

التقنيات الرقمية الجديدة في إدارة مخاطر المنظمات الاقتصادية الذكية

New Digital Technologies in Managing The Risks of Smart Economic Organizations

تاريخ الاستلام: 2022-09-13 تاريخ قبول النشر: 2022-10-12

منصوري هوارى^{*}، جامعة أحمد دراية أدرار (الجزائر)،
Sayah.2013@yahoo.fr

Abstract:

This research paper aims to shed light on one of the challenges posed by the current global economic system and represented in those risks resulting from the extensive use of information technology and networks and its various applications, As much as What this technology has become an essential and dynamic asset within modern business organizations, As much as What has become Its unsafe use poses a real threat and a major challenge to the security of its information systems and the integrity of its personal identity.

To delve In the details of this topic you ask us Adopting the descriptive analytical approach as the most reliable curriculum in the field of humanities and social sciences In order to display and list some theoretical concepts and to analyze some data and statistics, As for the results reached In this study It consisted in identifying the various types of information systems and networks risks that have come to haunt smart business organizations As a result of the unsafe use of its information systems and networks As well as knowing its various sources and the factors that cause it, After that, the most important modern strategies used to contain these risks and reduce their severity are presented.

Keywords: Information Technology, Networks, Information Security, Smart Organization, (ISO27001).

JEL Classification Codes: D83, M13.

* - المؤلف المراسل

ملخص:

تهدف هذه الورقة البحثية إلى تسليط الضوء على إحدى التحديات التي أفرزتها المنظومة الاقتصادية العالمية الراهنة والمتمثلة في تلك المخاطر الناتجة عن الاستعمال المكثف لتكنولوجيا المعلومات والشبكات وتطبيقاتها المختلفة، فبقدر ما أصبحت هذه التكنولوجيا تشكل عنصرا أساسيا وأصلا ديناميكيا داخل منظمات الأعمال الحديثة، فبقدر ما أصبح يشكل الاستعمال غير الآمن لها خطرا حقيقيا وتحديا كبيرا على أمن أنظمتها المعلوماتية و سلامة هويتها الشخصية.

إن الخوض في تفاصيل هذا الموضوع تطلب منا اعتماد المنهج الوصفي التحليلي باعتباره المنهج الأكثر اعتمادا في ميدان العلوم الإنسانية والاجتماعية وذلك لعرض وسرد بعض المفاهيم النظرية وتحليل بعض البيانات والإحصائيات، أما النتائج التي تم التوصل إليها في هذه الدراسة تمثلت في تحديد مختلف أنواع مخاطر نظم المعلومات والشبكات التي أصبحت تلاحق منظمات الأعمال الذكية نتيجة الاستعمال غير الآمن لأنظمتها وشبكات المعلوماتية وكذلك معرفة مختلف مصادرها والعوامل المسببة لها، ليتم على إثرها عرض أهم الاستراتيجيات الحديثة المتبعة في احتواء هذه المخاطر والتقليل من درجة خطورتها.

الكلمات المفتاحية: تكنولوجيا المعلومات، الشبكات، أمن المعلومات، المنظمة الذكية (ISO27001).

تصنيف JEL: D83, M13.

1. مقدمة:

شهد العالم خلال السنوات الأخيرة نموا سريعا لتكنولوجيا المعلومات والشبكات وابتكارات واسعة ومكثفة لمجالات استخداماتها وتطبيقاتها، واكتسبت أهمية متزايدة على نحو مطرد أصبحت تشكل فيه أصلا من الأصول الديناميكية والاستراتيجية التي لا غنى عنها لأي منظمة من منظمات الأعمال في سعيها إلى تحقيق أهدافها ورسالتها، وأصبح العالم بفضلها أكثر اتصالا وترابطا والأحداث غير المتوقعة أوسع احتمالا وانتشارا والهجوم على البنى التحتية والشبكات والأنظمة أكثر تعقيدا وخطورة.

إذا كان لهذه التكنولوجيا ما يؤهلها لأن تحظى بمكانة بارزة وأهمية قصوى وغير مسبوقة في مختلف مجالات حياتنا اليومية عامة وفي منظمات الأعمال على اختلاف أنواعها وأشكالها خاصة، فإنه بالمقابل كذلك أصبحت تتطوي على العديد من التهديدات والمخاطر الناتجة عن الاستخدام غير النزيه والوصول غير المشروع والاطلاع غير المبرر على معلومات وبيانات تتميز بالسرية والخصوصية داخل هيئات ومنظمات حساسة واستراتيجية توصي القوانين بعدم السماح للجميع الاطلاع على مضمونها ومحتواها.

أ- إشكالية الدراسة: تتمحور مشكلة الدراسة حول تشخيص مخاطر استخدام نظم المعلومات في المنظمات الحديثة (الرقمية) وما هي مسببات هذه المخاطر وأهم أنواعها وسبل الوقاية منها، من خلال طرح التساؤل: في ظل انتشار تكنولوجيا المعلومات ما هي الاستراتيجيات الواجب إتباعها لإدارة مخاطر نظم المعلومات في المنظمات الذكية؟ ب- فرضية الدراسة: ينطلق البحث في صياغة فرضيته من تساؤله المطروح واتساقاً مع أهدافه بموجب فرضية رئيسية نحاول صياغتها على النحو التالي:

- يعتبر الاستعمال المكثف وغير الآمن لوسائل تكنولوجيا المعلومات والشبكات وتطبيقاتها الحديثة مصدر تهديد وخطر على أمن واستقرار منظمات الأعمال الحديثة التي تنشط في ظل بيئة الأعمال الرقمية.

ج- أهمية الدراسة: تنبثق أهمية هذه الدراسة من حداثة وخصوصية الموضوع الذي تناولته وهو رصد مختلف مخاطر تكنولوجيا المعلومات والشبكات وسبل مواجهتها في المنظمات الذكية التي تعتمد تقنيات ونظم المعلومات بشكل واسع ومكثف، وكذا تناوله المحدود في أدبيات الدراسات التي تطرقت إلى إدارة مخاطر تكنولوجيا المعلومات.

الدراسات السابقة: تنوعت الدراسات التي عالجت موضوع مخاطر نظم المعلومات ومن زوايا مختلفة، فمنها الكتب، المجلات، التقارير الصادرة عن بعض الهيئات الإقليمية والدولية، ونظرا لوفرة هذه الدراسات فمن غير الممكن التطرق إليها كلها، وسوف تقتصر هذه الدراسة على ذكر بعض الدراسات ذات الصلة الأكبر بالموضوع ليتسنى لنا ربط ما يتم التوصل إليه من نتائج وتوصيات بالدراسات السابقة ومن أهم هذه الدراسات علاقة نذكر:

دراسة (العتيبي، 2010): بعنوان الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والعالمية: هدفت للتعرف على مدى توافق الأمن المعلوماتي للمواقع الالكترونية للأجهزة الأمنية والمدنية بالرياض مع المعايير المحلية والدولية وتوصلت الدراسة لوجود درجة توافق استراتيجيات الأمن المعلوماتي في المواقع الالكترونية للقطاع المدني والأمني مع المعايير المحلية والدولية متوسطة، ووجود درجة توافق تقنيات الأمن المعلوماتي وبيئة الأمن المعلوماتي للعنصر البشري في المواقع الالكترونية للقطاعين مع المعايير المحلية والدولية مرتفعة (العتيبي، 2010، الصفحات 1-213).

