًا لأفضل الممارسات لإدارة المخاطر عبر الإنترنت يمكن اعتماده من قِبل جميع الأنشطة التجارية.

ونجد أن أغلى الشركات على المستوى العالمي حاصلة شهادة هذا المعيار كشركة Microsoft, Verizon, Apple, Google, Intel, وشركة Amazon[21].

2- نموذج خطط افعل افحص تصرف PDCA: يعتمد معيار ISO / IEC 27001أو معيار نظام إدارة أمن المعلومات على نموذج خطط افعل افحص تصرف PDCA المعروف كما هو موضح في الشكل رقم 02.

ويسمى هذا النموذج أيضا بنموذج التحسين المستمر؛ نظرا لأن نظام الإدارة يتم مراقبته ومراجعته بانتظام للتحقق مما إذا كانت ضوابط إدارة المخاطر لا تزال فعالة وإذا لم تكن كذلك، فعندئذ يلزم تنفيذ ضوابط محسّنة[22].

وتتمثل خطوات نموذج خطط افعل افحص تصرف PDCA فيما يلي[23]:

2-1- خطط Plan: إنشاء سياسة نظام إدارة أمن المعلومات وأهدافها وعملياتها وإجراءاتها ذات الصلة بإدارة المخاطر وتحسين أمن المعلومات لتحقيق النتائج وفقًا للسياسات والأهداف العامة للمنظمة.

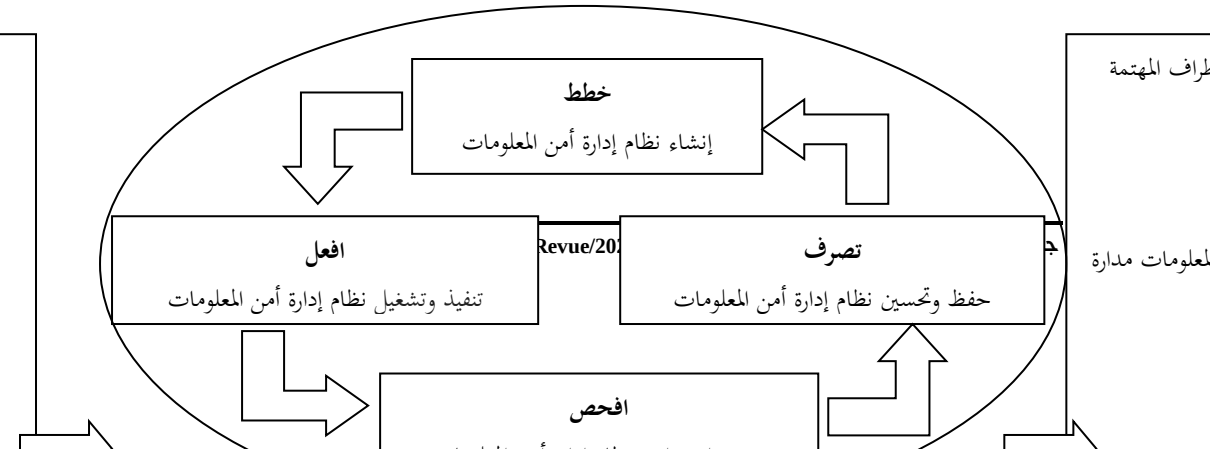
2-2- افعل Do: تنفيذ وتشغيل سياسة نظام إدارة أمن المعلومات وضوابطها وإجراءاتها.

2-3- افحص Check: تقييم، وحيثما ينطبق، قياس أداء العملية اتجاه سياسة نظام إدارة أمن المعلومات، والأهداف والخبرات العملية وتقديم تقرير عن النتائج للإدارة للمراجعة.

2-4- تصرف Act: اتخاذ الإجراءات التصحيحية والوقائية، استنادا إلى نتائج التدقيق الداخلي لنظام إدارة أمن المعلومات ومراجعة الإدارة أو غيرها من المعلومات ذات الصلة، لتحقيق تحسن مستمر في نظام إدارة أمن المعلومات.

والشكل التالي يوضح نموذج خطط افعل افحص تصرف PDCA.

شكل رقم 02: نموذج خطط افعل افحص تصرف PDCA



Source : Razieh Sheikhpour, Nasser Modiri, best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management, Indian Journal of Science and Technology, Vol. 5 No. 2 (Feb 2012), p 2170.

3- متطلبات تطبيق ISO / IEC 27001

إن عملية تبني نظام إدارة أمن المعلومات لمتطلبات معيار ISO / IEC 27001 تعد خطوة مثالية لبناء أمن فاعل لإدارة المعلومات في المنظمة، وهذه العملية قد تتسم بالتعقيد إن لم تكن هناك خطوات محددة من خلالها تتم عملية التبني بسهولة، لذلك جاء الدليل الإرشادي للمعيار ISO / IEC 27001 ليوضح أهم متطلبات تطبيقها، والتي حددها بما يأتي[24]:

- التعريف بحدود ونطاق نظام إدارة أمن المعلومات: يجب أن يحدد في ضوء المواصفات الخاصة بأنظمة معلومات المنظمة من ناحية الحجم والمصادر والأنواع، مع الأخذ بنظر الاعتبار للاحتياجات التنظيمية والتشريعية للمنظمة.

