مجلة أبحاث إقتصادية معاصرة | ISSN 2572-0171 EISSN: 2716-8891 | المجلد 04 ، العـدد: 02 (2021)، ص 164- 178

أمن نظام المعلومات المحاسبي في ضوء المعيار الدولي ISO 27005 دراسة ميدانية على عدد من الشركات الجزائرية

The accounting information system security in light of ISO 27005 An applied study on a number of Algerian companies

زعابطة عبد اللطيف [1] *، عجيلة محمد [2]

ADJILA MOHAMED ZAABTA ABDELLATIF

[1] جامعة غرداية، الجزائر، zeabta. abdlatif@univ-ghardaia.dz

[2] جامعة غرداية، الجزائر، adjila_78@yahoo.fr

تاريخ الاستلام: 2021-08-17 **تاريخ القبول:** 2021-09-15 **تاريخ النشر:** 2021-10-26

ملخص:

تهدف هذه الدراسة إلى قياس درجة أمن نظام المعلومات المحاسبي في الشركات الجزائرية في ضوء معايير الإيزو لأمن المعلومات وذلك بالتركيز على نقاط الضعف، وتأتي أهمية هذه الدراسة من واقع التطور المتسارع في تكنولوجيا المعلومات وما يصاحبه من مخاطر.

خلصت الدراسة إلى وجود علاقة إرتباطية عكسية ذات دلالة إحصائية بين أمن نظام المعلومات المحاسبي ونقاط الضعف الأمني فيه، بحيث ينبغي العمل على الحد من نقاط الضعف بهدف رفع مستوى أمن نظام المعلومات المحاسبي ليرقى إلى تلبية متطلبات مواصفات الإيزو.

الكلمات المفتاحية: أمن نظام المعلومات المحاسبي؛ نقاط الضعف الأمني؛ ISO 27005؛

تصنيف JEL : M150 ؛M41

Abstract:

This study aims to measure the degree of security in the accounting information system in Algerian companies in the light of ISO standards by focusing on the vulnerabilities. The study concluded that there is an inverse correlation relationship with statistical significance between security of accounting information system and security vulnerabilities.

Keywords: accounting information system security, security vulnerabilities, ISO 27005

JEL Classification Codes : M41, M150

* : المؤلف المرسل

1. مقدمة:

إن تطور استخدام تكنولوجيا المعلومات والاتصال قد وفر الكثير من الوقت والجهد للعاملين، فتحولت البيانات المحاسبية اليدوية إلى قاعدة بيانات إلكترونية متكاملة تحتوي على كافة البيانات المحاسبية لخدمة مختلف مستخدميها. لكن هذا التطور رافقه ظهور مخاطر وأعباء جديدة، إذ واجهت نظم المعلومات المحاسبية العديد من التهديدات والتي قد ينجم عنها أضرار تتسبب في خسائر جوهرية وهامة. من هنا كان على المؤسسات الإقتصادية أن تشدد من إجراءاتها الأمنية لحماية نظم المعلومات المحاسبية، وبغية الوصول إلى ذلك تحتاج هذه المؤسسات إلى تبني سلسلة من العمليات التنظيمية التي من ضمنها اكتشاف نقاط الضعف الأمنية والتي تعتبر بدورها منفذا للمخاطر التي تواجه نظم المعلومات المحاسبية.

إشكالية الدراسة:

من خلال ما سبق تتضح مشكلة البحث كما يلي:

ما حجم نقاط الضعف الأمنية في نظام المعلومات المحاسبي بالشركات الجزائرية؟

الفرضيات:

- حالة العناصر المادية الداعمة للعمليات لها تأثير نسبي على أمن نظام المعلومات المحاسبي؛
- نوعية البرامج التي تساهم في تشغيل مجموعة معالجة البيانات لها تأثير نسبي على أمن نظام المعلومات المحاسبي؛
- أجهزة الاتصالات السلكية واللاسلكية المستخدمة لربط أجهزة الكمبيوتر البعيدة فعليًا أو لربط عناصر نظام المعلومات لها تأثير نسبي على أمن نظام المعلومات المحاسبي؛
- مجموع الأشخاص المشاركين في نظام المعلومات لهم تأثير نسبي على أمن نظام المعلومات المحاسبي؛
- حالة الأماكن التي تحتوي على نطاق نظام المعلومات أو جزء منه والوسائل المادية اللازمة لتشغيله لها تأثير نسبي على أمن نظام المعلومات المحاسبي؛
- الإطار التنظيمي الذي يتكون من جميع هياكل الموظفين المعنية بأمن نظام المعلومات المحاسبي والإجراءات التي تتحكم في هذه الهياكل له تأثير نسبي على أمن نظام المعلومات المحاسبي.

أهداف الدراسة:

ترمي هذه الدراسة إلى تحقيق عدة أهداف من بينها التعرف على أمن نظام المعلومات المحاسبي وطبيعة المخاطر التي تهدده وأسباب حدوثها، وهي أيضا تهدف إلى قياس درجة أمن نظام المعلومات المحاسبي في الشركات الجزائرية في ضوء معايير الإيزو لأمن المعلومات وذلك بالتركيز على نقاط الضعف.