دراسة (عرفان نبي وآخرون، 2010) بعنوان دراسة عملية حول أمن المعلومات في المنظمات السعودية، هدفت إلى استكشاف حالة أمن المعلومات والعمل على تحقيق فهم أفضل للحقائق السائدة داخل المملكة العربية السعودية، وتوصلت لوجود أهمية سياسة أمن المعلومات في ضمان اتخاذ عوامل تحكم مناسبة وبينت الدراسة أن أكثر من نصف المنظمات يمتلك سياسة أمن المعلومات وغالبيتها يميل إلى تطبيقها واعتبار التحكم في الوصول إلى الشبكة Acces Control أمرا حاسما لأمن المعلومات، كما تتسم معالجة

قضايا أمن المعلومات بالتمييز بين حساسية المعلومات، وافترضت عدم المساواة في التعامل مع هذه المعلومات فليس كل المعلومات لها نفس القدر من الأهمية (الغنبر، 2008، الصفحات 1-53).

دراسة (البحيصي، 2008)، بعنوان مخاطر نظم المعلومات المحاسبية الالكترونية، دراسة تطبيقية على المصارف العاملة في قطاع غزة، هدفت الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، وأهم الأسباب التي تؤدي إلى حدوث تلك المخاطر وتوصلت الدراسة إلى عدم حدوث مخاطر نظم المعلومات المحاسبية الالكترونية في المصارف بقطاع غزة بشكل متكرر، يرجع حدوث بعض مخاطر نظم المعلومات المحاسبية الالكترونية لأسباب تتعلق بموظفي البنك نتيجة قلة الخبرة والكفاءة (الشريف، 2008، الصفحات 895-923). دراسة (تايه، 2008) بعنوان مدى فعالية إدارة أمن المعلومات في الشركات تكنولوجيا المعلومات في فلسطين، هدفت إلى التعرف على مدي فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين واعتمدت الدراسة على معيار ISO 17799 ومجالاته العشرة الخاصة بقياس مدى جودة نظم أمن المعلومات، توصلت إلى أن فعالية إدارة أمن النظم تتحقق بمقدار توفر سياسة أمن المعلومات، الأمن التنظيمي لا يؤثر على كفاءة وفعالية إدارة أمن نظم المعلومات وأرجعته الدراسة إلى عدم وجود آلية مراجعة دورية نظامية لسياسة أمن المعلومات (تايه، 2008، الصفحات 1-195).

دراسة (الفحطاني، 2008) بعنوان مهددات الأمن المعلوماتي وسبل مواجهته، هدفت إلى التعرف على مهددات الأمن المعلوماتي وسبل مواجهتها في ضوء تزايد معدلات الاختراقات والحاجة لاتخاذ وسائل حماية للبيانات والمعلومات، توصلت إلى أن الاتصال المباشر بشبكة الانترنت وإساءة الاتصالات وإساءة الاتصال الداخلي بين الأفرع تعتبر مصادر تهديد متوسطة الدرجة، استخدام الفيروسات في إتلاف المعلومات وتغيير

البيانات وسرقة المعلومات هي أشكال التهديدات المحتملة للأمن المعلوماتي بدرجة متوسطة، استقطاب خبراء حماية نظم المعلومات وتزويد المراكز بالتقنيات المتطورة واستخدام مكافحة الفيروسات هي أهم السبل بدرجة كبيرة لتطوير قدرات المراكز (القحطاني، 2008، الصفحات 1-229).

بعد عرض الدراسات السابقة والتي تتقاطع مع موضوع الدراسة الحالية، وبعد عرض أهدافها ونتائجها، يمكن القول أن ما يميز دراستنا هذه عنها هو تركيزها على عرض مفهوم المنظمات الحديثة (الرقمية) وتحديد مختلف المخاطر التي تتعرض لها في ظل البيئة الرقمية التي تنشط فيها وأهم الاستراتيجيات التي يتم الاعتماد عليها في مواجهة هذه المخاطر.

2. منظمة الأعمال الذكية:

يشير مفهوم الذكاء في المنظمات إلى المدخل الإداري والتكنولوجي الذي يطبق في مواجهة التحديات الداخلية والخارجية لتطوير أداء المنظمة، وبالتالي فإن مفهوم الذكاء يرتبط بشكل واضح بمفهوم إدارة المعرفة، فالذكاء إذن هو القدرة على نقل المعرفة والمهارة واليقظة واستخدامها وتوظيفها من طرف المنظمة حينما تبرز تحديات ومستجدات جديدة.

1.2 تعريف المنظمة الذكية: هي نوع جديد من المنظمات بدأ بالظهور في ظل اقتصاد المعرفة، تمثل الأصول غير المادية والمنتجات غير الملموسة المكون الأساسي لهذه المنظمات (Pilamunga Poveda, 2019, p. 2).

وعرفت بأنها عملية اشتراك المعرفة والمهارة في كل الأصول الملموسة وغير الملموسة التي تتوفر في عملية حل المشاكل واتخاذ قرار داخل المنظمة" (آخرون، 2013، صفحة 133).

وعرفت بأنها المنظمات التي حدث فيها تحول من التركيز على الأصول المادية إلى التركيز على رأس المال الفكري، وأن منظمة الأعمال التي لديها أفكار كثيرة لديها فرصة

كبيرة للنجاح والنمو بسرعة وإن الأصول الفكرية حلت محل الأصول المادية (صالح، 2009، صفحة 172).

الشكل 1: المنظمة الذكية



المصدر: (محمد، 2005، صفحة 40)

2.2 خصائص بيئة المنظمة الذكية: تتميز المنظمات المسيرة رقميا بما يلي (العبادي، 2012، صفحة 265):

1.2.2 العولمة: المنظمة الذكية الحديثة بمثابة منظمة دولية، ففي نطاق العولمة يصبح من الضروري أن يوجد للمنظمة الذكية مهما كان حجمها ونوع نشاطها توجه عالمي نحو التجارة الالكترونية وتقليص الحدود والحد من المعوقات التي تعوق تدفق المعلومات منها وإليها، وفي الوقت الحالي يتطلع المنتجين المحليين إلى أن يكون لهم تواجد خارج الحدود الوطنية أو المحلية ويحصلوا على حصة من سوق تصدير منتجاتهم وخدماتهم من خلال المنافسة عبر العالم المفتوح.

2.2.2 المنافسة: أصبحت كل منظمة سواء كانت كبيرة أو صغيرة إنتاجية أو خدمائية تواجه منافسين لها على كافة المستويات المحلية الوطنية والدولية ومن الواضح أن العولمة أدت إلى زيادة المنافسة، كما أن تكنولوجيا المعلومات والشبكات المتقدمة تعتبر من أسباب نمو المنافسة فهي تساعد على تحقيق أسعار أقل وجود أعلى واكتشاف أسواق جديدة، كما تسمح أيضا بتطبيق وسائل إبداعية ومبتكرة للوصول إلى العملاء وتقديم ما يطلبونه تحقيقا لرضاهم.

3.2.2 المعلومات كمورد رئيسي واستراتيجي: أصبح المعلومات أهمية

عظمى ودور بارز في بيئة الأعمال المعاصرة ومن الواضح أن المعرفة تمثل مفتاح الميزة التنافسية، فمعرفة العملاء والموردين والمنافسين والحصول على معلومات دقيقة وصحيحة وفورية عنهم يؤدي إلى نجاح المنظمة وتطورها.

3.2 متطلبات التحول إلى المنظمات الذكية: تسعى منظمات الأعمال حاليا

إلى ولوج عالم الرقمنة وتطوير أعمالها من شكلها التقليدي إلى الشكل الذي تعتمد فيه على وسائل تكنولوجيا المعلومات والشبكات بشكل كبير، وهو أمر يحتاج بدوره إلى إمكانيات ومتطلبات ينبغي توفيرها للقيام بعملية التحول الرقمي ومن متطلبات التحول الرقمي ما يلي:

1.3.2 القيادة الالكترونية: قيام القائد بمهمة الاتصالات بما يتيح له مناخ يوفر

إيصال رسائله، وقيامه بمسؤولية التحفيز المباشر، في ظل التحول للمنظمات الذكية شهد دور القيادة تغير من خلال النقاط التالية:

- توفير الاتصال المستمر بين القادة والمروّسين من خلال الشبكات الداخلية والخارجية؛
- زيادة القدرة على ابتكار وجلب خدمات ومنتجات وأساليب جديدة؛

- زيادة المرونة في التغير والتكيف مع البيئة المتغيرة (شديد، 2021، صفحة 204).