- وضع إستراتيجية لنظام إدارة أمن المعلومات: تتمثل في مجموعة من الإجراءات والخطوات اللازمة لتطبيق نظام إدارة أمن المعلومات، ويعد العامل الرئيس للنجاح في هذه المرحلة هو دعم الإدارة العليا لإستراتيجية نظام إدارة أمن المعلومات.
- تحديد المخاطر واكتشافها: يجب أن تحدد طريقة منهجية ومدخل مناسب لاكتشاف المخاطر.
- التمييز بين المخاطر: العمل على التمييز بين الأنواع المختلفة للمخاطر التي تهدد أمن المعلومات.
- فهم وتقييم المخاطر: تقييم المخاطر الحالية والمحتملة من أجل ضمان الاستخدام الأكثر فعالية للموارد المتاحة.
- تقييم خيارات معالجة المخاطر.
- اختيار أهداف الرقابة المناسبة.
- الحصول على موافقة الإدارة فيما يخص المخاطر المثبتة.
- الحصول على موافقة الإدارة في تنفيذ نظام إدارة أمن المعلومات.

– البدء بالتطبيق: تنطوي هذه المرحلة على إعداد بيان التطبيق. والذي يصف الوثائق المختارة ومراقبة الأهداف وضوابط وأسباب الاختيار أو الاستبعاد.

4- تطور عدد الحاصلين على شهادة معيار ISO / IEC 27001: أصبح معيار ISO / IEC 27001 أكثر معايير أمن المعلومات انتشارًا على مستوى العالم، وقد صدقت عليه العديد من الشركات، ففي عام 2015 تم إصدار ما مجموعه 53627 شهادة في جميع أنحاء العالم، مقارنةً بـ 23005 في عام 2014، أي بزيادة قدرها 20٪[25]. وحسب المسح

الذي قامت به منظمة الإيزو لعام 2017 بلغ عدد الشركات الحاصلة على معيار 39501 شهادة سنة 2017، مقارنةً بـ 33290 في عام 2016 أي بنسبة زيادة قدرها 20٪ سنويا[26].

كما تعتبر شهادة معيار ISO / IEC 27001 من بين أكثر الشهادات منحا سنويا بالمقارنة مع باقي شهادات المعايير الأخرى المعتمدة من منظمة الإيزو.

والشكل التالي يبين تطور عدد الحاصلين على شهادة معيار ISO / IEC 27001 من 2006 إلى 2017.

والجدير بالذكر أن أكثر الحاصلين على شهادة معيار ISO / IEC 27001 من آسيا الشرقية والمحيط الهادي لاسيما اليابان والصين، تليها أوروبا، ثم آسيا الوسطى والجنوبية، ثم أمريكا الشمالية، ثم الشرق الأوسط، ثم أمريكا الوسطى والجنوبية وأخيرا أفريقيا[27].

خاتمة

يعد أمن المعلومات من أولويات أي منظمة مهما كان طبيعة نشاطها أو حجمها أو نوعها، نظرا للأهمية الكبيرة التي تكتسبها المعلومات في هذه المنظمات، فهي تعمل على توفير مختلف المتطلبات اللازمة من وسائل وأدوات وإجراءات لضمان حماية المعلومات من الأخطار التي تواجهها.

من بين المعايير الدولية التي وضعتها منظمة الإيزو بالمشاركة مع اللجنة الدولية الإليكتروتقنية نجد عائلة معايير ISO / IEC 27000 وهي مجموعة من الأساليب والتدابير وأفضل الممارسات المعترف بها دوليًا في مجال أمن المعلومات.

ويعتبر المعيار ISO / IEC 27001 من أهم معايير إدارة أمن المعلومات، وهو جزء من مجموعة معايير ISO 27000 التي تساعد المؤسسات في الحفاظ على أمن

معلوماتها، فهذا المعيار يحدد المتطلبات لتأسيس وتطبيق وتشغيل ومراقبة ومراجعة وصيانة وتحسين المعلومات الموثقة في نظام إدارة المعلومات في سياق المخاطر الكلية التي يتعرض لها النشاط. كما يحدد متطلبات تطبيق ضوابط الأمن والسرية وفقاً لاحتياجات كل كيان أعمال على حدة.

يعتمد هذا المعيار على منهجية منظمة تعرف بنموذج خطط افعل افحص تصرف PDCA لضمان التحسين المستمر لنظام إدارة أمن المعلومات. يتم الحصول على عشرات الآلاف من الشهادات لهذا المعيار سنويا لما له من أهمية بالغة.

وقد تزايد مؤخرا عدد المنظمات عبر مختلف دول العالم الحائزة على شهادة معيار ISO IEC 27001 /، ذلك لأن المنظمات الحائزة على هذا المعيار ستعزز من مكانتها على المستوى المحلي والإقليمي، وسيشكل حصولها على هذا المعيار دافعا قويا للاستمرار في تطوير خدماتها ومنتجاتها وفق أعلى وأفضل المعايير والأنظمة الدولية للرفع من ثقة المواطنين والعملاء والمستثمرين في كافة الأنشطة والعمليات التي تقوم بها.