منهجية الدراسة:

تم الإعتماد على المنهج الوصفي في وصف مختلف الجوانب النظرية المتعلقة بالموضوع، بالإضافة إلى المنهج التحليلي من خلال اختبار الفرضيات وتحليل النتائج المتوصل إليها.

2. الإطار النظري للدراسة :

1.2 أمن نظام المعلومات المحاسبي:

1.1.2 النظام ونظام المعلومات:

يعرف النظام بأنه مجموعة الموارد والعناصر (الأفراد، التجهيزات، الآلات، الأموال، السجلات... الخ) المترابطة والمتجانسة، التي تتفاعل مع بعضها البعض داخل إطار معين (حدود النظام) ، تعمل كوحدة واحدة لتحقيق هدف، أو مجموعة من الأهداف العامة في ظل الظروف (بيئة النظام) ، وتتم مراقبتها روتينيا من قبل المسؤولين (علي و أحمد، 2011، صفحة 13)، أما نظام المعلومات، فهو مجموعة من الموارد والمكونات المترابطة مع بعضها البعض بشكل منتظم، تسمح بتجميع بيانات ومعالجتها لإنتاج معلومات وإيصالها إلى المستخدمين بالشكل الملائم، وفي الوقت المناسب من أجل مساعدتهم في اتخاذ القرارات (قاسم ، 2008، صفحة 19).

2.1.2 أشكال نظم المعلومات:

نظم المعلومات اليدوية: تجرى جميع عملياتها من إدخال وإخراج بشكل يدوي باستخدام أدوات تقليدية، مثل الورق والأقلام (Ball, 2001, p. 677).

نظم المعلومات المتكاملة: تعد تطبيقا لمجموعة نظم بالمؤسسة في الوقت نفسه، لتجنب تكرار استخدام المعلومات في كل نظام، بهدف زيادة الفعالية وخفض التكاليف (Dyrieux, A, 2004, p. 10).

نظم المعلومات الالكترونية: تعتمد على الأجهزة الآلية، وشبكات الربط والاتصال في عملياتها، وتتميز بمعالجة كمية ضخمة من البيانات بسرعة ودقة عاليتين (Denisi, A & Griffin, R, 2010, p. 09).

3.1.2 نظام المعلومات المحاسبي:

يعرف بأنه:" ذلك الجزء من نظام المعلومات الكلي الذي يختص بتجميع وتشغيل وتخزين واسترجاع البيانات الكمية والنقدية وغير النقدية لأغراض توفير المعلومات لمتخذي القرارات من خلال التنظيم". (صلاح الدين و لطفي ، 1996، صفحة 79).

يتكون نظام المعلومات المحاسبي مما يلي: (ثامر ، 2012، الصفحات 28-31)

- المدخلات (الأحداث المالية): وهي عبارة عن المعاملات ذات الطبيعة المالية، والموثقة بمستندات تثبت وقوعها بتواريخ محددة؛
- المعالجة: حيث تخضع المدخلات للمعالجة والتسجيل والتبويب والتلخيص لقيود تلك المعاملات المالية؛

- المخرجات: وهي تتمثل في التقارير والقوائم المالية التي ينتجها النظام وهي بمثابة المنتج النهائي لنظام المعلومات المحاسبي؛
- الرقابة: وتتم عملية الرقابة على كل من المدخلات وعمليات المعالجة التي تتم داخل النظام؛
- التغذية العكسية: تعد التغذية العكسية عملية أساسية لنجاح النظام المحاسبي ونموه فهي عملية قياس ردة فعل المستفيدين والمتعاملين مع الشركة على عمل نظام المعلومات المحاسبي.

4.1.2 مفهوم أمن المعلومات (أمن نظام المعلومات):

توجد العديد من التعاريف لمصطلح أمن المعلومات، فقد عُرف بأنه "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المؤسسة نفسها والأفراد العاملين فيها وأجهزة الحاسوب المستخدمة فيها ووسائل المعلومات التي تحتوي على بيانات المؤسسة، ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عدة تضمن في النهاية سلامة المعلومات" (داوود، 2000، صفحة 23)

ويعبر عن أمن المعلومات بأنه "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية" (لمين، 2008، صفحة 02).

أمن المعلومات هو كذلك "مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي، للحفاظ على المعلومات والأجهزة والبرمجيات، إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال (نجم ، 2005، صفحة 265).

ينقسم أمن المعلومات إلى: (Whitman & Mattod , 2011, p. 62)

- الأمن المادي: بما يشمله من مصادر وممتلكات ومباني لمنع الوصول غير المشروع؛
- أمن الأفراد: لحماية الافراد والمجموعات الذين لهم حق الوصول للمعلومات؛
- أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون؛
- أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى؛
- أمن الشبكات: لحماية مكونات الشبكة والتراسل والمحتويات؛
- أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات.