2.3.2 أمن المعلومات: الوثوق في معالجة وتخزين المعلومات يرتبط بمستوى امن

وخصوصية وسرية المعلومات المتوفرة والمتدفقة التي ينبع منها مدى الثقة فيها والاعتماد عليها وتشمل عناصر وخواص امن المعلومات على ما يلي:

- تقوية الحماية القانونية لحقوق الملكية الفكرية المرتبطة بإبداعات المنظمة الرقمية (شحاتة، 2020، صفحة 16)؛

- سن تشريعات التي تحمي خصوصية وسرية المعلومات للمنظمات والأفراد على حد سواء (إكرام، 2019، صفحة 49)؛

-فرض عقوبات جنائية على جرائم الكمبيوتر والاتصالات والتوقيع الإلكتروني والنشر الإلكتروني.

3.3.2 رأس المال الفكري: لقد بات من المتعارف عليه أن لرأس المال الفكري دور كبير في منظمات الأعمال في الاقتصاديات الحديثة لاسيما منذ بداية عقد التسعينيات من القرن الماضي؛ حيث لا يمكن لأية منظمة في أي قطاع كان وبأي حجم كانت أن تحقق الميزة التنافسية من دونة بعد أن كانت المصادر المادية تعد الثروة الحقيقية للمنظمات، لذا صار الرأس المال غير المادي (الفكري) نقطة الارتكاز الأساسية لكل الاستراتيجيات الحديثة في إدارة وتسيير المنظمات.

4.3.2 مناخ الأعمال: تعمل المنظمة الذكية في سياق معقد من السياسات والتشريعات والقوانين التي تضع قواعد التصرفات والمعاملات الخاصة بها في سوق التنافسية المفتوحة والممتدة، وكلما زاد تشجيع ومزاوالات المنظمة الذكية ارتفع العائد على الاستثمار والعكس صحيح، ومن أهم العناصر المدعمة لتهيئة مناخ المنظمة الذكية نذكر ما يلي:

-شفافية وإمكانية التبؤ بالتنفيذ الفعلي للمنظمة الذكية والانفتاح الحكومي عليها وتحديد مخاطر القوانين والتشريعات التي تعمل في ظلها بالإضافة إلى دعم الاستقرار السياسي لها والمحيط المتواجدة فيه (العوفي، 2020، صفحة 9)؛

-تأكيد قدرات المنظمة المالية لمساندة التصرفات والأفعال الخاصة بالأداء الرقمي (مكي، 2021، صفحة 21).

3. نظم المعلومات:

1.3 مفهوم النظام: وجدت النظم قبل وجود الإنسان ذاته إلا أن استخدامها في مجال العلوم لم يتم إلا منذ عام 1937، كان أول استخدام لهذا المفهوم في مجال العلوم الطبيعية وبصفة خاصة علم الأحياء، ثم انتقل إلى العلوم الاجتماعية، حظي هذا

المفهوم باهتمام عديد الكتاب والباحثين في الآونة الأخيرة، ومن أهم التعاريف التي حظي بها نجد:

1.1.3 تعريف النظام: عرف بأنه مجموعة من العناصر أو المكونات المرتبطة والمتفاعلة مع بعضها البعض والتي تعمل معا ضمن بيئة معينة لتحقيق هدف محدد، وتشمل هذه المكونات الموارد، الأجهزة، الخبرات، الأفراد، الأموال... الخ، وكل ما يحتاج إليه النظام من تسهيلات (Djenane Abdelhak, 2012, pp. 6-7).

كما عرف بأنه مجموعة من الأجزاء التي تتفاعل وتتكامل مع بعضها البعض ومع بيئتها لتحقيق هدف أو أهداف محددة (Noureddine Myriam, 2018, p. 298). وعرف بأنه مجموعة عناصر ذات علاقة متبادلة والتي تسعى إلى تحقيق هدف معين (الشرمان، 2004، صفحة 44).

2.1.3 عناصر النظام: يتكون النظام من العناصر التالية:

المدخلات: تمثل الموارد اللازمة للنظام لكي يتمكن من القيام بالأنشطة اللازمة لتحقيق أهدافه، وتشمل المدخلات عديد العناصر كالمخامات والطاقة والمعلومات والآلات، يلاحظ أن هذه المدخلات غير متجانسة وهي تمثل مخرجات لنظم أخرى.

المخرجات: منتجات النظام أو مخرجات الأنشطة والعمليات التحويلية ويقدم النظام المخرجات للمستفيدين على شكل منتجات جاهزة للاستخدام مثل السلع النهائية أو المعلومات المفيدة أو الخدمات المطلوبة والتي بدورها تشبع حاجيات ورغبات المستفيد وتحقق أهداف المؤسسة (بروبة، 2021، صفحة 372).

التغذية العكسية: وهي التغذية الراجعة أو تأثير البيئة الخارجية على النظام، والتي تحدد مدى ملائمة وصلاحيّة النظام وكفائته في تحقيق الأهداف المطلوبة وتلبية الحاجات للمستفيدين من خلال تمرير الملاحظات عن أي قصور أو عيب في تطبيق النظام ليتم إصلاحها وتفاذي تكرارها مستقبلا، الشكل الموالي يبين طبيعة عمل العناصر السابقة:

الشكل 2: عناصر (مكونات) النظام



المصدر: (اللطيف، 2004، صفحة 43)

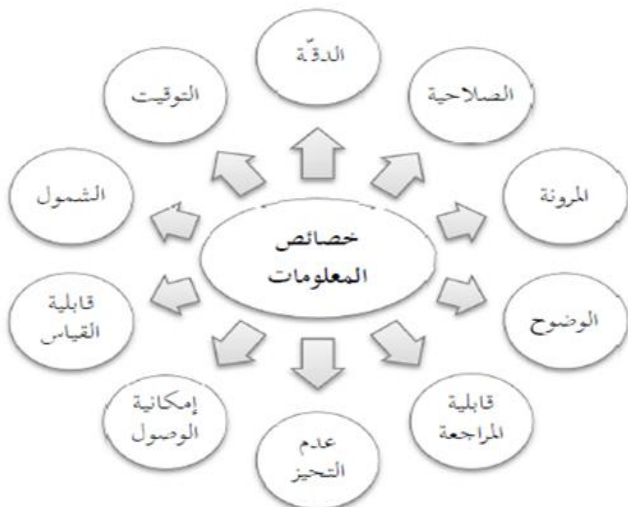
2.3 مفهوم المعلومات: أصبح للمعلومات دور مهم في نواحي الحياة، خاصة العلمية، تعتمد عليها عمليات اتخاذ القرارات، فكلما كانت هذه المعلومات صحيحة ودقيقة فالقرارات المعتمدة عليها تكون على درجة عالية من الصحة والدقة.

1.2.3 تعريف المعلومات: عرفت بأنها البيانات التي أجريت عليها معالجة معينة وذلك بترتيبها وتنظيمها وتحليلها بغرض الاستفادة منها والحصول على نتائج معينة من خلال استخدامها (Lamaria, 2020, pp. 739-740).

