ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الالكترونية

The Practices of Information Systems Security Governance in Institutions: Acceptance or Reduction of Cyber Attacks

كمال مسوس[1]، أستاذ محاضر ب، جامعة الجزائر3، الجزائر.
kamel.messous@gmail.com

تاريخ الاستلام: 2022/11/16 ؛ تاريخ القبول: 2022/12/27

مستخلص:

نظرا للأهمية التي يكتسيها أمن نظام المعلومات في المؤسسة والذي أعتُبر خلال السنوات الأخيرة حسب الدراسات المتخصصة من أهم الرهانات والتحديات التي تواجهها المؤسسة، يهدف هذا البحث إلى دراسة مساهمة ممارسات حوكمة أمن نظم المعلومات في الحد من الاعتداءات الالكترونية في المؤسسة. ومن أجل معالجة هذا الموضوع اعتمدنا على المنهج الاستنباطي للوصول إلى المبادئ العامة المتعلقة بأمن وحوكمة أمن نظم المعلومات. أما فيما يخص الطريقة المعتمدة في جمع المعلومات بغرض تحليلها فتمثلت في الطريقة الكيفية. كما اعتمدنا على مجموعة من الأدوات تجمع بين مختلف المراجع والمصادر الحديثة التي تخدم موضوع البحث، معتمدين على أحدث المعلومات والإحصائيات المتعلقة بمسألة أمن نظم المعلومات وحوكمته. وقد تم التوصل في هذه الدراسة إلى أن أمن نظم المعلومات في أي مؤسسة هو دائما عرضة للاعتداءات الالكترونية نظرا للحساسية والخصوصية التي تتميز بها هذه المؤسسة، وهو ما يجعلها اليوم بغض النظر عن طبيعتها وبالإضافة إلى ما تستخدمه من حلول تقنية جعلها تتوجه إلى استخدام مختلف المرجعيات الدولية التي تحد من الاعتداءات الالكترونية.

الكلمات المفتاحية: الاعتداءات الالكترونية، أمن نظم المعلومات، حوكمة أمن نظم المعلومات، المرجعيات والمعايير الدولية.

تصنيف JEL: M15؛ O19.

Abstract:

The research aims to study the contribution of the practices of information systems security governance to reduce the cyber attacks in these institutions or organizations. To address this issue, we relied on the deductive approach

[1] كمال مسوس: kamel.messous@gmail.com

to reach the general principles of information security and governance. As for the method used to gather information for analysis, it was qualitative. We have also adopted a set of tools that combine the various references and modern sources that serve the subject of the research, relying on the latest information and statistics on the issue of security and information systems in the institutions. The study concluded that the security of the information systems in any institution is always subject to electronic attacks, according to the sensitivity and privacy that characterize it, which made the institution today - looking at the nature and in addition to the use of technical solutions - to use Various international references that limit these cyber attacks.
Key Words: cyber attacks, information systems security, information systems security governance, international Standards and Referentiels.

Jel Classification Codes : M15 ; O19.

مقدمة:

نجاح تطبيق نظم المعلومات في المؤسسة مرتبط بمدى جودة المعلومات التي تقدمها لمستخدميها، ومرهون بنوعية الوصول إليها بيضاء، رمادية وسوداء وبحسب المستويات الإدارية التي تستخدم فيها : تشغيلية، معرفية، تكتيكية وإستراتيجية.

اليوم النظم المعلوماتية في المؤسسة هي أكثر عرضة للاعتداءات الالكترونية، وتتطلب حمايتها تحقيق مجموعة من الشروط أهمها السرية، السلامة، التوافر، وهذا من خلال توفير الحلول التقنية، كالتشفير الالكتروني، التوقيع الالكتروني، الحلول المتعلقة بأمن الشبكة، البرمجيات المضادة للاعتداءات الالكترونية، وغيرها من الحلول، بالإضافة إلى توفير الأمن الالكتروني على خدمات الحوسبة السحابية وعلى الأجهزة الشخصية المستعملة لأغراض مهنية، لكن بالرغم من توفر هذه الحلول، مسألة أمن نظم المعلومات حسب الدراسات المتخصصة لا تزال من الأولويات الأساسية في المؤسسة، والتي تحتاج وتتطلب تبني مقاربة جديدة تضمن المزيد من الحماية لهذه النظم.

ويتزايد اليوم الاعتراف بحوكمة أمن نظم المعلومات كمقاربة جديدة يجب أن تتبناها المؤسسة للحد والتخفيف من حدة الاعتداءات الالكترونية، وذلك بفضل ما تُتيحه هذه الحوكمة من مختلف المرجعيات والمعايير مثل : مرجعية Risk IT، والمعايير التي تقدمها منظمة التقييس الدولية ISO 27001، مرجعية Cobit5، مرجعية ITIL V3، وغيرها من المرجعيات والمعايير، والتي تتضمن الشروط الأساسية لضمان سرية، سلامة وتوافر المعلومات الخاصة بهذه المؤسسة.

من خلال ما سبق سنحاول من خلال هذه الدراسة الإجابة عن التساؤل الرئيس الأتي : **ما هي مساهمات حوكمة أمن نظم المعلومات في الحد والتخفيف من الاعتداءات الالكترونية التي تواجه المؤسسة ؟**

وعليه هذه الدراسة هي محاولة لتحديد طبيعة الاعتداءات التي تتعرض لها المؤسسة بمختلف أشكالها والتطرق لأهم الإحصائيات الخاصة بالاعتداءات الالكترونية، التطرق إلى الحلول الحديثة لأمن المعلومات. بالإضافة إلى تحديد المفاهيم والأهداف المتعلقة بمقاربة حوكمة أمن نظم المعلومات، وفي الأخير نستعرض أهم المرجعيات والمعايير الدولية التي يجب أن تتبناه المؤسسة للحد والتخفيف من الاعتداءات الالكترونية.

1- الاعتداءات الالكترونية دو افعها و أثارها على المؤسسات:

حسب المختصين في أمن المعلومات، فإن الاعتداءات الالكترونية cyber attacks هي كل اعتداء يهدف إلى إلحاق الضرر أو أضرار بنظم معلومات المؤسسة، ويتجلى ذلك من خلال مجموعة من العناصر أهمها سلامة المعلومات، توافرها وسريتها وغيرها من العناصر، هذه الاعتداءات تختلف درجة وحدة خطورتها حسب طبيعة الدافع من الاعتداء، وعادة ما يكون بدافع سياسي، اقتصادي بالدرجة الأولى وبدوافع اجتماعية وغيرها من المجالات بدرجة أقل، وحسب الهدف من الاعتداء منها من يكون بهدف الحصول على الأولى، ومنها من يقوم بالاعتداء للفضول والافتخار، وغيرها من الاعتداءات. وعليه سنقوم فيما يلي بعرض الأسباب والدوافع من الاعتداءات الالكترونية، أثارها على مؤسسة ومن ثم تقديم بعض المعلومات والأرقام عن هذه الاعتداءات.