5.1.2 مكونات أمن المعلومات:

يرى خبراء ومختصون في أمن المعلومات أن هناك ثلاثة مكونات (و تسمى ثلاثية أمن المعلومات) على درجة واحدة من الأهمية، حيث أنه لو انتهك أحدها فنعتبر أن المعلومة قد تعرضت للخطر. وهذه المكونات هي: (خالد و محمد ، 2009، صفحة 22 23)

- سرية المعلومات: ويشتمل هذا العنصر على كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة أو السرية؛
- سلامة المعلومات: التأكد أن هذه المعلومات لم تتعرض لأي عملية حذف أو تخريب أو اتلاف كلي أو جزئي سواء بصفة متعمدة أو غير متعمدة في أي مرحلة من مراحل المعالجة او التبادل؛

- توفر المعلومات: من يحق له الإطلاع عليها يمكنه الوصول إليها، والوصول إليها يمكن أن يتم في التوقيت المناسب (لا يحتاج وقتا طويلا).

6.1.2 المخاطر التي تواجه نظام المعلومات المحاسبي:

قبل الخوض في أنواع المخاطر، لا بد من توضيح بعض المصطلحات المستخدمة في هذا المجال، فمصطلح الخطر (risk) يشير إلى أي حدث معادي مقصود أو أي حدث غير مقصود يمكن أن يتسبب في أضرار لنظام المعلومات المحاسبي أو للمؤسسة. أما أثر الخطر (Impact of exposure) فيعني الخسائر المادية التي تحدث نتيجة حصول الخطر. كما يشير مصطلح الاحتمال الأرجح (Likelihood) إلى قوة احتمال حدوث الخطر (Romney و Steinbart، 2006، صفحة 191).

تم تقسيم مخاطر نظم المعلومات المحاسبية إلى ما يلي:

أ. **من حيث مصادرها:** تقسم إلى (سعد و حنان، 2011، صفحة 226 228):

- المخاطر الداخلية؛
- المخاطر الخارجية.

ب. **من حيث المتسبب:** يمكن تصنيفها بشكل عام إلى ثلاث فئات (سعد و حنان، 2011، صفحة 225):

- المخاطر البشرية؛
- الجرائم المحوسبة؛
- المخاطر البيئية.

ج. **من حيث العمدية:** وتصنف إلى نوعين هما: (محمد العلمي ، 2015، صفحة 29)

- مخاطر ناتجة عن تصرفات متعمدة؛
- مخاطر ناتجة عن تصرفات غير متعمدة.

د. **من حيث الآثار الناتجة عنها:** وهي كما يلي: (محمد العلمي ، 2015، صفحة 31)

- مخاطر تنتج عنها أضرار مادية؛
- مخاطر فنية ومنطقية.

هـ. **من حيث علاقتها بمراحل النظام** (Abu-Musa, 2004, p. 05):

- مخاطر المدخلات؛
- مخاطر معالجة البيانات؛
- مخاطر المخرجات.

2.2 المعيار الدولي ISO 27005

الإيزوISO: هي منظمة تعمل على وضع المعايير، وتضم ممثلين من عدة منظمات قومية للمعايير. تأسست في 1947 وهي تصدر معايير تجارية وصناعية عالمية. يكمن مقرها في جنيف، سويسرا. تملك منظمة الأيزو صلات قوية مع الحكومات وتضم حوالي 163 عضوا من هيئة المعايير الدولية وقد أصدرت هذه المنظمة أكثر من 22000 وثيقة في مجالات عديدة (International Organization for Standardization , ISO, 2020).

1.2.2 سلسلة ISO / IEC 27000: (أو "ISO27K" باختصار)

والمعروفة أيضًا باسم "مجموعة معايير نظام إدارة أمن المعلومات "(Information Security Management System Standards) ISMS Standards"، و تشتمل على معايير أمن المعلومات التي تم نشرها بشكل مشترك من قبل المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهروتقنية الدولية (IEC) (International Organization for Standardization , ISO, 2020).

يتكون نظام إدارة أمن المعلومات (ISMS) من السياسات والإجراءات والمبادئ التوجيهية والموارد والأنشطة المرتبطة بها، والتي تدار بشكل جماعي في السعي لحماية أصول المعلومات الخاصة بها.

ISMS هو نهج منظم لإنشاء وتنفيذ وتشغيل ومراقبة ومراجعة وصيانة وتحسين أمن معلومات المؤسسة لتحقيق أهدافها. وهو يعتمد على تقييم المخاطر ومستويات قبول المخاطر في المؤسسة ومصمم لمعالجة وإدارة المخاطر بشكل فعال. (International Organization for Standardization, ISO/IEC 27000, 02-2018, p. 11).

"أصول المعلومات" هي أي شيء له قيمة للمؤسسة، تعرف أيضًا باسم سلعة المعلومات. هناك العديد من أنواع الأصول، بما في ذلك: المعلومات، البرمجيات، الأجهزة، الخدمات، الأفراد ومؤهلاتهم، الخبرة والتجربة، والأصول غير الملموسة مثل السمعة والصورة (ISACA, p. 41).