2.2.3 خصائص المعلومات: تحتاج المؤسسات إلى كم هائل من المعلومات للقيام بأعمالها المتعددة، ويجب أن تتميز هذه المعلومات بخصائص ومميزات معينة تجعلها مفيدة وموثوقة تساهم في اتخاذ القرارات الصحيحة، وحتى تتصف هذه المعلومات بالجيدة يجب أن تتوفر فيها العناصر التالية:

- الواقعية: بمعنى أن المعلومات تدور حول الموضوع وذات علاقة منطقية ووثيقة؛
- الدقة: وتكون في إجراءات القياس المستخدمة في إعداد المعلومات وتشغيلها وتجهيزها وتلخيصها وعرضها؛
- الوضوح: يجب أن تكون المعلومات خالية من الغموض ومفهومة بشكل كبير لمستخدميها؛
- الشمولية: يعني احتواء المعلومات على الحقائق الأساسية لاتخاذ القرارات اللازمة (كمال، 2019، صفحة 80).

الشكل 3: خصائص المعلومات الجيدة



المصدر: إعداد الباحث بناء على الدراسات السابقة

3.2.3 أنواع المعلومات: لقد أخذت المعلومات في السنوات الأخيرة بعدا استراتيجيا وذلك لتنمashi والتطور السريع وخاصة التكنولوجيا منه، فأصبح لزاما على أي منظمة استيعاب أكبر كمية من المعلومات حتى تستطيع البقاء والمنافسة (نينو، 2007، صفحة 61)، ومن أهم أنواع مصادر هذه المعلومات نذكر التالي:

أ- معيار الجهة مصدر المعلومة: قد تكون

معلومات داخلية: تتمثل في المعلومة الخاصة بنشاط المنظمة المتولدة عن العمليات التي تقوم بها مثل رقم الأعمال، كمية الإنتاج، التكاليف، الأفراد.

معلومات خارجية: هي معلومات تأتي من خارج المنظمة وتكون متعلقة بالمحيط مثل معلومات حول الزبائن، الموردين، المنافسين، القوانين.

ب- معيار الموثوقية: قد تكون

معلومات رسمية: تشكل المعلومات الرسمية الجزء الأكبر من المعلومات المتداولة في المنظمة فهي محددة من قبل الإدارة وتتمتع بمميزات أهمها: مؤرخة وتتبع قنوات أو طرق محددة مسبقاً.

معلومات غير رسمية: وهي عكس الرسمية من خصائصها أنها غير محدودة وغير معروفة المصدر، وتعتبر الإشاعات من بين هذا النوع من المعلومات.

3.3 نظم المعلومات

1.3.3 تعريف نظام المعلومات: مجموع الوسائل، الأدوات التي تسمح بجمع، تخزين وتحليل البيانات لاتخاذ قرار إشباع المتطلبات التنظيمية وحفظ ذاكرة المؤسسة بما يسمح لها بإعادة بناء ذاتها (الشكري، 2016، صفحة 182).

وعرف بأنه أسلوب رسمي يستخدم لتوفير المعلومات الدقيقة والموثوقة للإدارة، لتسهيل اتخاذ القرارات والتي تمكن المديرين من القيام بوظائف التخطيط والتشغيل والرقابة لتتمكن من تحقيق أهدافها بفاعلية (Sihem, 2015, p. 54).

2.3.3 أهداف نظام المعلومات: يحقق نظام المعلومات أهداف منها:

تحقيق الكفاءة: تشير الكفاءة إلى أداء المهام بأكبر سرعة أقل تكلفة، كتقليل تكاليف العمالة من خلال إحلال الحاسب الآلي محل الإنسان (Djamil, 2020, p. 3).

الفعالية: تشير الفعالية إلى مدى تحقيق أهداف المؤسسة وتحقيق الفعالية من خلال مساعدة المديرين في اتخاذ قرارات ذات جودة أفضل (حسن، 2015، صفحة 289).

تطوير المنتج: تلعب المعلومات دوراً هاماً في خلق وتطوير المنتجات الخاصة في بعض الصناعات مثل البنوك، التأمين والسياحة (نقاز، 2019، صفحة 118).

3.3.3 وظائف نظام المعلومات: يقوم نظام المعلومات خلال معالجته للمعلومات

بوظائف مختلفة نذكر منها:

جمع البيانات: تجمع البيانات من مختلف مصادر الداخلية والخارجية التي تدخل في صورتها الأولية ثم يتم تحويلها إلى قسم المعالجة (قايد، 2019، صفحة 378).

أمن البيانات: يعني استعمال مختلف وسائل الرقابة والأمان لتفادي الأخطاء عند إدخال البيانات أو لتفادي التلاعب أو ضياع المعلومات.

إيصال المعلومات: هي الوظيفة النهائية التي تمثل إنتاج التقارير وتوصيلها إلى مستخدميها في صورة مفهومة ومفيدة (Mohamed, 2007, p. 82).

4. مخاطر نظم المعلومات: في ظل البيئة الرقمية لم تعد هناك أي منظمة آمنة من مخاطر تكنولوجيا المعلومات، فكل منظمة يوجد بها نقاط ضعف قابلة للإصابة بالمخاطر، والمطلوب من إدارة المخاطر المعلوماتية تحديد هذه التهديدات وتقييم الضرر الناتج عنها والأخذ بالإجراءات لمنع حدوثها والتقليل من أثارها (خياط، 2019، صفحة 336).

1.4 تعريف مخاطر نظم المعلومات: تتجه عديد الشركات للاعتماد على تكنولوجيا المعلومات والشبكات من خلال نظم معلومات متكاملة، والتي تؤدي إلى دقة وسرعة تشغيل العمليات مما ينتج عنه تحقيق عديد المزايا التنافسية للشركات.

-تعرف مخاطر تكنولوجيا المعلومات والشبكات بصفة عامة على أنها " كل ما ينتج عنه وجود خطأ أو خلل في تكنولوجيا المعلومات يؤدي إلى تأثير سلبي على أعمال المنظمة (الرزاق) (2017, p. 111).

تعريف جمعية مراجعة ومراقبة نظم المعلومات ISACA لمخاطر نظم المعلومات: احتمال حدوث تصرف أو حدث ما له تأثير سلبي على المنظمة وعلى نظم معلوماتها (عطية، 2018، صفحة 139).

2.4 خصائص مخاطر نظم المعلومات: لمخاطر نظم المعلومات سمات تميزها عن غيرها من المخاطر، وتكمن خطورتها في ضعف إيجاد الصلة بين المجرم ووسيلة

ارتكابه للجريمة وصعوبة التعرف على شخصيته وبعده أحيانا عن موقع ارتكاب الجريمة، وعلى العموم يمكن تلخيص أهم خصائص المخاطر المعلوماتية أو المخاطر التكنولوجية فيما يلي:

1.2.4 الصعوبة في كشفها: تعني الصعوبة في اكتشاف أن هناك جريمة وقعت بغض النظر عن مرتكبها، فقد تقع جرائم معلوماتية ولا يشعر بها أحد بأن هناك جريمة وقعت إلا بعد مرور وقت طويل، وربما لا تكتشف نهائيا والسبب يعود إلى طبيعتها، حيث تقع في بيئة افتراضية غير ملموسة في غالب الأحيان ولا يمكن استشعارها بشكل مادي ملموس.

2.2.4 صعوبة إثباتها: تعني الصعوبة في إثبات وقوع الجريمة بعد اكتشافها أو الصعوبة في إثبات التنفيذ، فبعد اكتشاف الجريمة والعلم بوقوعها هناك صعوبة في إثبات أحداثها، والسبب في ذلك هو أن هذا النوع من الجرائم غالبا ما يتم تنفيذه بطرق مركزية صعبة ومهارات تخصصية عالية ويتم في الوقت نفسه إخفاء أو مسح أي آثار قد يتركها الجاني.