1-1- دو افع الاعتداءات الالكترونية على المؤسسات:

يتفق المختصون بأن الاعتداءات الالكترونية على المؤسسات تختلف باختلاف الدافع من الاعتداء الالكتروني، فعلى سبيل المثال تشير دراسة حديثة قامت بها فريق Radware (مجموعة من الخبراء في مجال امن المعلومات) خلال سنة 2017 بأن الاعتداء يستهدف بالدرجة الأولى طلب الفدية بما يقارب 40 %، وبدرجة أقل كل من التهديدات الداخلية، الأسباب السياسية ، المنافسة، بالإضافة إلى ما يعرف بالحرب الالكترونية(تتراوح ما بين 24 و 27 % لكل اعتداء)، في حين يمثل فيه غضب المستخدمين 20 % كدافع للاعتداء، و11 % تبقى أسباب ودوافع غير معروفة. وفي دراسة أخرى قامت بها مؤسسة Verizon للاتصالات سنة 2017 أيضا أظهرت بأن الدوافع الأساسية للاعتداءات الالكترونية ترتبط بدرجة أولى بأسباب مالية والتجسس، وبغرض الفضول والافتخار (https://www.visualcapitalist.com/hakers-hack-motives-behind-cyberattacks/, 01/2019) .

وحسب المختصين في أمن المعلومات أيضا، أن المؤسسات التي ترتكز ثقافتها على الانفتاح على أصحاب المصالح من زبائن وموردين وشركاء ومساهمين وما إلى ذلك، عادة ما ينظر لها كهدف سهل للقرصنة، وذلك نظرا لما تتيحه لهم من تواصل وتعاون في أي وقت ومن أي مكان عبر شبكاتها المختلفة (أنترنت، أنترانت، إكسترانت...)، الأمر الذي يجعل من هذه المؤسسات هدفا جذابا للمهاجمين السيبيرانيين.

وعليه فإن الدافع من وراء الاعتداءات الالكترونية يختلف باختلاف حجم المؤسسات وسمعتها، ومن المرجح أن تكون مؤسسات مستهدفة بالخصوص من قبل عصابات الجريمة المنظمة أو الحكومات الأجنبية التي ترغب في الوصول إلى البيانات القيمة والحساسة، وعلى العموم هناك العديد من الأسباب التي تؤدي إلى استهداف المؤسسات نذكر منها (Raman, 2016, P51):

- التهديد يكون من أجل الإضرار بسمعة المؤسسة وبسبب الدوافع المالية؛
- التهديد يكون من أجل الظهور إعلاميا وإثبات أن المؤسسة غير قادرة على مواجهة الخروقات الأمنية؛
- التهديد يمكن أن يأتي من الداخل للتلاعب بنظم المؤسسة ومن أجل المساعدة على اعتداء سبيراني منظم ؛
- التهديد يمكن أن يأتي من الحكومات الأجنبية التي تريد الوصول إلى الأبحاث السرية مثل المتعلقة بالطاقة النووية؛
- التهديد يكون من أجل التجسس على أسرار المؤسسات، وذلك للحصول على الأبحاث السرية.

2-1- تأثير الاعتداءات الالكترونية على المؤسسات:

يمكن أن تتسبب الاعتداءات الالكترونية في إلحاق أضرار كبيرة على المؤسسات، بحيث يمكن أن تؤثر من الناحية المالية، بالإضافة إلى ذلك يمكن أن تؤثر على سمعة المؤسسات وثقتها بالزبائن أو العملاء وما إلى ذلك. وفي الغالب يتم تقسيم أثر الاعتداءات في المؤسسات إلى ثلاث أصناف، منها ما له علاقة بالجانب المالي، السمعة والجانب القانوني(nibusinessinfo.co.uk, 10/2022) .

- **التكلفة الاقتصادية للاعتداء الالكتروني**: غالبا ما تؤدي الاعتداءات الالكترونية إلى تكبيد المؤسسات خسائر مالية كبيرة، في الغالب تنشأ عن سرقة معلومات المؤسسات، سرقة الأموال والمعلومات المالية (بطاقات الدفع الإلكتروني)، تعطيل

تنفيذ المعاملات عبر الانترنت، خسارة الأعمال والعقود، كما تنجر عن هذه الاعتداءات تكاليف أخرى ترتبط عموما بإصلاح الأنظمة، والشبكات والأجهزة المتأثرة.

- **الأضرار الناتجة عن السمعة**: الثقة هي عنصر أساسي في علاقة المؤسسات بعملائها أو ذوي أصحاب المصالح، وعليه يمكن أن تتسبب الاعتداءات الالكترونية في الإضرار بسمعة المؤسسات، وهذا ما قد يؤثر عليها كخسارة العملاء، خسارة المبيعات، التخفيض في الأرباح، كما قد يؤثر أيضا على علاقاتها مع جميع أصحاب المصالح كالموردين، المساهمين، الشركاء، وغيرهم.
- **العواقب القانونية للاعتداءات الالكترونية**: تتطلب الاعتداءات الالكترونية توفر الإطار القانوني لحماية البيانات والخصوصية إدارة أمن جميع البيانات الشخصية التي تمتلكها – سواء كان ذلك على موظفيك أو عملائك. بحيث إذا تم اختراق هذه البيانات عن طريق الخطأ أو عن طريق العمد ، وفشلت المؤسسات في توفير التدابير الأمنية المناسبة ، فقد تواجه غرامات وعقوبات تنظيمية .

1-3- بعض الحالات والمعلومات عن الاعتداءات الالكترونية في بعض المؤسسات:

فيما يلي جدول يلخص بعض أهم الاعتداءات الالكترونية تأثيرا، والتي جرت ما بين سنة 2013 وسنة 2022:

جدول رقم (1): بعض أهم الاعتداءات الالكترونية ما بين 2013 و 2022.

السنة	أبرز الاعتداءات الالكترونية
2013	• قنبلة نووية أطلق العميل السابق بوكالة الأمن القومي الأمريكي إدوارد سنودن بأن الولايات المتحدة الأمريكية وبريطانيا تقومان بالتنصت على جميع الاتصالات في جميع أنحاء العالم، هذا التنصت شمل الإرهابيين المحتملين والحكومات والشركات الصديقة ؛ • اختراق حساب تويتر لـ Burger King's من قبل هاكرز ووضع مكانه شعار McDonald's.
2014	• الويب تلقى إعتداء كارثي يسمى Heartbleed، هذا الاختراق ضرب قلب أمن الويب، حيث سمح هذا الاعتداء بجمع البيانات الحساسة من الخوادم الآمنة دون أن يترك أي أثر.
2015	• اختراق email لمدير وكالة المخابرات الأمريكية، حيث تم الوصول إلى وثائق جد حساسة .
2016	• اختراق البريد الالكتروني للمرشحة للرئاسيات الأمريكية هيلاري كلينتون، حيث كانت تحتوي على وثائق سرية حكومية، هذا الاختراق أثر على نتائج النهائية للانتخابات التي فاز بها ترامب.
2017	• هجوم Wannacry، مس هذا الهجوم أكثر 300000 جهاز في أكثر من 150 دولة وسبب خسائر مالية تجاوزت مليار دولار.

يتبع الجدول رقم (1): أهم الاعتداءات الالكترونية ما بين 2013 و 2022

2018	• إختراق أكثر من 50 مليون حساب فايسبوك مما أدى إنخفاض أسهم الشركة.
2019	• إختراق مؤسسات الأنترنت ICANN وبعض تطبيقات Google .
2020	• إطلاق mises à jour piégées لمنصة أحد المؤسسات الأمريكية المتخصصة في أدوات المراقبة عن بعد، مما أثر ذلك على 18000 من زبائن المؤسسة ومئات الشركات الأمريكية .
2021	• هجوم DarkSide الذي سبب شلل في خط أنابيب البترول الأمريكية وخسارة أكثر من 40 مليون دولار؛ • ظهور برنامج بيغاسوس يسمح بالتجسس على الشخصيات والحكومات التي تستعمل أنظمة التشغيل IOS.
2022	• تعرض العديد من المواقع التي تعتمد على العملات الرقمية للهجمات الالكترونية باستعمال أسلوب الاصطياد الالكتروني والهندسة الاجتماعية.