تقدم السلسلة توصيات لتطبيق أفضل الممارسات حول إدارة أمن المعلومات (إدارة مخاطر المعلومات من خلال ضوابط أمن المعلومات) في سياق نظام إدارة أمن المعلومات الشامل (ISMS)، وهو مماثل في التصميم لأنظمة الإدارة لضمان الجودة (سلسلة ISO 9000)، وحماية البيئة (سلسلة ISO 14000) وأنظمة الإدارة الأخرى. هذه السلسلة واسعة النطاق بشكل متعمد، وتغطي أكثر من مجرد الخصوصية والسرية وقضايا تكنولوجيا المعلومات، التقنية، والأمن السيبراني. فهي قابلة للتطبيق على المؤسسات من جميع الأشكال والأحجام. بحيث يتم تشجيع جميع المؤسسات على تقييم مخاطر المعلومات الخاصة بها، ثم معالجتها وفقًا لاحتياجاتها. (International Organization for Standardization , ISO, 2020).

تضم هذه السلسلة عدداً من المعايير، ويبين الشكل 01 سلسلة معايير أمن المعلومات والعلاقات فيما بينها.

2.2.2 المعيار ISO 27005:

يوفر المعيار "إرشادات لإدارة مخاطر أمن المعلومات" ويدعم المفاهيم العامة المحددة في ISO / IEC 27001 وهو مصمم للمساعدة في التنفيذ المرضي لأمن المعلومات على أساس نهج إدارة المخاطر. لا يحدد المعيار أو يوصي أو حتى يسمي أي طريقة معينة لإدارة المخاطر. ومع ذلك، فهي تعني عملية مستمرة تتكون من تسلسل منظم من الأنشطة، وبعضها تكراري. تم نشر الإصدار الثالث من ISO / IEC 27005 في سنة 2018 (Ltd, IsecT, 2020).

يجب تحديد نقاط الضعف التي يمكن استغلالها من خلال التهديدات لإلحاق الضرر بالأصول أو بالمؤسسة. يمكن أن يشمل هذا المجالات التالية: التنظيم، العمليات والإجراءات، إجراءات الإدارة، الموظفون، البيئة المادية، تكوين نظام المعلومات، الأجهزة أو البرامج أو معدات الاتصالات، الاعتماد على أطراف خارجية.

لا يسبب وجود نقاط الضعف ضررًا في حد ذاته، حيث يجب أن يكون هناك تهديد موجود لاستغلالها، لهذا قد لا تتطلب نقاط الضعف الأمنية التي ليس لها تهديد مقابل لها تنفيذ إجراء رقابي، ولكن يجب التعرف عليها ومراقبتها من أجل التغييرات. على العكس من ذلك، فإن التهديد الذي لا يقابله نقطة ضعف أمنية قد لا يؤدي إلى مخاطر (International Organization for Standardization, ISO/IEC 27005:2011(E), p. 15 16).

يظهر الملحق D من المعيار ISO/IEC27005 قائمة تحوي أمثلة على نقاط الضعف والمخاطر المقابلة لها (International Organization for Standardization, ISO/IEC 27005:2011(E), pp. 45-48). هذه القائمة تم استخدامها في الدراسة الميدانية حيث قمنا بصياغة أسئلة الإستبيان إنطلاقا من أمثلة نقاط الضعف الواردة فيها.

يعتبر إجراء تحديد نقاط الضعف مرحلة جزئية من عملية تحديد المخاطر والتي هي بدورها مرحلة أولى في عملية تقييم المخاطر، وكل ذلك يندرج ضمن إدارة مخاطر أمن المعلومات.

3. الدراسة الميدانية:

1.3 الطريقة والأدوات:

في هذا المحور سنحاول إسقاط ما تطرقنا له في الجانب النظري على الدراسة الميدانية باستخدام قائمة استقصاء.

1.1.3 مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة من فئة مستعملي نظام المعلومات المحاسبي في الشركات على المستوى الوطني، أما العينة فقد بلغ عددها 100 فرد، وتحرينا في اختيار أفراد العينة أن يكونوا عاملين في شركات كبيرة تملك نظام معلومات محاسبي إلكتروني مستخدم على نطاق شبكي وطني، وهم موزعون على الشركات التالية: إتصالات الجزائر، بريد الجزائر، الصندوق الوطني للتأمينات الإجتماعية، الصندوق الوطني للمعاشات، شركة توزيع الكهرباء والغاز وسط (سونلغاز). قمنا بتوزيع قائمة الاستقصاء عليهم باعتبارها من أهم الأدوات البحثية الناجعة للتحليل، فكانت عدد الاستمارات الصالحة للتحليل 86 استمارة بنسبة 86% .

2.1.3 الأدوات الإحصائية المستعملة في التحليل:

تم استخدام ليكرت الخماسي المكون من خمس درجات لتحديد أهمية كل فقرة من فقرات الاستبيان، وذلك لقياس استجابات المبحوثين لفقرات الاستبيان، وذلك حسب الجدول 1، كما تم تحديد خمس مستويات للتعليق على المتوسط الحسابي كما هي في الجدول 2.

ومن حيث الأدوات المستعملة في تحليل البيانات فقد تم استعمال برنامج الحزم الإحصائية للعلوم الاجتماعية SPSS لتفريغ البيانات المجمعة ومعالجتها إحصائيا، ومن حيث أسلوب التحليل فقد اعتمدنا الإحصاء الاستدلالي (Alpha Cronbach) لاختبار ثبات وصدق الاستبيان، وعلى مقاييس النزعة المركزية المتمثل في حساب المتوسط الحسابي والانحراف المعياري، ولاختبار الفرضيات تم الإعتماد على معامل الإرتباط بيرسون.