3.2.4 لا تحتاج إلى أدوات وأنشطة غير مألوفة: كل ما يحتاج إليه مرتكب الجرائم المعلوماتية هو جهاز حاسب آلي واتصال بشبكة الانترنت، فلا تجده يحتاج لأدوات تثير الانتباه كالسلاح مثلا بل يمكنه أن يرتكب الجريمة وهو يعمل على جهازه كما لو كان يؤدي عملا من الأعمال العادية وأيضا لا يحتاج إلى القيام بأنشطة تثير الشكوك.

3.4 مصادر مخاطر نظم المعلومات:

1.3.4 المخاطر الطبيعية: هي الكوارث الطبيعية التي ليس للإنسان أو التجهيزات الفنية دخل في حدوثها، كالزلازل والبراكين والفيضانات، وقد تلحق مثل هذه الكوارث أضرارا بأنظمة المعلومات، وتؤدي لانقطاع الخدمات الالكترونية حال إصابة المراكز

الرئيسية لتقديم تلك الخدمات وتعتبر مخاطر خارجية التي لا تتنبأ بها المنظمات (أمنية ,
(2016, p. 168).

2.3.4 المخاطر البشرية: المخاطر الناجمة عن العنصر البشري، فقد يتسبب
عمداً أو عن طريق الخطأ في الضرر أو الوصول إلى معلومات والاطلاع عليها دون
أن يكون له صلاحية ذلك وتزداد الخطورة عندما يكون لدى هذا العنصر صلاحية
الدخول إلى أنظمة المعلومات لما يكون أحد موظفي المنظمة، تتمثل مصادر المخاطر
البشرية فيما يلي:

-موظف المنظمة الفاسد؛

-موردو الأجهزة والبرامج؛

-المهندسون والمبرمجون وفنيو الصيانة والدعم الفني (الجبلي، 2019، صفحة 12).

3.3.4 المخاطر الفنية: مخاطر ناجمة عن القصور والأخطاء الفنية في أنظمة
أمن المعلومات، التي يغلب عليها الطابع الفني دون أي تدخل للعنصر البشري أو أن
تكون بسبب كارثة طبيعية ومنها (ذكاء، 2018، الصفحات 37-38):

4.3.4 مخاطر عيوب التصميم والتشغيل: تشمل عيوب التصميم في الأجهزة
والبرامج، أو مكون من الأنظمة المعلوماتية، تبرز أهمية تصميم البنية التحتية لتقنية
المعلومات وأمن المعلومات كالبنية التحتية لخوارزميات التشفير.

5.3.4 مخاطر تشتت المعلومات: إذا كانت معلومات المنظمة مشتتة ومخزنة
في أماكن فإن التشتت يحتم تطبيق أنظمة أمن معلومات متعددة بحسب هذه المعلومات
وهو ما يتسبب بضعف أمن المعلومات وزيادة تكاليف توفيرها وإدارتها.

4.4 أنواع مخاطر نظم المعلومات:

1.4.4 المخاطر حسب المصدر: ويقسم إلى

مصادر داخلية: موظفي المنظمة هم مصدر المخاطر الداخلية كونهم على معرفة بمعلومات ودراية بالنظام الرقابي للمنظمة ومعرفة نقاط القوة والضعف للنظام ولهم القدرة على التعامل مع المعلومات والوصول إليها من صلاحيات الدخول الممنوحة لهم ولذلك فموظفي المنظمة غير الأمناء يمكنهم الوصول للبيانات وإمكانية تدميرها أو (مدوكي، 2017، صفحة 125).

مصادر خارجية: تتمثل في أشخاص خارج المنظمة ليس لهم علاقة مباشرة بالمنظمة مثل قرصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الأمنية للنظام للحصول على معلومات سرية عن المنظمة قد تتمثل في كوارث طبيعية مثل الزلازل أو البراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنظمة (الشوابكة، 2019، صفحة 169).

2.4.4 المخاطر حسب المتسبب فيها : وتنقسم إلى

مخاطر ناتجة عن العنصر البشري: وهي تلك المخاطر التي تنتج عن العنصر البشري بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ (المالك، 2021، صفحة 206).

مخاطر ناتجة عن العنصر غير البشري: وهي تلك المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان دخل فيها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه.

3.4.4 المخاطر وعلاقتها بمراحل عمل نظم المعلومات:

مخاطر التدخلات: وهي المخاطر الناتجة عن عدم تسجيل بيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال.

مخاطر التشغيل: تتعلق بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيلها وتتمثل في الاستخدام غير المصرح به لنظام و برامج التشغيل وتعديل البرامج بطريقة غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي.

5. سياسات إدارة مخاطر نظم المعلومات: في دراسة أجرتها مدرسة "سلون" التابعة لمركز إدارة بحوث نظم المعلومات في معهد "ماساتشوس" للتكنولوجيا بشأن عملية إدارة مخاطر تكنولوجيا المعلومات والشبكات تناولت أكثر من 300 مؤسسة أعمال في 20 بلد، خلصت لحدوث قيمة مضافة في العمل وزيادة في الناتج الوطني الإجمالي المتصل بتكنولوجيا المعلومات ناتجة مباشرة عن الإدارة الفعالة لهذه التكنولوجيا (الله، 2009، صفحة 33)، وأشارت إلى أن المنظمات التي لديها إدارة مخاطر فعالة بدرجة أكبر لتكنولوجيا المعلومات تحقق أرباحا أعلى بنسبة 20% على الأقل عن مثيلتها لدى الشركات التي لديها إدارة رديئة وغير آمنة لهذه التكنولوجيا، وذلك في ظل وجود أهداف استراتيجية موحدة.

1.5 تعريف إدارة مخاطر نظم المعلومات: هي ممارسة لعملية اختيار نظامية لطرائق ذات تكلفة فعالة للتقليل من أثر تهديد على المنظمة، وهي مقترنة مع مبدأ استمرارية العمل، وتعني تقييم للمخاطر وتطوير استراتيجيات لإدارتها، وهذه الاستراتيجيات تتضمن نقل المخاطر لجهة أخرى أو تجنبها أو التقليل من آثارها السلبية وقبول بعض أو كل تبعاتها.

2.5 تعريف إدارة الخطر المعلوماتي (الخطر التكنولوجي) عرف بأنه عملية تقوم من خلالها المنظمة بتوجيه الأعمال المتعلقة بتكنولوجيا المعلومات والشبكات لتحقيق أهدافها وتحديد المسؤولية بشأن تلك الأعمال ونتائجها. وعرف بأنه مجموعة الإجراءات والسياسات التي تضمن أن نظام تكنولوجيا المعلومات يدعم استراتيجياتها لتوجيه وظيفة تكنولوجيا المعلومات والرقابة عليها لإضافة قيمة وتقليل مخاطر تكنولوجيا المعلومات (شنب، 2009، صفحة 24).

3.5 الهيكل الهرمي لإدارة مخاطر نظم المعلومات والشبكات: يقسم إلى

خمس طبقات، وهي كالتالي:

-التشريعات: يتم إعدادها من قبل الحكومة وتؤثر على المؤسسة بغض النظر عن حجمها.

-السياسات: يتم صياغتها ووضعها من قبل المنظمة ويتم الموافقة عليها من قبل الإدارة العليا.

-المعايير: وهي التي يتم اشتقاقها من السياسات وتكون محددة ويمكن قياسها لتحديد مدى التزام العاملين بها.

-الإجراءات: وهي تعليمات توضح للمستخدم ما يجب القيام به المستفيد لتنفيذ السياسة وتكون موضحة خطوة بخطوة

-التوجيهات: وهي عبارة عن توصيات توضح ما تفضل المؤسسة أن تراه من قبل أعضائها وتكون اختيارية.

الشكل رقم 4 يبين هذه المراحل، حيث أن التشريعات هي الأساس الذي تنبثق عنه السياسات ومن ثم تشتق المعايير من السياسات وتنبثق عنها الإجراءات وفي النهاية التوجيهات وهي توصيات إضافية على الإجراءات وتكون اختيارية.