المصدر: من إعداد الباحث بالاعتماد على مصادر متخصصة في أمن المعلومات.

2- الحلول الحديثة لأمن المعلومات:

يعتبر أمن أنظمة المعلومات من الركائز الأساسية التي تأخذها المؤسسة بعين الاعتبار وتضع له ميزانيات ضخمة، وذلك من أجل الحد أو التقليل من مختلف المخاطر والاعتداءات الالكترونية التي تواجهها، وبالتالي السماح لها بالتقليل من مختلف الخسائر التي قد تصيبها، فأمن نظم المعلومات مصطلح يصف الحاجة لحماية المعلومات ولذلك استناد إلى حقيقة أن المعلومات تعتبر موردا قيما في المؤسسة.

2-1- مفهوم أمن نظم المعلومات وشروطه:

الأمن بشكل عام هو الجودة أو الحالة التي تضمن بأنها آمنة من أي خطر، وهذا يعني أن تكون محمية من الأعداء الذين يريدون الضرر بها سواء بقصد أو بغير قصد، ولكي تضمن المؤسسة نوعا ما الحماية لعملياتها يجب أن تضع طبقات متعددة للأمن، تتمثل هذه الطبقات في العناصر التالية (Singh & al., 2014, P1073) :

- **الأمن المادي**: لحماية المؤسسة من الوصول غير المصرح به وإساءة الاستخدام ؛
- **أمن الأفراد**: لحماية الفرد/ مجموعة من الأفراد المصرح لهم بالدخول إلى بيانات المؤسسة؛
- **أمن العمليات**: لحماية تفاصيل عملية أو سلسلة من أنشطة معينة ؛
- **أمن الاتصالات**: لحماية المؤسسة من وسائل الاتصال والتكنولوجيا ؛
- **أمن الشبكة**: لحماية شبكات المؤسسة ؛
- **أمن نظم المعلومات**: لحماية المعلومات وعناصرها الهامة بما في ذلك الأنظمة والأجهزة.

من وجهة نظر الباحثين والمختصين يعتبر أمن نظم المعلومات عبارة عن الطرق والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من السرقة والتشويه والتلف والضياع والتزوير، والاستخدام غير المرخص، وغير القانوني (فضال السامرائي، 2009،ص 283)، ويشير أيضا إلى التدابير والإجراءات المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية من أجهزة ، برمجيات بيانات وأفراد، ومن التجاوزات والتدخلات غير المشروع التي تقع عن طريق الصدفة أو عمدا أو عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير كافية تستخدمها الإدارة (الفتال، 2008، ص-ص: 11-12).

ومن وجهة نظر الهيئات والمؤسسات المتخصصة في أمن المعلومات، نجد أن أمن المعلومات أو نظم المعلومات حساب وكالة الأمريكية للأمن القومي يشير إلى حماية المعلومات ضد أي وصول غير مرخص إلى المعلومات أو أي تعديل غير مرخص به أثناء حفظها ومعالجتها ونقلها، وضد منع تقديم الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لاشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف ومواجهة المخاطر والاعتداءات (Urbina, 2006, P724)، وحسب منظمة التقييس العالمية (ISO) ووفق ما جاء في معيار ISO 27000 فإن أمن نظم المعلومات يشير إلى الحفاظ على سرية، سلامة وتوافر المعلومات (International Standard, 2009, P7)، ويعني حسب لجنة الأمن القومي للنظام الأمريكية CNSS هو حماية المعلومات ونظم المعلومات من الوصول غير المصرح به، الاستخدام، الافصاح، الإخلال أو التعديل أو التدمير وذلك من أجل توفير سرية وسلامة وتوافر البيانات (Committee on Natinal Security Systems, April 2010, P37). وحسب جمعية تدقيق ومراقبة نظم المعلومات ISACA أمن المعلومات يعني ضمان للمستخدمين المخولين فقط، الحصول على معلومات دقيقة وكاملة وعند الحاجة (ISACA, 2015, P49)، أما المعهد القومي للمعايير والتكنولوجيا هو عبارة عن الاجراءات التي تحمي وتدافع عن المعلومات ونظم المعلومات من خلال ضمان توافرها، سلامتها وموثوقيتها، سريتها وعدم الإنكار (Kissel, 2013, P93).

وعليه من خلال التعاريف السابقة نستنتج أن أمن نظم المعلومات هو حماية المعلومات ونظم المعلومات من الأشخاص غير المخول لهم سواء بقصد أو بغير قصد والذين يهدفون إلى التغيير، التعديل أو الكشف، بما يضمن سرية، وسلامة وتوافر المعلومات .

ونستنتج أيضا من خلال ما سبق أن جميع الباحثين والهيئات والمؤسسات الدولية المتخصصين في أمن المعلومات بأن ثلاثية CIA من الشروط المهمة جدا في أمن نظم المعلومات، والتي تعني سرية، سلامة وتوافر المعلومات (Taylor, 2008, P2) .

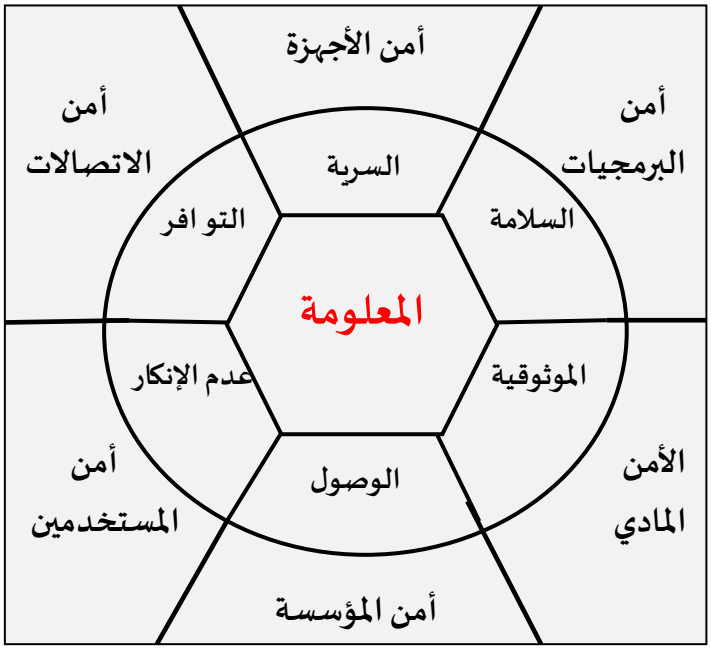
- **سرية المعلومات**: المعلومة هي أصل من الأصول المهمة للمؤسسة، وخاصة فقط بالمستخدمين المخولين الوصول إليها؛
- **سلامة المعلومات**: المعلومة هي مورد حساس، تتطلب أن تكون دقيقة وكاملة وخالية من أي تغيير أو تعديل، سواء بقصد أو غير قصد؛
- **تو افر المعلومات**: والتي تعني أن المعلومة يجب أن تكون المتوفرة ومتاحة في الوقت المناسب، وعادة ما يتم التعبير عنها بنسبة مئوية.