3.1.3 حساب الصدق والثبات للاستبيان:

من خلال الجدول 3 الموضح لاختبار معامل ألفا كرونباخ في صورته النهائية نلاحظ أن معامل ألفا كرونباخ الخاص بالاستبيان كوحدة واحدة يساوي 0.678 وهي تعبر على أن الاستبيان يتميز بالثبات، كما نلاحظ أن معامل ألفا كرونباخ الخاص بكل محور بشكل مستقل مرتفعة فكلها تجاوزت القيمة المقبولة المساوية لـ 0.6، وهذا ما يعني توفر درجة عالية من الثبات الداخلي في الإجابات، مما يمكننا من الاعتماد على هذه الإجابات في تحقيق أهداف الدراسة وتحليل نتائجها.

4. تحليل النتائج:

سنقوم من خلال هذا العنصر بدراسة مدى ثبات الإستبيان، ثم القيام بتحليل نتائج إجابات أفراد عينة الدراسة.

من خلال الجدول 4 يتضح لنا أن نقاط الضعف الأمنية في نظام المعلومات المحاسبي لدى الشركات المعنية هي موجودة بدرجة منخفضة وبشكل معقول. حيث جاءت درجات المتوسط الحسابي لفقرات الإستبيان موزعة كما يلي: 16 بتقدير "ضعيف"، 13 بتقدير "متوسط"، و5 بتقدير "مرتفع". كما نجد أن مستوى المتوسط الحسابي لمحاور الإستبيان الستة هو 2 بتقدير "ضعيف" و3 بتقدير " متوسط"

و 1 بتقدير "مرتفع"، حيث يلاحظ أن المستوى العام لنقاط الضعف الأمنية الذي يتعلق بمحور "الموقع" هو مرتفع وتحديدا فقرة "شبكة الكهرباء غير مستقرة" ما يدل على تقصير الإدارة في توفير الإمكانات المادية المطلوبة لتعزيز أمن نظام المعلومات مثل تجهيز الموقع بنظام إحتياطي للتزويد بالطاقة الكهربائية، كما يلاحظ أن الإنحرافات المعيارية لمحاور الإستبيان ضعيفة ما يدل على تقارب المتوسطات المحاسبية.

توجد علاقة ارتباطية عند مستوى دلالة $\alpha=0.05$ بين أمن نظام المعلومات المحاسبي ونقاط الضعف الأمنية في نظام المعلومات المحاسبي، ونلاحظ من خلال الجدول 5 أن قيمة مستوى الدلالة لمحاور نقاط الضعف الأمنية أقل من 0.05 باستثناء محور "شبكة الإتصال".

وفيما يلي تحليل الفرضيات بالإعتماد على معامل الإرتباط بيرسون انطلاقا من النتائج المبينة في الجدول 5:

الفرضيتان الأولى والثانية: قيمة معامل الإرتباط المحسوبة للمتغير المستقل "المعدات" (0.304-) سالبة، مما يشير إلى وجود علاقة ارتباط عكسية بينها وبين المتغير التابع "أمن نظام المعلومات المحاسبي"، وعليه فإن الفرضيتان الأولى والثانية صحيحتان، أي أن " حالة العناصر المادية الداعمة للعمليات لها تأثير نسبي على أمن نظام المعلومات المحاسبي "، و " نوعية البرامج التي تساهم في تشغيل مجموعة معالجة البيانات لها تأثير نسبي على أمن نظام المعلومات المحاسبي".

الفرضية الثالثة: قيمة معامل الإرتباط المحسوبة للمتغير المستقل "شبكة الإتصال" (0.559-) سالبة، مما يشير إلى وجود علاقة ارتباط عكسية بينها وبين المتغير التابع "أمن نظام المعلومات المحاسبي"، وعليه فإن الفرضية الثالثة صحيحة، أي أن " نوعية البرامج التي تساهم في تشغيل مجموعة معالجة البيانات لها تأثير نسبي على أمن نظام المعلومات المحاسبي ".

الفرضية الرابعة: قيمة معامل الإرتباط المحسوبة للمتغير المستقل "الموظفون" (0.484-) سالبة، مما يشير إلى وجود علاقة ارتباط عكسية بينها وبين المتغير التابع "أمن نظام المعلومات المحاسبي"، وعليه فإن الفرضية الرابعة صحيحة، أي أن " أجهزة الاتصالات السلكية واللاسلكية المستخدمة لربط أجهزة الكمبيوتر البعيدة فعليًا أو لربط عناصر نظام المعلومات لها تأثير نسبي على أمن نظام المعلومات المحاسبي ".