وفي الأخير نقدم جملة من التوصيات:

- العمل على التعريف بالمعايير الدولية الخاصة بأمن المعلومات لاسيما المعيار ISO / IEC 27001.
- زيادة التوعية بأن نظم أمن المعلومات التقليدية غير كافية لتحقيق درجة الأمان العالية والتوجه نحو تبني المعايير الدولية لأمن المعلومات.
- تكثيف الدورات التدريبية الخاصة بمعيار ISO / IEC 27001 للموظفين والمديرين للتركيز على أهمية هذا المعيار.

ISSN: 1112-4938, EISSN: 2600-6456

- توجيه المنظمات نحو اتساق نظم إدارة أمن معلوماتها مع متطلبات معيار ISO / IEC 27001.
- العمل على تشكيل فريق عمل لتهيئة متطلبات تطبيق المعيار ISO / IEC 27001.

الهوامش:

[1] J. Velasco, R. Ullauri, L. Pilicita, B. Jácome, P. Saa and O. Moscoso-Zea, "Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry," *2018 International Conference on Information Systems and Computer Science (INCISCOS)*, Quito, 2018, pp. 294-300, doi: 10.1109/INCISCOS.2018.00049.

[2] Candiwan, Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia.
, Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security, Kuala Lumpur, Malaysia, 2014.

3 Vladislav V. Fomin, Henk J. De Vries, Yves Barlette, Iso/Iec 27001 Information Systems Security Management Standard : Exploring The Reasons For Low Adoption, Euromot 2008 Conference, Nice, France.

[4] حسن طاهر داود، الحاسب وأمن المعلومات، الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة، الرياض، 2000، ص 23.

[5] خالد محمد خالد، أمن المعلومات والمواقع وأجهزة الكمبيوتر والدفع الإلكتروني، موسوعة التجارة الإلكترونية رقم 12، المركز العالمي لتبسيط العلوم، الإسكندرية، ص 40.

[6] حسن طاهر داود، مرجع سابق، ص 30.

[7] خالد محمد خالد، مرجع سابق، ص ص 42-45.

[8] أمير عكاشة، الإنترنت عالم مخيف ... مزاياه لا تحصى، وكالة الصحافة العربية، 2015، ص ص 73-75.

[9] أحمد عبد السلام أبو موسى، محمد شحاتة خطاب، عوامل نجاح برامج أمن نظم المعلومات المحاسبية ودورها في تفعيل حوكمة الشركات: دراسة ميدانية على الشركات السعودية، مجلة كلية التجارة للبحوث العلمية، الإسكندرية، 2012، ص ص 12-13.

[10] دلال صادق، حميد ناصر الفتال، أمن المعلومات، اليازوري، عمان، كتاب إلكتروني طبع في 21-02-2018، ص 23.

[11] https://www.cases.lu/la-famille-des-normes-iso-iec-27000.html Vu le 27-08-2020.

[12] https://www.iso.org/fr/isoiec-27001-information-security.html Vu le 15-07-2020.

[13] https://www.ysosecure.com/iso-27000.html Vu le 09-04-2020.

[14] http://www.iso27001security.com/html/timeline.html Vu le 19-07-2020.

[15] http://www.iso27001security.com/html/timeline.html Vu le 07-07-2020.

[16] http://www.iso27001security.com/html/timeline.html Vu le 29-07-2020.

[17] https://www.iso.org/fr/isoiec-27001-information-security.html Vu le 18-08-2020.

[18] Carol Hsu, Tawei Wang, Ang Lu, The Impact of ISO 27001 Certification on Firm Performance, 2016 49th Hawaii International Conference on System Sciences, p 4843.

[19] https://www.anitechconsulting.com.au/what-is-iso-27001/ Vu le 22-08-2020.

[20] الشريف بوفاس، فاطمة الزهراء طلحي، نحو بناء نظم لإدارة حماية المعلومات ISO 27001 في المؤسسات الجزائرية، المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقظة الإستراتيجية ونظم المعلومات في المؤسسة الاقتصادية، جامعة باجي مختار عنابة، 29-30 أفريل 2014، ص 7.

[21] https://www.itgovernance.eu/blog/en/why-are-so-many-organisations-getting-certified-to-iso-27001

[22] Razieh Sheikhpour, Nasser Modiri, best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management, Indian Journal of Science and Technology, Vol. 5 No. 2 (Feb 2012), p 2170.

[23] ISO/IEC 2005, International Standard, ISO/IEC 27001, First edition 2005-10-15, p vi.

[24] سعيد بن حمود الزهراني، المواصفة القياسية ISO 27000، مجلة عالم الجودة، العدد الثالث، أغسطس 2011، ص 9.

[25] https://www.anitechconsulting.com.au/what-is-iso-27001/ Vu le 14-08-2020

[26] https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/00._Overall_results_and_explanatory_note_on_2017_Survey_results.pdf?nodeid=19208898&vernum=-2 Vu le 09-07-2020

[27] http://www.iso27001security.com/html/27001.html Vu le 11-08-2020