بالإضافة إلى ذلك هناك بعض الباحثين، قاموا بإضافة عناصر أخرى لا تقل أهمية عن الشروط السابقة، أهمها (Hélie, 2008, P2):

- **موثوقية المعلومة**: والتي تعني ضرورة التحقق من هوية المستخدم والجهات المتعامل معها عند بث المعلومة ؛
- **عدم الإنكار**: بمعنى الطرف المتعامل معه لا يمكن إنكار القيام بالمعاملة، وعادة ما يتم التأكد من هذا الشرط عن طريق ما يعرف بالشهادة الالكترونية؛
- **ضبط الوصول**: ويعني القدرة على الحد أو السيطرة على الوصول إلى النظم والتطبيقات عن طريق وصلات الاتصال .

فيما يلي الشكل التالي يوضح النموذج المعدل لشروط أمن نظم المعلومات

الشكل رقم (01): النموذج المعدل لشروط أمن المعلومات



المصدر: من إعداد الباحث وفقا لما عكسه الأدبيات

2-2- مبادئ أمن نظم المعلومات:

يوجد ثلاث مبادئ أساسية في أمن نظم المعلومات، يجب على القائمين على المؤسسة أخذها بعين الاعتبار ، وذلك عن استخدام نظم المعلومات من جهة والجوانب المتعلقة بأمنها من جهة أخرى. تتمثل هذه المبادئ في العناصر التالية (Gelbstein, 2002, P-P : 16-18):

- **الأمن قابل للتحقق بنسبة 100 % :** بمعنى أنه لا يوجد نظام معلوماتي آمن بنسبة 100% على الإطلاق في الماضي والحاضر والمستقبل، فحسب أحد المختصين في أمن المعلومات والتشفير Bruce Shneire " فقط الحاسوب المطفأ والمغلق عليه في خزانة حديدية والموجود على بعد ست أقدام تحت الأرض وفي مكان سري يمكن اعتباره محميا (كربيط، 2018، ص71)، ويعود هذا السبب وراء تلك الحقيقة إلى طبيعة السجال بين أخصائي أمن نظم المعلومات بمختلف تخصصاتهم من جهة والمخترقين والمهاجمين والمتطفلين بكافة أنواعهم وأهدافهم وطرقهم من جهة أخرى، حيث أن المعركة الالكترونية بين هذين الفريقين تدور رحاها بين الكر والفر، حيث أنه كلما نجح أخصائيو أمن نظم المعلومات في إبتكار تقنيات أمنية جديدة، كلما سارع خصومهم من المخترقين لمحاولة إبطال فعالية تلك التقنيات، ومن المعروف أن مهام الدفاع التي يقوم بها أخصائيو أمن نظم المعلومات تقتضي أن يتم إغلاق جميع الثغرات الأمنية في الأنظمة الإلكترونية التي يقومون بحمايتها، بين وجود ثغرة أمنية واحدة في حال إكتشافها كفيل بتنفيذ الهجوم الذي قد ينجر عنه خسائر مالية كبيرة جدا وغيرها من الجوانب.
- **المخاطر والنفقات بحاجة إلى توازن:** يشير Stephane Nappo مختص في أمن المعلومات " بأن أحد المخاطر الالكترونية الرئيسية في المؤسسة هو إما إعتقاد أنها غير موجودة أو الإعتقاد بمحاولة معالجة جميع المخاطر المحتملة " (Nappo, 04/2020, https://www.goodreads.com/quotes/10043276) وعليه ضمان أمن نظم المعلومات يوجب على المؤسسة اتخاذ جميع التدابير اللازمة من أجل حماية المعلومات،

حيث تتأثر الدرجة التي يتم اتخاذها في هذه التدابير بتقييم المخاطر والاعتداءات الالكترونية المحتملة واستعداد المؤسسة لقبول القيود والمعوقات، فالتدابير سوف تحمل المؤسسة تكاليف معين خلال دورة حياتها، بحيث أنه أيا كانت التدبير المتخذة ليس هناك من يضمن بأنها ستكون فعالة في أي وقت، والمخاطر التي تسعى المؤسسة لحمياتها نفسها منها سوف تتغير أيضا في أي وقت، وبالتالي عملية التقييم واتخاذ التدابير الوقائية تحتاج إلى تغيير لتكون فعالة، كما أن التدابير الأمنية ستتطلب من المؤسسة استثمارات ونفقات متكررة قد تكون كبيرة جدا.

فحسب Bruce Shneire أنه إذا كانت تكاليف أمن المعلومات أقل من التكاليف المحتملة للخسائر بسبب نقص الأمن، حيث في هذه الحالة يكون الأمن مرضي للمؤسسة، وأما إذا كانت تكاليف الأمن أكثر فما على المؤسسة إلى تقبل الخسائر (www.goodreads.com, p3)؛

- الحماية والسلبيات بحاجة إلى توازن: في عالم الحماية لا يوجد شيء مثالي، وهذا ينطبق على المعلومات، فالتدابير الأمنية التي تتخذها المؤسسة قد تنطوي على سيرورات إضافية، تكون بمثابة عقبات لمستخدمي المؤسسة، وبالتالي تتطلب منهم التغلب عليها بغض النظر عن حجم هذه العقبات كالأقفال المتعددة، أجهزة الإنذار، والحاجة إلى تذكر العديد من كلمات السر وغيرها من العقبات.

2-3- الوسائل المعتمدة في أمن نظم المعلومات:

يستخدم في مجال أمن نظم المعلومات، العديد من أدوات ووسائل الحماية ضد مختلف الاعتداءات الالكترونية، لذا سنذكر أهم هذه الوسائل على النحو التالي:

- **التشفير الإلكتروني**: هو عبارة عن عملية رياضية (معادلات خوارزمية)، يتم من خلالها تحويل النص المراد إرساله إلى رموز وإشارات، لا يمكن فهمها إلا بعد القيام بفك الشفرة، وتحويل الرموز والإشارات إلى نص مقروء من خلال استخدام مفاتيح عامة وخاصة (محمد فواز، 2006، ص 159)؛
- **تطبيقات دالة التجزئة** : هي مجموعة من التطبيقات تهدف إلى تحقيق شرط من شروط أمن المعلومات يتعلق بسلامة المعلومات، وهي عبارة عن خوارزمية تعمل على ضمان على تبادل المعلومات بطريقة آمنة (www.cyber-arabs.com/, 10/2022)، ولعلى من أبرز البرامج المستخدمة في هذا النوع من التطبيقات نجد: MD5 و MD6 (Stevens , 2012, P:13).