الفرضية الخامسة: قيمة معامل الإرتباط المحسوبة للمتغير المستقل "الموقع" (0.764-) سالبة، مما يشير إلى وجود علاقة ارتباط عكسية بينها وبين المتغير التابع "أمن نظام المعلومات المحاسبي"، وعليه فإن الفرضية الخامسة صحيحة، أي أن " مجموع الأشخاص المشاركين في نظام المعلومات لهم تأثير نسبي على أمن نظام المعلومات المحاسبي "

الفرضية السادسة: قيمة معامل الإرتباط المحسوبة للمتغير المستقل "الإدارة" (0.564-) سالبة، مما يشير إلى وجود علاقة ارتباط عكسية بينها وبين المتغير التابع "أمن نظام المعلومات المحاسبي"، وعليه

فإن الفرضية السادسة صحيحة، أي أن " حالة الأماكن التي تحتوي على نطاق نظام المعلومات أو جزء منه والوسائل المادية اللازمة لتشغيله لها تأثير نسبي على أمن نظام المعلومات المحاسبي ".

5. خاتمة:

عالجت هذه الدراسة أحد المواضيع المهمة في مجال المحاسبة، ويتعلق الأمر بـ: " أمن نظام المعلومات المحاسبي في ضوء المعيار الدولي ISO 27005 دراسة ميدانية على عدد من الشركات الجزائرية "، حيث تم من خلالها طرح الإشكالية الآتية " ما حجم نقاط الضعف الأمنية في نظام المعلومات المحاسبي بالشركات الجزائرية؟ وبعد عرض الجانب النظري، تم القيام بالدراسة الميدانية من خلال توزيع الإستبيان على عينة من مستخدمي نظام المعلومات المحاسبي لمعرفة آرائهم والخروج بنتائج، ومن خلال تلك النتائج يتم تقديم التوصيات اللازمة لتقويم نقاط الضعف ودعم نقاط القوة.

بعد التطرق لمختلف عناصر هذه الدراسة، تم الخروج بمجموعة من النتائج يمكن تلخيصها في النقاط الموالية كما يلي:

- الأخطاء غير المتعمدة هي أقل حدوثا وأقل ضررا على أمن نظام المعلومات المحاسبي، حيث أن العنصر البشري يمتلك الكفاءة المطلوبة للتعامل مع التكنولوجيا المستخدمة ضمن النظام؛
- تفتقر شبكات الإتصال إلى المزيد من إجراءات الحماية وخصوصا فيما يتعلق بعمليات نقل المعلومات عبر الشبكة وتحديد الهويات؛
- تفتقر مواقع عمل أفراد العينة إلى مخططات أمنية أكثر صرامة وكذلك إلى توفير نظم إحتياطية للتزويد بالكهرباء لتفادي مشكلة الإنقطاعات؛
- قصور رقابي في جانب توزيع مسؤوليات الولوج إلى برمجيات نظام المعلومات المحاسبي وغياب إجراءات رسمية تنظم عمليات منح وإلغاء الولوج؛
- علاقة إرتباطية عكسية بين أمن نظام المعلومات المحاسبي ونقاط الضعف الأمني فيه، تؤكد إلزامية العمل على معالجة نقاط الضعف من أجل رفع مستوى أمن نظام المعلومات المحاسبي ليرقى إلى تلبية متطلبات مواصفات الأيزو.

بناء على النتائج التي تم التوصل إليها من خلال هذه الدراسة يمكن أن نقترح التوصيات التالية:

- ضرورة وجود خطط ووسائل حماية أمنية شاملة لنظام المعلومات المحاسبي وخاصة لاجتناب المخاطر الناتجة عن تصرفات متعمدة؛
- إجراء عملية تقييم منتظمة لأمن نظام المعلومات المحاسبي لفحص واختبار التغير في نقاط الضعف والمخاطر المرتبطة بها؛
- الحرص على التحكم في مراقبة الولوج إلى مواقع توفر نظام المعلومات المحاسبي وتحديد مسؤوليات الولوج إلى البرمجيات؛

- توفير شبكة إتصال مؤمنة لحماية تبادل المعلومات المحاسبية وتفعيل تسجيل الهوية عند الولوج إلى الشبكة؛
- تهيئة الموقع بالتجهيزات التي من شأنها حماية المعدات من العطل وحماية حفظ البيانات؛
- بشكل عام، ينبغي على الشركات الجزائرية العمل على معالجة مختلف نقاط الضعف في أمن نظام المعلومات المحاسبي كخطوة نحو الحصول على شهادة الأيزو في إدارة أمن المعلومات.

6. قائمة المراجع:

المؤلفات:

بن سليمان الغثبر خالد، و بن عبد الله القحطاني محمد، (2009)، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية، الرياض.

حسن طاهر داوود، (2000)، الحاسب و أمن المعلومات، معهد الإدارة العامة، الرياض.

عبد الرزاق محمد قاسم، (2008)، نظم المعلومات المحوسبة، دار الثقافة للنشر والتوزيع، عمان.

عبد الله الحميدي نجم، (2005)، نظم المعلومات الإدارية (مدخل معاصر)، دار وائل للنشر، عمان.

Denisi, A, & Griffin, R,(2010), Human Resource Management, Houghton Miflin Company edition, Boston.

Dyrieux, A, (2004), Le système d'information, edition MAXIMA,Paris.

Romney, M & Steinbart, P, (2006), Accounting Information Systems, Pearson Prentice Hall, New Jersey.

Whitman, M, & Mattod , H, (2011), Principles of Information Security , cengage learning/course technology, Boston.