الشكل 4: الهيكل الهرمي لإدارة مخاطر نظم المعلومات



المصدر: من إعداد الباحث بالاعتماد على دراسة (Hare, 2001)

4.5 استراتيجيات إدارة مخاطر نظم المعلومات: تتطلب إدارة المخاطر المعلوماتية تحديد الإجراءات المتعلقة بإدارة المخاطر وتوثيقها، ثم تفويض فريق إدارة المخاطر لممارسة مهامه، ويجب أن تكون سياسة إدارة المخاطر المعلوماتية تابعة لسياسة امن المعلومات العامة داخل المنظمة، ومن أهم السياسات الواجب إتباعها من طرف إدارة المخاطر نجد:

1.4.5 التشفير (Encryption): هو العملية التي يتم بها تغيير البيانات وجعلها في شكل غير مقروء، بحيث لا يستطيع إرجاعها لوضعها الأصلي إلا الأشخاص المرخص لهم الذين لديهم الأدوات اللازمة، ويتكون التشفير من عمليتين هما التشفير وفك التشفير، وحسب نوعية التشفير فانه يمكن استخدام مفتاح تشفير أو أكثر لإتمام هاتين العمليتين.

الشكل 5: طريقة عمل التشفير



المصدر: (المدرع، 2016، صفحة 18)

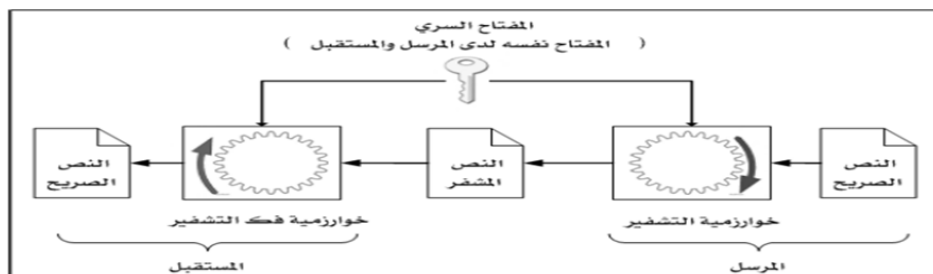
ينقسم التشفير لنوعان هما التشفير المتناظر والتشفير غير المتناظر (القحطاني د.، 2015، صفحة 113):

التشفير المتناظر (Symmetric Encryption): نظام تشفير يستخدم مفتاحا متناظرا لدى كل من المرسل والمستقبل بحيث يستخدم المفتاح نفسه في عمليتي التشفير وفك التشفير الشكل رقم 6، وتتم عمليتا التشفير وفك التشفير كالتالي:

عملية التشفير: تشفير الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح السري المشترك للحصول على رسالة مشفرة.

فك التشفير: يفك تشفير الرسالة المشفرة بخوارزمية فك التشفير والمفتاح السري المشترك للحصول على الرسالة الأصلية.

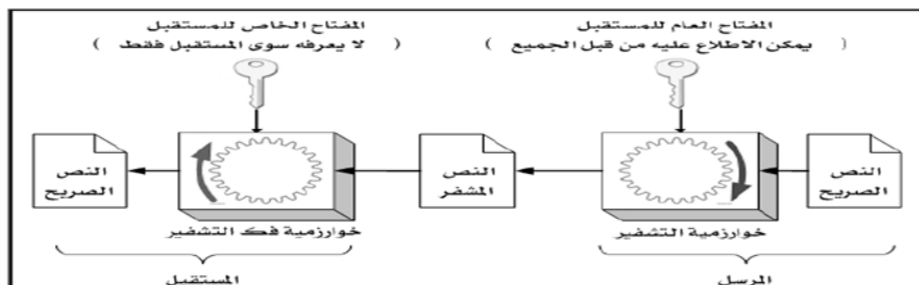
الشكل 6: عملية التشفير المتناظر



المصدر: القحطاني، (القحطاني ذ، 2015، صفحة 114)

التشفير غير المتناظر (التشفير باستخدام المفتاح العام): قدم التشفير باستخدام المفتاح العام طريقة جديدة تختلف تماما عن التشفير المتناظر فهو تشفير غير متناظر أي لا يوجد مفتاح سري مشترك بين المرسل والمستقبل منذ البداية وإنما يستخدم مفتاحان منفصلان، يستخدم احدهما للتشفير والآخر (وهو مرتبط بالأول) لفك التشفير، في هذا التشفير يولد كل مستخدم زوجا من المفاتيح مرتبطتين ببعضهما البعض بطريقة رياضية معقدة لا تسمح بكشف أي منهما إذا عرف الآخر احدهما عام ويوضع في سجل المجلد عام يمكن الاطلاع عليه من قبل جميع المستخدمين والآخر خاص ويعدا مفتاحا سريا خاصا بالمستخدم ويجب أن لا يطلع عليه الآخرون ثم بعد ذلك تتم عمليتا التشفير وفك التشفير.

الشكل 7: عملية التشفير غير المتناظر



المصدر: (القحطاني ذ، 2015، صفحة 146)

عملية التشفير: تشفر الرسالة الأصلية باستخدام خوارزمية التشفير والمفتاح العام للمستقبل للحصول على رسالة مشفرة، حيث يمكن للمرسل الحصول على المفتاح العام للمستقبل لأنه علني مشاع.

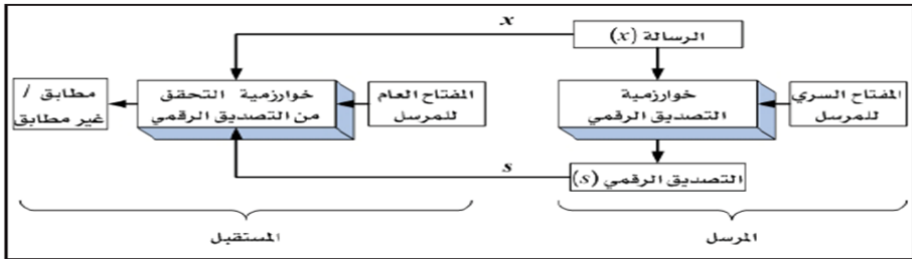
عملية فك التشفير: يتم فك تشفير الرسالة المشفرة باستخدام خوارزمية فك التشفير والمفتاح الخاص (السري) للمستقبل للحصول على الرسالة الأصلية ولن يستطيع أي شخص آخر فك تشفير الرسالة لأنه لا يملك المفتاح الخاص للمستقبل.

2.4.5 التصديق (التوقيع) الرقمي: أحد أهم أدوات إدارة مخاطر تكنولوجيا المعلومات والشبكات، يعد وحدة بناء لتحقيق عدد من عناصر أمن المعلومات مثل التحقق من هوية أصل البيانات وعدم الإنكار، فعندما يوقع الشخص المخول بالتوقيع (اليدي) على رسالة أو خطاب معين فيكتسب صيغته الرسمية ويتم التحقق من أصل هذه البيانات بأنها صدرت من الجهة أو الشخص المخول بالتوقيع، إذن فالتوقيع الرقمي يتكون من عمليتين أساسيتين كما هو موضح في الشكل وهما:

التوقيع (Sign): وهو عملية إجراء (إنتاج) التصديق الرقمي ومدخلاتها وهي الرسالة والمفتاح السري للموقع ونتيجتها هي التوقيع الرقمي نفسه وهو رقم صحيح

التحقق من صحة التوقيع (Verify): وهو عملية التحقق من أن التوقيع تم من الشخص المعني على الرسالة المعنية ومدخلاتها وهي الرسالة والمفتاح العام للموقع ونتيجتها إحدى حالتين إما مطابق أو غير مطابق.