- **التوقيع الإلكتروني**: هي نتاج أي وسيلة إلكترونية للتوقيع (Davis, 2016)، ويقصد به استخدام طريقة معينة للتحقق من أن صاحب المعاملة هو نفس الشخص الذي قام إرسالها أو تنفيذها (إسماعيل برهم، 2005، ص 84)، وللتوقيع الالكتروني عدة أشكال أبرزها التمثيل الإلكتروني بخط اليد الإلكتروني، البصمة الإلكترونية، الفحص بشبكية العين، وشهادة المصادقة عبر الموقع.
- **حلول أمن الشبكة:** يتشكل أمن الويب في المؤسسة من سبعة طبقات، وكلما تمكنت المؤسسة تعزيز هذه الطبقات بمختلف الأجهزة والتطبيقات كلما ساعد في تعزيز أمن الشبكة، ولعلى من أبرز التطبيقات والأجهزة التي تساعد على توفير الحماية اللازمة للشبكة نجد:
  - **المصادقة الأساسية:** تتطلب المصادقة الأساسية توفير اسم المستخدم وكلمة المرور للمستخدمين، حتى يتمكن من الوصول إلى جزاء أو كل المحتوى، وذلك وفق الصلاحيات المخولة له (technet.microsoft.com/, 10/2022).
  - **برتوكول (TLS/SSL):** ينص هذا البرتوكول على خصوصية الاتصالات عبر الانترنت ويسمح بالمرور إلى المعلومات بطريقة آمنة (www.ietf.org/, 2019).
  - **الشبكة الخاصة الافتراضية:** تسمح هذه الشبكة بإنشاء ممر آمن بين المرسل والمستقبل . (حديد،2007، ص 187)، وهو عبارة عن معيار يسمح بضمان التواصل الآمن عبر بروتوكول الانترنت (Singh, January 2014, P1076)؛
  - **برتوكول مصادقة الشبكة kerberos:** هذا البروتوكول مصمم لتوفير مصادقة قوية بين الخادم والزبون باستخدام مفتاح سري لتشفير كافة الاتصالات عبر الشبكة (http://web.mit.edu/kerberos/, 26 May 2022).
  - **التحكم في الوصول عن طريق الجدران النارية:** وهي عبارة عن نظام يفرض سياسة التحكم في الوصول بين شبكتين، ويحدد الخدمات الداخلية التي يمكن الوصول إليها من الخارج والعكس، وهو بهذا يعمل وفق آليتين واحدة لمنع حركمة المرور والثاني للسماح بحركة المرور (3Com Corporation, 2000, P2)، وهي تنقسم إلى نوعين جدران المادية وجدران النار البرمجية..
  - **البرمجيات المضادة للاعتداءات الالكترونية :** تعمل هذه البرمجيات على كشف وتدمير وتجميد البرمجيات الخبيثة وبرامج الجوسسة وغير ها من الاعتداءات الالكترونية (Kaseya Corporation, septembre 2013, P1).

3- حوكمة أمن نظم المعلومات – المفهوم والأهداف:

حسب Kiven Mitnick مستشار في أمن المعلومات ومن أبرز الهاكرز في العالم يقول "يمكن أن تنفق المؤسسة مئات الآلاف من الدولارات على الجدران النارية وأنظمة كشف التسلل والتشفير وغيرها من تقنيات الآمان، ولكن إذا كان المهاجم يستطيع الاتصال بأحد الأشخاص الموثوق بهم داخل المؤسسة، فإن كل الأموال التي تنفق على التكنولوجيا تصبح لا معنى لها ". (https://www.azquotes.com/author/10219-Kevin_Mitnick, 2022).

وعليه يجب على المؤسسة الاستعداد والاستباق لأي هجوم سيبراني، بدلا من تركيز كل الجهود على التدابير الأمنية التقليدية، وهذا من أجل مواجهة مختلف التغيرات المعقدة التي تشهدها البيئة في مجال أمن المعلومات.

وكنتيجة لزيادة الوعي الإستراتيجي للمؤسسة بأهمية مواجهة مختلف التحديات، المتعلق بالاعتداءات الالكترونية، ظهور مفهوم المرونة الالكترونية، هذا الأخيرة أدت إلى ظهور مقاربة جديدة في أمن المعلومات تسمح بتقديم أفضل الممارسات في المؤسسة تمثلت في حوكمة أمن نظم المعلومات.

3-1- مفهوم المرونة الالكترونية:

تشير المرونة الالكترونية إلى قدرة النظام على الاستعداد، الاستيعاب، التعافي، والتكيف مع الآثار الضارة، لا سيما تلك المرتبطة بالهجمات الالكترونية (Linkov I. & Kott A., 2018)، ويعرف أيضا على أنه قدرة المؤسسة على الاستمرار في تنفيذ مهمتها من خلال توقع التهديدات الالكترونية والتكيف معها والتغييرات الأخرى ذات الصلة في البيئة ومن خلال تحمل الحوادث الالكترونية واحتوائها والتعافي منها بسرعة (Islam E. & Christoforides C., 2019, P4) والذي يكون من خلال التحليل الإستباقي الجيد لنقاط الضعف البيئة الرقمية الداخلية والخارجية للمؤسسة

3-2- مفهوم حوكمة أمن نظم المعلومات:

حسب معهد حوكمة نظم المعلومات تعرف حوكمة أمن نظم المعلومات على أنها جزء لا يتجزأ من حوكمة المؤسسات، تعمل على توفير التوجيه الاستراتيجي، وتضمن تحقيق الأهداف، وإدارة المخاطر بشكل مناسب، واستخدام الموارد التنظيمية بمسؤولية، ورصد وتتبع نجاح أو فشل البرامج المستخدمة في أمن المعلومات (IT Governance Institute, 2006, P17)، وتعرف أيضا على أنه مجموعة من المسؤوليات والممارسات التي يقوم بها مجلس الإدارة والإدارة التنفيذية

بهدف توفير اتجاه نحو إستراتيجية أمن المعلومات وضمان تحقيق أهدافها، والتأكد من أن موارد نظم المعلومات يتم استخدامها بشكل فعال (علي خليل، 2013، ص11)، وتعرف أيضا على أنها بناء نظري يصفه Von Solmsc من حيث الموجات، الموجة الأولى تتعلق بالاطار التكنولوجي أو عناصر تكنولوجيا المعلومات في أمن المعلومات، الموجة الثانية فتتعلق بمفهوم إدارة أمن المعلومات أو الهياكل التنظيمية المرتبطة بالأمن، أما الموجة الثالثة والأخيرة فترتبط بإضفاء الطابع المؤسسي على أمن المعلومات (Luesebrink, 2011, P51).

3-3- أهداف حوكمة أمن نظم المعلومات:

الهدف الأساسي من حوكمة أمن نظم المعلومات هو ضمان التحكم في مختلف المخاطر المتعلق بنظم المعلومات، مع عدم إهمال كل ماله علاقة بالشفافية، بما يسمح بضمان سرية وسلامة وتوافر المعلومات إلى مستويات تتقبلها المؤسسة، ولتحقيق هذا الهدف وتحقيق حوكمة فعالة لأمن نظم المعلومات يجب على الإدارة إعداد ووضع إطار يسمح بتطبيق أفضل الممارسات المتعلقة بأمن نظم المعلومات، وعلى العموم يمكن أن يشمل هذا الإطار العناصر التالية (IT Governance Institute, 2006, P 18):

- منهجية لإدارة مخاطر أمن نظم المعلومات ؛
- إستراتيجية أمنية شاملة مرتبطة صراحة بأهداف الأعمال وتكنولوجيا المعلومات ؛
- هيكل تنظيمي أمني فعال ؛
- إستراتيجية أمنية تتحدث عن قيمة المعلومة المحمية وتسليمها؛
- سياسات الأمن التي تعالج كل جانب من الجوانب الإستراتيجية والمراقبة والتنظيم؛
- مجموعة كاملة من المعايير الأمنية لكل سياسة، لضمان المطابقة للإجراءات والمبادئ التوجيهية للسياسة ؛
- سيرورة رصد ومتابعة لضمن المطابقة وتوفير التغذية العكسية بشأن الفعالية والتخفيف من المخاطر ؛
- سيرورة لضمان استمرار تقييم وتحديث السياسات والمعايير والإجراءات المتعلقة بالمخاطر الأمنية .