المقالات:

عبد الكريم سعد، و علي حنان، (2011)، مخاطر استخدام تكنولوجيا المعلومات و أثرها على نظم المعلومات المحاسبية، مجلة دراسات المعلومات، (11)، صفحة 226-228.

عبد المنعم مبارك صلاح الدين، و الرفاعي لطفي،(1996)، نظم المعلومات المحاسبية مدخل رقابي، الجمعية السعودية للمحاسبة، (9)، صفحة 79.

عصام محمد البحيصي، و حرية شعبان الشريف،(2008)، مخاطر نظم المعلومات المحاسبيةالالكترونية. مجلة الجامعة الاسلامية، (2)، صفحة 905.

لمين علوطي، (2008)، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، مجلة علوم إنسانية، (38)، صفحة 2.

Abu-Musa, A, (2004), Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations. Public Administration, vol 44, (3), page 5.

Ball, K, (2011), The Use of Human Resource Information Systems Survey. Personnel Review, vol 30, (5-6), page 677.

مواقع الانترنيت:

International Organization for Standardization (2020), Publicly Available Standards .https://standards.iso.org/ittf/PubliclyAvailableStandards (consulté le 30/08/2020).

Ltd, IsecT (2020), ISO/IEC 27005:2018, https://www.iso27001security.com/html/27005.html, (consulté le 02/09/2020).

7. ملاحق :

الجدول 1: درجات إجابة المبحوثين

الاستجابة	دائما	غالبا	أحيانا	نادرا	أبدا
	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
الدرجة	5	4	3	2	1

المصدر: من إعداد الباحثين

الجدول 2: مستويات المتوسط الحسابي

المتوسط الحسابي	من 1 الى1.79	من 1.80 الى2.59	من 2.6 الى3.39	من 3.4 الى4.19	من 4.2 الى5
المستوى	ضعيف جدا	ضعيف	متوسط	مرتفع	مرتفع جدا

المصدر: من إعداد الباحثين

الجدول 3: حساب ألفا كرونباخ

البيان	عدد الفقرات	معامل ألفا

		كرونباخ
المحور الأول: أمن نظام المعلومات المحاسبي	5	0.663
المحور الثاني: المعدات	13	0.688
المحور الثالث: شبكة الاتصال	6	0.641
المحور الرابع: الموظفون	5	0.740
المحور الخامس: الموقع	2	0.674
المحور السادس: الإدارة	3	0.647
الإستبيان الكلي	**34**	**0.675**

المصدر: من إعداد الباحثين

الجدول 4: المتوسط الحسابي والإنحراف المعياري لإجابات عينة الدراسة

الرقم	الفقرة	المتوسط الحسابي	الإنحراف المعياري	المستوى
1	السرية: نظام المعلومات المحاسبي يشتمل على كل التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة أو السرية	2,6047	0,42481	متوسط
2	السلامة: المعلومات لا تتعرض لعمليات غير مشروعة بصفة متعمدة	2,5465	0,44432	ضعيف
3	السلامة المعلومات لا تتعرض لعمليات غير مشروعة بصفة غير متعمدة	3,4884	0,41208	مرتفع
4	الوفرة: كل من يحق له الإطلاع على المعلومات يمكنه الوصول إليها	2,6047	0,55131	متوسط
5	الوفرة: من يحق له الإطلاع على المعلومات يمكنه الوصول إليها في التوقيت المناسب	2,6512	0,29039	متوسط
أمن نظام المعلومات المحاسبي		2,7791	0,42458	متوسط
6	الصيانة غير كافية	2,1628	0,32657	ضعيف
7	تخزين البيانات غير محمي	2,3256	0,25623	ضعيف
8	نسخ البيانات غير مراقب	2,0814	0,22653	ضعيف

9	توجد عيوب معروفة في البرنامج	2,7442	0,19031	متوسط
10	لا يوجد "تسجيل الخروج" عند مغادرة مكان العمل	2,1279	0,19552	ضعيف
11	يوجد تخصيص خاطئ لحقوق الولوج	2,7326	0,37044	متوسط
12	واجهة المستخدم معقدة	2,5465	0,12209	ضعيف
13	التواريخ غير صحيحة	2,9186	0,60107	متوسط
14	آليات ضعيفة في تحديد الهوية والمصادقة	2,1628	0,27289	ضعيف
15	إدارة كلمات المرور ضعيفة	2,5930	0,40046	متوسط
16	البرنامج غير ناضج أو جديد	2,4070	0,31518	ضعيف
17	لا يوجد رقابة فعالة على عمليات التعديل	2,7209	0,33176	متوسط
18	لا يوجد نسخ احتياطية	2,2442	0,17014	ضعيف
المعدات		2,4436	0.21378	ضعيف
19	لا يوجد دليل على إرسال أو استلام رسالة	3,5930	0,06048	مرتفع
20	خطوط الاتصال غير محمية	3,3372	0,98996	متوسط
21	كابلات مشتركة ضعيفة	2,6395	0,31002	متوسط
22	عدم تحديد هوية ومصادقة المرسل أوالمستقبل	3,6279	0,34133	مرتفع
23	بنية الشبكة غير آمنة	2,4070	0,16334	ضعيف
24	نقل كلمات المرور مكشوف	2,4884	0,17241	ضعيف
شبكة الاتصال		3,0155	0.17292	متوسط
25	تدريب أمني غير كافٍ	2,3488	0,24072	ضعيف
26	الاستخدام غير صحيح للبرامج والأجهزة	2,3023	0,97099	ضعيف
27	الوعي الأمني قليل	2,2326	0,16422	ضعيف
28	لا يوجد آليات للرقابة على الموظفين	3,0814	0,33566	متوسط
29	لا يوجد سياسات للاستخدام الصحيح لوسائل الاتصالات السلكية واللاسلكية والبريد الإلكتروني	2,6395	0,96795	متوسط
الموظفون		2,5209	0.13591	ضعيف