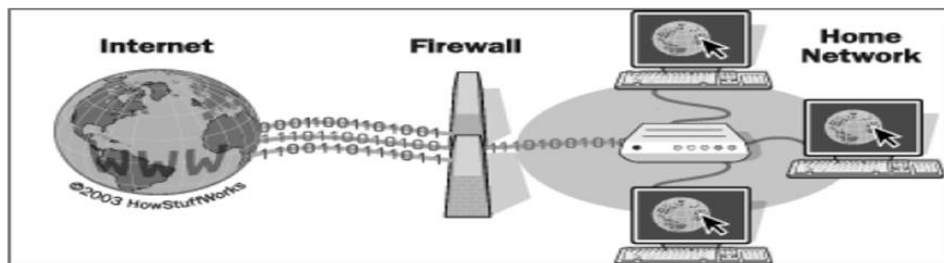
الشكل 8: التصديق الرقمي



المصدر: (القحطاني د.، 2015، صفحة 163)

3.4.5 جدار الحماية: أداة تحجز مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية، والهدف هو حجز المستخدم في حيز سياسة أمنية، هذه السياسة قد تكون منع أي دخول من الخارج مع السماح بالمرور من الداخل إلى الخارج، وقد تكون سياسة السماح بالدخول من أماكن معينة أو من جانب مستفيدين معينين أو دخول أنشطة معينة دون أخرى، وضع السياسة الأمنية السليمة التي تلبي احتياجات المنظمة هو تحدي تواجه المنظمة عندما تقرر حماية شبكتها بجدار الحماية ويستطيع المستخدم من خلاله الخروج إلى عالم الانترنت، ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله، ويوضح الشكل 9 موقع جدار الحماية في بيئة نظم المعلومات وكيفية صده للهجمات من الخارج.

الشكل 9: آلية عمل جدار الحماية



المصدر: (المدرع، 2016، صفحة 23)

4.4.5 برمجيات مكافحة الفيروسات: هي برامج تستخدم لمنع اكتشاف الحاسوب وبرامج التجسس، لكن ومهما كانت برامج مكافحة الفيروسات مفيدة فإنه في بعض الأحيان تكون لها عيوب، فيمكن لبرامج مكافحة الفيروسات أن تقلل من أداء الحاسوب إذا لم تكن مصممة بكفاءة، وقد يواجه المستخدمون غير الخبراء مشكلة في فهم الأوامر والقرارات التي يقدمها برنامج الحماية من الفيروسات وقد يؤدي القرار أو الاستعمال غير الصحيح إلى الإخلال بالأمن.

4. خاتمة:

توصلت هذه الدراسة إلى النتائج التالية:

-تتعدد صور المخاطر التي تتعرض لها تكنولوجيا المعلومات والشبكات الالكترونية ما بين مخاطر داخلية ومخاطر خارجية وتعتبر المخاطر الداخلية من أكثر المخاطر تهديدا لأمن وسلامة نظم المعلومات في المنظمات الرقمية.

-تعمل استراتيجية إدارة مخاطر تكنولوجيا المعلومات على توفير إطار للرقابة لضمان أن المخاطر التي تتعرض لها المنظمات يتم الوصول بها للمستوى المسموح به، والتأكيد بأن استراتيجيات الأمن المتبعة تتفق مع أهدافها الاستراتيجية؛

- يحقق التطبيق الجيد لإدارة مخاطر تكنولوجيا المعلومات عديد الفوائد والتي لا تؤدي فقط إلى تخفيض المخاطر أو الحد من تأثير إجراءات خاطئة بل يمكن أن تعمل على تحسين الثقة داخل وخارج المنظمة مما يؤدي لتحسين سمعة المنظمة؛

- تعتبر المواصفة (ISO 27001:2005) قاعدة لتقييم إدارة حماية المعلومات، باعتبارها وثيقة لتقييم النظام.

- معيار المواصفة (ISO 27001:2005) من المعايير العالمية الوحيدة المتميز بمرونته، بحيث يتوافق مع جميع المنظمات حكومية كانت أو خاصة، بحيث تقوم المنظمة بدراسة المخاطر المتعلقة بمعلوماتها وفهمها ومن ثم بناء نظام أمن معلومات متكامل يقلل المخاطر وقابل للتطوير والتكيف.

توصي هذه الدراسة بما يلي:

- زيادة الاهتمام بتوعية المنظمات بأهمية استخدام مبادئ ومعايير إدارة مخاطر تكنولوجيا المعلومات حتى يتسنى لها مواجهة التحديات والمخاطر التي تواجه بيئة تكنولوجيا المعلومات؛

- يتوجب على المنظمات التركيز على الحفاظ على المعلومات حيث أنها لن تنتهي أو تضمحل قيمتها بل ستتغير قيمتها مع مرور الزمن الأمر الذي يوجب ضرورة توفير وسائل الخزن الملائمة وتوفير سهولة في عمليات الاسترجاع والتحديث.

- وضع استراتيجية مؤسسية بشأن إدارة مخاطر تكنولوجيا المعلومات تتلاءم واحتياجات العمل لدى المنظمات بما يجعل من الاستثمار في هذه التكنولوجيا يحقق القيمة الحقيقية المتوخاة منه، وهي الاستراتيجية التي يجب مرجعتها بشكل دوري.

-حث المنظمات على ضرورة الربط بين إدارة مخطر تكنولوجيا المعلومات والمواصفة (ISO 27001)، مما سيوفر وسائل فاعلة للتعامل مع المعلومات، كما أن حصول المنظمات على شهادة ISO يسمح للمنظمات بالحصول على ميزة تنافسية.

5. المراجع:

- Djamil, M. B. (2020). Intelligence économique Et Système D'information Dans Les Entreprises Algériennes. *Revue Maghrébine Management des Organisations* , 5(1).
- Djenane Abdelhak, H. D. (2012). Computerized Information Systems In The Jordanian Banking Sector: An Empirical Study. Djenane Abdelhak Hammoudi Dalel. *Revue des Economies financières bancaires et de management* , 1(1).
- Lamaria, S. (2020). Maîtrisons- Nous L'information . *Revue Afak Ilmia*, 12(2).
- Mohamed, A. (2007). La Mondialisation Des Affaires Et Les Technologies De L'information . *la revue des sciences commerciales*, 6(1).
- Noureddine Myriam, R. A. (2018). Mise en place d'un système d'information pour évaluer la performance d'un service hospitalier. *Algerian Business Performance Reviiew*, 7(3).
- Pilamunga Poveda, S. A. (2019). Smart Institution Model. *IOP Conference Series: Materials Science and Engineering*. Cartagena, Colombia.
- Sihem, B. Y. (2015). les systèmes d'information un atout concurrentiel pour l'entreprise. *Revue des reformes Economique et intégration dans l'économie mondiale*, 10(19).

أحمد مصباح خياط. (2019). تصور مقترح لتطوير إدارة الأعمال في ضوء مدخل إدارة المخاطر بمؤسسات الأعمال الكويتية. *المجلة العلمية للاقتصاد والتجارة*, 49(4).

إسلام هلايلي، نور الدين أحمد قايد. (2019). مساهمة نظام المعلومات المحاسبية في تحسين عملية اتخاذ القرارات بالمؤسسة الاقتصادية. *مجلة دفاتر اقتصادية*, 10(2).