4- مرجعيات ومعايير حوكمة أمن نظم المعلومات:

ترتبط مسألة ضمان التطبيق الجيد لممارسات حوكمة أمن نظم المعلومات بالعديد من المرجعيات والمعايير الدولية أهمها :

4-1- مرجعية مخاطر تكنولوجيا المعلومات Risk IT:

تعتبر هذه المرجعية من أبرز المرجعيات الحديثة التي تعالج مخاطر تكنولوجيا المعلومات، تم إنشاؤها من قبل جمعية تدقيق ومراقبة نظم المعلومات، وهي عبارة عن دليل يسمح بإعطاء نظرة شاملة عن المخاطر المرتبطة بتكنولوجيا المعلومات، ويساعد المؤسسة على إدارتها من أجل تحقيق الأهداف المسطرة.

يتم التعبير عن المخاطر المعلوماتية وفق هذه المرجعية من منطلق مفهوم المهن، وعلى هذا الأساس تستند هذه المرجعية على العديد من المرجعيات والنماذج تتمثل فيما يلي (ISACA, 2009 , P23):

- **مرجعية COBIT5**: من حيث معايير جودة المعلومة (الكفاءة، الفعالية، السرية، السلامة، التوافر، المطابقة والخصوصية)؛
- **بطاقة الأداء المتوازن**: التي تقيم أداء المؤسسة من أربع جوانب (المنظور المالي، منظور السيرورات الداخلية، منظور التعلم والنمو و منظور الزبائن)؛
- **قانون COSO**: وفق أربع جوانب تتمثل في: الإستراتيجية، السيرورات، التقارير والمطابقة ؛
- **نموذج Westerman**: الذي يهتم بكيفية تحويل مخاطر تكنولوجيا المعلومات إلى ميزة تنافسية ؛
- **نموذج تحليل معامل مخاطر المعلومات**: وذلك من حيث الإنتاجية، تكاليف المعالجة، تكاليف الإستبدال، الميزة التنافسية، القوانين والسمعة .

إن استخدام مرجعية مخاطر تكنولوجيا المعلومات يمكن أن يساعد المؤسسة من تحقيق العديد من المزايا أهمها(ISACA, 2012, P5):

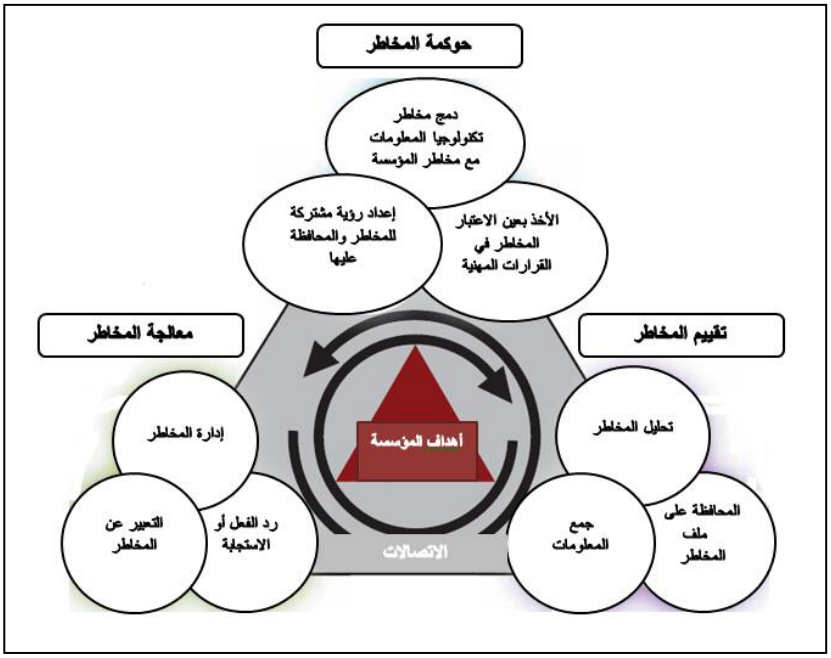
- تقديم لغة مشتركة تساعد في التواصل بين الإداريين وتكنولوجيا المعلومات، وإدارة المخاطر؛
- تسمح بتقديم توجيهات من طرف إلى طرف بشأن كيفية إدارة المخاطر المتعلقة بتكنولوجيا المعلومات ؛
- تقديم لمحة كاملة عن المخاطر، والسماح بفهم أفضل لها وذلك للاستفادة بشكل أفضل من موارد المؤسسة ؛
- فهم أفضل للأدوار والمسؤوليات فيما يتعلق بإدارة مخاطر تكنولوجيا المعلومات؛
- الاصطفاف مع إدارة المخاطر الأخرى المتعلقة بالمؤسسة ؛
- تسمح بتحقيق رؤية أفضل للمخاطر المتعلقة بتكنولوجيا المعلومات وآثارها المالية ؛

- تسمح بتحقيق عدد أقل من المفاجآت والخفاقات التشغيلية؛
- زيادة جودة المعلومات ؛
- زيادة ثقة أصحاب المصالح وتخفيض المخاوف التنظيمية ؛
- تقديم تطبيقات مبتكرة تدعم مبادرة التحسين الجيدة للمؤسسة .

ومن أجل تحقيق هذه المزايا ترتكز هذه المرجعية على مجموعة من المبادئ، و على نموذج ذو ثلاث ميادين أساسية تتمثل في حوكمة المخاطر، تقييم المخاطر، ومعالجة المخاطر، وكل ميدان من هذه الميادين يتضمن ثلاث سيرورات (9 سيرورات في المجموع)، تنقسم بدورها إلى 43 نشاط أو هدف (ISACA, 2009, P34)، وإذا تمكن المؤسسة من تحقيق هذه الأهداف يمكن القول بأنها تحكمت إلى حد كبير في المخاطر والاعتداءات التي تتعرض لها المؤسسة.

فيما يلي الشكل التالي يوضح الميادين والسيرورات الخاصة بهذا النموذج :

الشكل رقم (02): مرجعية مخاطر تكنولوجيا المعلومات



Source : ISACA, The IT Framework, op. cit., P34.