30	التقصير أو الإهمال في مراقبة الوصول إلى المباني والغرف	3,3488	0,13934	متوسط
31	شبكة الكهرباء غير مستقرة	3,9302	0,14526	مرتفع
الموقع		3,6395	0.14230	مرتفع
32	لا يوجد إجراءات رسمية بخصوص تسجيل المستخدم وإلغاء التسجيل	3,8605	0,15839	مرتفع
33	لا يوجد تقارير حدوث أخطاء	2,4651	0,28060	ضعيف
34	لا يوجد إجراءات خاصة بسرية التعامل مع المعلومات	2,2558	0,31663	ضعيف
الإدارة		2,8605	0.25187	متوسط

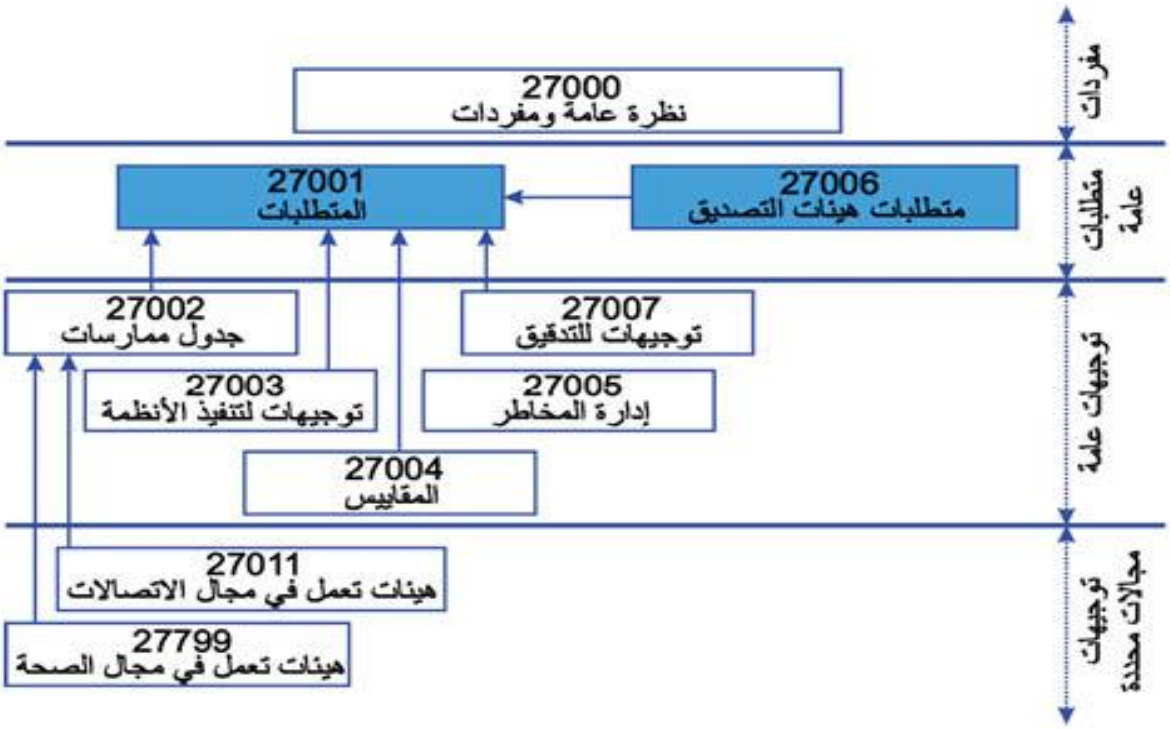
المصدر: من إعداد الباحثين بالإعتماد على spss v25

الجدول 5: يبين معامل الإرتباط بين أمن نظام المعلومات المحاسبي ونقاط الضعف الأمنية

		المعدات	شبكة الاتصال	الموظفون	الموقع	الإدارة
أمن نظام المعلومات المحاسبي	معامل الإرتباط بيرسون	−0.304	−0.559	−0.484	−0.764	−0.564
	مستوى الدلالة	0.026	0.070	0.015	0.000	0.029

المصدر: من إعداد الباحثين بالإعتماد على spss v25

الشكل 1: العلاقة بين معايير السلسلة 27000



المصدر: الموسوعة العربية، الهندسة المعلوماتية أمن المعلومات – معايير–
(consulté le 02/09/2020).http://arab-ency.com.sy/tech/detail/168898