- أشرف عبد الرحمن محمد. (2005). دور إدارة الموارد البشرية في منظمات الأعمال في ظل إقتصاد المعرفة. القاهرة: منشورات كلية التجارة.
- الرزاق بق. م. (2017). دور نظم المعلومات الإلكترونية في إدارة مخاطر الصناعة التأمينية دراسة حالة عينة من شركات التأمين الجزائرية. مجلة الاكاديمية للدراسات الاجتماعية و الانسانية. (2)9 ,
- الطاهر بن عمارة، خالد رجم، العربي عطية. (2018). أثر نظام الحماية الالكترونية في الحد من مخاطر تكنولوجيا المعلومات و الاتصال دراسة مقارنة لعينة من المؤسسات . مجلة رؤى اقتصادية، 8(2).
- إلهام بروية. (2021). أهمية نظام المعلومات المحوسب في اتخاذ القرارات المالية في منظمات الأعمال. مجلة نور للدراسات الاقتصادية، 6(10).
- أمينة بق. (2016). استراتيجية أمن المعلومات. مجلة ابعاد اقتصادية. (1)6 ,
- جودة إبراهيم، توفيق حسن. (2015). نظم وتكنولوجيا المعلومات المستخدمة في دائرة ضريبة الدخل والمبيعات وأثرها على فاعلية الدائرة في الأردن . مجلة الاقتصاد الصناعي، 5(2).
- خالد بن سليمان، القحطاني محمد بن عبد الله. (2009). أمن المعلومات بلغة ميسرة. (جامعة الملك سعود، المحرر) الرياض: مركز التميز لأمن المعلومات.
- خالد رجم، الطاهر بن عمارة، محمد يزيد ذكار. (2018). تقييم كفاءة نظام المعلومات الإلكتروني دراسة مقارنة بين المؤسسة الوطنية للجيو فيزياء و مؤسسة الشراكة Hess (اجنبية- سونطراك) . مجلة العلوم الاقتصادية وعلوم التسيير ، 18(1).
- خلفي سفيان، شريط كمال. (2019). نظم المعلومات الإستراتيجية: كآلية لدعم القرارات المتعلقة بإدارة الموارد البشرية في منظمات الأعمال. مجلة المشكاة في الاقتصاد والتنمية والقانون، 3(1).

- خليفة أحمد، ضيف الله محمد الهادي، زين عبد المالك. (2021). أثر حوكمة تكنولوجيا المعلومات على مخاطر نظام المعلومات المحاسبي: دراسة ميدانية لعينة من المحاسبين من 2019/09/14 إلى 2019/10/30. *مجلة الدراسات المالية والمحاسبية والإدارية*، 8(1).
- ذيب بن عايض القحطاني. (2015). *أمن المعلومات*. (مكتبة الملك فهد الوطنية للنشر، المحرر) الرياض: مدينة الملك عبدالعزيز للعلوم والتقنية.
- زياد محمد الشрман. (2004). *مقدمة في نظم المعلومات الإدارية* (المجلد الطبعة الأولى). عمان: دار صفاء للنشر والتوزيع.
- سعد علي حمود العنزي، أحمد علي صالح. (2009). *إدارة راس المال الفكري في إدارة الأعمال*. عمان: دار اليازوري للنشر والتوزيع.
- سلوي ثابت مكي. (2021). *الإصلاح الهيكلي للمؤسسات والحوكمة الرقمية*. مجلة *السياسة والاقتصاد*، 12(11).
- عدنان عواد الشوابكة. (2019). دور إجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات في جامعة الطائف . *مجلة دراسات وأبحاث*، 11(4).
- عرفان نبي، عبد الرحمن مزرا، خالد الغثير. (2008). *رسالة عملية حول أمن المعلومات في المنظمات السعودية*. جامعة الملك سعود. مركز التميز لأما المعلومات.
- عصام محمد البحيصي، حرية شعبان الشريف. (2008). *مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في غزة*. مجلة *الجامعة الإسلامية (سلسلة الدراسات الانسانية)*، 16(2).
- عصام محمد البحيصي، حرية شعبان الشريف. (2008). *مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة*. مجلة *الجامعة الإسلامية (سلسلة الدراسات الانسانية)*، 16(2).

- علاء الدين محمد تايه. (2008). مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين. غزة: الجامعة الإسلامية.
- عماد أحمد محمد أبو شنب. (2009). إدارة وتحليل مخاطر أمن المعلومات. مؤتمر أمن المعلومات والحكومة الإلكترونية. كوالالمبور.
- عمر بن محمد العتيبي. (2010). الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية . جامعة نايف العربية للعلوم الأمنية. كلية الدراسات العليا، قسم العلوم الإدارية.
- فهد فايز المدرع. (2016). المعايير العالمية لأمن المعلومات. مركز التميز لأمن المعلومات.
- قورين حاج قويدر، نور الهدى نقاز. (2019). نظام المعلومات المحاسبي وتكنولوجيا المعلومات وتأثيرهما على جودة المعلومات المالية دراسة حالة مؤسسة Nover Spa بالشلف . مجلة المحاسبة التدقيق والمالية ، 1(1).
- محمد دباس الحميد، ماركو إبراهيم نينو. (2007). حماية أنظمة المعلومات (المجلد الطبعة الأولى). عمان: دار ومكتبة الحامد للنشر والتوزيع.
- محمد موسى علي شحاتة. (2020). دور تفعيل آليات التحول الرقمي في تحسين كفاءة النظام الضريبي المصري كمرتكز للحد من التهرب الضريبي في ضوء رؤية مصر 2030م " بين حتمية التغيير ... ونتائج التطبيق". المجلة العلمية للدراسات والبحوث المالية والإدارية، 6(1).
- محمود سليم عبد الرحمن الشوكت، ياسر عيسى المومني، قدري سليمان الشكري. (2016). دور نظم المعلومات الإدارية في اتخاذ القرارات دراسة ميدانية على جامعتي اليرموك وعجلون الوطنية. مجلة دفاتر بولكس، 5(2).

- مصطفى علي شديد. (2021). تأثير التحول الرقمي على مستوى أداء الخدمة المقدمة بالتطبيق على موظفي الإدارة العامة للمرور بمحافظة القاهرة. مجلة كلية الاقتصاد والعلوم السياسية، 22(4).
- منصور بن سعيد القحطاني. (2008). مهددات الأمن المعلوماتي وسبل مواجهتها : دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية (السعودية بالرياض). جامعة نايف العربية للعلوم الأمنية. كلية الدراسات العليا، قسم العلوم الإدارية.
- ناصر نور الدين عبد اللطيف. (2004). نظم المعلومات المحاسبية. الاسكندرية: الدار الجامعية للنشر والتوزيع.
- نوال بنت علي البلوشية، نيهان بن حارث الحراصي، علي بن سيف العوفي. (2020). واقع التحول الرقمي في المؤسسات. *Journal of Information Studies & Technology (JIS & T)*، 3(1).
- هاشم فوزي العبادي. (2012). الذكاء التنظيمي كممارسة أعمال نجو بناء منظمة ذكية. المؤتمر العلمي السنوي الحادي عشر حول: نكاء الأعمال واقتصاد المعرفة. عمان: جامعة الزيتونة.
- وليد سمير عبد العظيم الجبلى. (2019). أثر مخاطر تكنولوجيا المعلومات على مكونات هيكل الرقابة الداخلية مسئولية مراجعي الحسابات عنها - دراسة ميدانية - مجلة الدراسات المالية والمحاسبية ، 10(1).
- يوب أمال، بودبزة إكرام. (2019). أثر التغيير التنظيمي في نجاح التحول الرقمي بالمؤسسات العمومية الجزائرية -دراسة استطلاعية لعينة من بلديات ولاية سكيكدة. مجلة الاقتصاد الجديد، 10(3).

-
- يوسف حجيم الطائي وآخرون. (2013). صياغة الاستراتيجية المستدامة للشركة في بناء المنظمات الذكية: دراسة استطلاعية لأراء عينة من المدراء في شركة زين العراق للاتصالات. مجلة الغري للعلوم الاقتصادية والادارية، 9(25).
- يوسف مدوكي. (2017). إدارة مخاطر وأمن المعلومات في ظل ثورة نظم وتكنولوجيا المعلومات . مجلة الأفاق للدراسات الاقتصادية، 2(1).