4-2- معيار إيزو27001:

يهتم هذا المعيار ويعالج نظام إدارة أمن المعلومات ومتطلباته، وهو عبارة عن معيار دولي لنظام إدارة أمن المعلومات، تم إصداره سنة 2005 وأخر تحديث له كان في سنة 2013، فيما يلي أهم العناصر التي يعالجها هذا المعيار (www.itgovernance.co.uk, 2013, P-P : 2-5):

- الهيكلة: تتضمن الهيكلة الجديدة سبعة بنود تتمثل في: سياق المؤسسة، القيادة، التخطيط ، دعم العمليات، تقييم الأداء والتحسين، وتعمل هذه البنود على التأكد من أن النظام يتماشى مع أهداف المؤسسة وسيروراتها، ويفي بالتزامات الأعمال، والالتزامات التنظيمية منذ البداية ؛
- السيرورة: هذه النسخة من المعيار، تعتمد على سيرورة التحسين المستمر بهدف تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المؤسسة ؛
- **الإدارة والحوكمة**: هذه النسخة من المعيار تأخذ المؤسسة من ناحية السياق لا من ناحية الطبيعة القانونية، وتصف الأدوار على المستوى الإداري ومستوى الإدارة العليا وتزيل مفهوم مجلس الإدارة ؛
- **تقييم المخاطر**: المخاطر تقييمها ومعالجتها يتماشى مع معيار إيزو 31000، الذي يعرف الخطر على أنه تأثير عدم اليقين على الأهداف سواء من ناحية إيجابية أو سلبية ؛
- **الضوابط**: من أجل إدارة المخاطر وتحقيق أهداف الأمن الخاصة بالمؤسس، هذا المعيار يتوفر على 114 ضابط مقسم على 14 صنف على عكس المعيار السابق الذي كان يتوفر على 133 ضابط مقسم على 11 صنف ؛
- **الملفات**: المعيار المنقح لا يميز بين الوثائق والسجلات من جهة، ومن جهة أخرى هذه الأخيرة تخضع لنفس متطلبات الرقابة، وذلك من أجل تبسيط الإجراءات الأمنية لكل منها؛
- **قياس الفعالية**: نظام إدارة أمن المعلومات وسيروراته وضوابطه يتم وفق متطلبات معينة، ويتم تم تحديد متطلبات قياس فعاليته من قبل المؤسسة .

3-4- مرجعية مراقبة أهداف وتكنولوجيا المعلومات النسخة الخامسة (Cobit5):

تعتبر هذه المرجعية أكثر توسعا في مجال أمن نظم المعلومات وأكثر وضوحا من المرجعية في نسختها الرابعة (Cobit4)، حيث تتميز بإعطاء توجهات حول المحركات الأساسية وحول المزايا

المتعلقة بأمن المعلومات، بالإضافة إلى ذلك هذه المرجعية تعمل على شرح كل بعد من الأبعاد الأساسية للنموذج من منظور أمن المعلومات.

أما فيما يخص المحركات الرئيسية التي أدت إلى تطوير هذه المرجعية فتتمثل في العناصر التالية (ISACA , 2012, P13):

- ضرورة وصف أمن المعلومات في سياق المؤسسة؛
- الحاجة المتزايدة للمؤسسة في:
  - الإبقاء على المخاطر عند مستويات مقبولة؛
  - الحفاظ على توافر المعلومات والخدمات ؛
  - الامتثال للقوانين واللوائح ذات الصلة؛
- الحاجة إلى الاتصال والمواءمة والاصطفاف مع المعايير والأطر الرئيسية الأخرى؛
- الحاجة إلى ربط جميع البحوث الرئيسية لجميع تدقيق ومراقبة نظم المعلومات مع الأطر والتوجيهات، حيث أن استخدام المرجعية من أجل أمن المعلومات يمكن أن يؤدي إلى تحقيق العدد من المزايا أهمها:
  - زيادة رضا المستخدمين عن ترتيبات ونتائج أمن المعلومات؛
  - تقليل التعقيد بسبب تحسن وسهولة دمج معايير أمن المعلومات؛
  - تحسين تكامل أمن المعلومات في المؤسسة ؛
  - اتخاذ قرارات مستنيرة بشأن المخاطر والوعي بها؛
  - تحسين الوقاية والكشف والتعافي من المخاطر والاعتداءات الالكترونية؛
  - تقليل تأثير الحوادث الأمنية ؛
  - تعزيز الدعم لتحسين الابتكار وتعزيز القدرة التنافسية ؛
  - تحسين إدارة التكاليف المتعلقة بوظيفة أمن المعلومات ؛
  - توفير فهم أفضل لأمن المعلومات.

4-4- مرجعية مكتبة البنية التحية لنظم المعلومات (ITIL V3):

تتضمن مرجعية البنية التحتية في إصدارها الثالث على خمسة مراحل أساسية تتمثل في إستراتيجية الخدمة، تصميم الخدمة، انتقال الخدمة، تشغيل الخدمة والتحسين المستمر للخدمة، هذه المرجعية تعالج وتتناول مسألة أمن المعلومات في مرحلتين أساسيتين من المراحل

السابقة هما: إستراتيجية الخدمة وبدرجة أقل مرحلة تصميم الخدمة، وذلك من خلال ما يعرف بسيرورة إدارة أمن المعلومات .

- مرحلة إستراتيجية الخدمة: تسمح هذه المرحلة بتحديد العناصر المتعلقة بأمن نظم المعلومات على النحو التالي (أوكسنر، 2011، ص 14):
  - تعريف الخطر المتعلقة بالحاسوب، وتعمل على تحديده عندما يكون هناك عدم يقين في نتائج نشاط معين ؛
  - ترجمة هذا الخطر عندما يتم تنفيذ مخطط استمرارية الأنشطة ومخطط تشغيل الأنشطة ؛
  - عرض المخاطر على أنها سيرورة من سيرورات المراقبة والتقييم.
- مرحلة تصميم الخدمة: تأخذ هذه المرحلة أمن نظم المعلومات من خلال سيرورتين، الأولى تتعلقة بإدارة التوافر التي تعطي مؤثرا على سلامة المعايير المتعلقة بأمن أنظمة المعلومات: السرية، السلامة والتوافر، وسيرورة إدارة أمن المعلومات التي تعمل على التعريف بمجموعة من التيمات المرتبطة بإدارة أمن المعلومات، حيث تتمثل هذه العناصر في النقاط التالية: الهدف أو الأهداف، النطاق، القيمة، المبادئ والسياسات، المفاهيم الأساسية، الأنشطة والأساليب والتقنيات، ومؤشرات الأداء الرئيسية (Rudd, 2007, P195).

الخاتمة:

نستخلص من خلال هذا البحث بأن بيئة المؤسسة أصبحت أكثر تعقيدا، نتيجة للتطورات والتغييرات الكبيرة المرتبطة بتكنولوجيا المعلومات، الأمر الذي حتم على أي مؤسسة مهما كان حجمها وطبيعتها العمل على تبني أحسن التكنولوجيات لمسايرة المؤسسات المنافسة و مواكبة مختلف التطورات التي تضمن لها الحفاظ على الاستقرار والاستمرارية في البيئة.

التنافس الشديد بين المؤسسات في تبني التكنولوجيا الجديدة واستعمالها في مختلف الوظائف والأنشطة الخاصة بالمؤسسة ساهم في ظهور العديد من الاعتداءات الالكترونية هدفها الأساسي الإضرار بسرية، توافر وسلامة المعلومات عن طريق مجموعة من الأساليب والأشكال، يكون فيها الفرد في الغالب المتسبب الأول في حدوث هذه الاعتداءات.

إن إهمال المؤسسة لهذه الاعتداءات، وعدم العمل على الوقاية منها، وعدم وجود ضوابط وإجراءات مناسبة، والاعتماد فقط على الحلول التكنولوجية التقنية من أجل حماية الأنظمة

المعلومات من خلال اعتماد التشفير الالكتروني والبرمجيات والتطبيقات والوسائل، أبقى على فرص كبيرة للمخترقين والمعتدين للإضرار بها وزيادة حجم الخسائر المالية، والإضرار بسمعتها وسرقة الأبحاث السرية لها وغيرها من الجوانب.

الأمر الذي يستدعى من هذه المؤسسة ضرورة تبني مقاربات جديدة تتمثل في حوكمة أمن نظم المعلومات، هذه الأخيرة تعمل على توفير ممارسات جيدة تضمن للمؤسسات بأن الاعتداءات الالكترونية التي تتعرض لها أنظمتها المعلوماتية يتم التحكم بها أو يتم الوصول بها إلى مستوى مقبول، كما تعمل وتأكد بأن الإستراتيجية الخاصة بأمن المعلومات التي تتبعها المؤسسة تساهم وتحقيق الأهداف الإستراتيجية لها، وتساهم في ضمان بقاءها استمراريتها.

وتتمثل الممارسات الجديدة حوكمة أمن المعلومات للحد أو تقبل الاعتداءات الالكترونية إلى مستوى مقبول، وتحقيق الأهداف الإستراتيجية المرتبة بأمن المعلومات في المؤسسة في مجموعة من المرجعيات والمعايير، أبرزها مرجعية مخاطر تكنولوجيا المعلومات IT Risk، معيار ISO 27001، مرجعية مراقبة أهداف تكنولوجيا في نسختها الخامسة COBIT5، ومكتبة البنية التحتية لتكنولوجيا المعلومات في نسختها الثالثة ITIL3.

ولعلى من بين أهم النتائج المتوصل إليها من خلال هذا البحث هو أن مختلف المرجعيات والمعايير المتعلقة بحوكمة أمن المعلومات، بأنها تساعد على تحقيق ما يلي:

- ضمان بأن التحكم المخاطر أو الصول بها إلى مستوى مقبول ؛
- ضمان سرية المعلومات وتوافرها وسلامتها ؛
- وضع سيرورة واضحة بأمن المعلومات واعتبارها وظيفة أساسية من وظائف المؤسسة
- خلق ثقافة أمنية لدى المستخدمين والمسؤولين في المؤسسة ؛
- تحسين إدارة التكاليف المرتبطة بأمن المعلومات ؛
- المحافظة على سمعة المؤسسة وزيادة ثقة أصحاب المصالح بها ؛
- الإبقاء على تركيز المؤسسة قدراتها الابتكارية وتعزيز وتحسين ميزتها التنافسية .

قائمة المراجع

I.المراجع باللغة العربية:

- **الكتب:**

1- إيمان فاضل السامرائي و وأخرون، **مصادر المعلومات التقليدية والالكترونية**، دار اليازوري، الأردن، عمان، 2009.

2- حميد ناصر الفتال ودليل صادق، **أمن المعلومات**، دار اليازوري ، الأردن، عمان ، 2008.

3- يورغ أوكسنر،**أفضل إطارعملي وقياس فعلي عالمي، مكتبة البنية التحتية لنظم المعلومات**، ترجمة أبوستروف ش م، الإصدار 3، سويسرا 2011.

4- نضال إسماعيل برهم ،**أحكام عقود التجارة الالكترونية**، دار الثقافة النشر والتوزيع، عمان، الأردن، 2005، ص 84 .

➢ **المجلات:**

1- علي خليل، منى إبراهيم، **الدور التأثيري لحوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية**، مجلة جامعة بنها، مصر، 2013.

➢ **الرسائل الجامعية:**

1- حنان كريبط، **الثقافة التنظيمية كمحدد لنجاح تطبيق الإدارة الالكترونية – دراسة حالة إدارة عمومية**، أطروحة دكتوراه في علوم التسيير، جامعة الجزائر 03، 2018.

2- نوفيل حديد، **تكنولوجيا الانترنت وتأهيل المؤسسة للاندماج في الاقتصاد العالمي**، دكتوراه في العلوم الاقتصادية وعلوم التسيير، جامعة الجزائر3، 2007.

II.المراجع باللغة الأجنبية:

➢ **الكتب:**

1- International Standard, **Information technology-Security techniques-Information security management systems -Overview and vocabulary**, ISO/IEC 27000, First edition, 2009.
2- A .Taylor &al., **Information Security Management Principles An ISEB Certificate**, edition British Computer Society, 2008.
3- S. G. Hélie, **Sécurité informatique et réseaux,** Dunod, Paris, 2008.
4- E. Gelbstein& A. Kamal, Information Insecurity: A survival guide to the uncharted territories of cyber-threats and cyber-security, United Nations ICT Task Force and the United Nations Institute for Training and Research, New York, USA, 2002.
5- ISACA, The risk IT Framework, USA,2009.
6- C.Rudd & V. Lloyd, **ITIL :Service-Design**, OGC official product, USA, 2007.
7- Linkov I. & Kott A., **Fundamental Concepts of Cyber Resilience: Introduction and Overview**, Springer, 2018.

➢ **المقالات:**

1- A .Raman &al.**, Cybersecurity in higher education: the changing threat landscape,** journal Performance, Vol8, N° 3, August 2016.

2- A. Singh et al., Information Security: Components and Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4, n° 1, January 2014.
3- G .Urbina&al.**, Hacking interdit : Toutes les techniques des hackers enfin décryptées pour ne plus jamais vous laisser piéger !**, Micro application, Paris,2006.

➢ **الرسائل الجامعية:**

1- M .Luesebrink, **The Institutionalization of information security governance structures in academic institutions: A case study**, doctorate on Philosophy, Florida state university, USA, 2011.

➢ **التقاريروالقواميس:**

1- Committee on National Security Systems, **National Information Assurance (IA) Glossary**, CNSS Instruction No. 4009, 26 April 2010.
2- R .Kissel, **Glossary of Key Information Security Terms**, National Institute of Standards and Technology, USA, 2013.
3- 3Com Corporation, **Network Security: A Simple Guide to Firewalls**, Massachusetts, USA, 2000.
4- KASEYA CORPORATION, **AntiMalware**, User Guide, 09/2013.
5- Islam E. & Christoforides C., **Fundamentals of cybersecurity and the Cyber Resilience Oversight Expectations**, European Central Bank, 2019.
6- IT Governance Institute, **Information Security Governance: Guidance for Boards of Directors and Executive Management**, 2nd Edition, USA, 2006.
7- ISACA , **Risk-IT-Brochure: Risk IT A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk**, USA, 2012.
8- **ISACA, Cobit5 :** A Business Framework for the Governance and Management Of Enterprise IT, 2012.

➢ **المو اقع الالكترونية**

1- https://www.visualcapitalist.com/hakers-hack-motives-behind-cyberattacks/consulted: 27/01/2019
2- https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business/consulted: 10/2022.
3- Nappo, https://www.goodreads.com/quotes/10043276-one-of-the-main-cyber-risks-is-to-think-they-don-t, consulted: 04/2020.
4- [1]https://www.goodreads.com/author/quotes/175417.bruce_schneier ?page=3. Consulted : 30/01/2019.
5- https://www.cyber-arabs.com/?p=10115 consulté le : 10/2020

6- https://technet.microsoft.com/en-us/library/8c270506-79bd-41e9-8d96-8a9fc81d9e09 consulted: 04/10/2022
7- https://www.ietf.org/rfc/ consulted: 12/2019.
8- http://web.mit.edu/kerberos consulted: 26/05/2022.
9- https://www.azquotes.com/author/10219-Kevin_Mitnickconsulted: 10/2022.
10- **Comparing ISO 27001:2005 to ISO 27001:2013**, October 2013, Available on: www.itgovernance.co.uk, Consulted 12/2021.