أثر نظام الحماية الالكتروني في الحد من مخاطر تكنولوجيا المعلومات والاتصال
دراسة مقارنة لعينة من المؤسسات

الطاهر بن عمارة [*1] خالد رجم[2] العربي عطية[3]

1. جامعة ورقلة، الجزائر
2. جامعة ورقلة، الجزائر
3. جامعة ورقلة، الجزائر

The impact of the electronic protection system in reducing the risks of information and communication technology, a comparative study of a sample of institutions

Ben amara Taher & REDJEM Khaled & ATIA Larbi

OUARGLA University –Algeria

تاريخ الاستلام: 2018/09/24 **تاريخ المراجعة:** 2018/10/06 **تاريخ القبول:** 2018/11/08

ملخص:

هدفت هذه الدراسة الى تقييم مدى مساهمة نظام الحماية الكتروني في الحد من مخاطر تكنولوجيا المعلومات و الاتصال دراسة مقارنة لعينة من المؤسسات في ولاية ورقلة، حيث تم الاعتماد على المنهج الوصفي باستخدام كل من أداة المقابلة و الاستبيان حيث تمثلت عينة الدراسة في ثلاثة مؤسسات اتصالات الجزائر ،سونلغاز، ليند غاز، بمجمل 228 استبيان موجه إلى مسيري و مستخدمي تكنولوجيا المعلومات والاتصال في المؤسسة، وكانت نسبة الاستجابة 97% ،كما تم الاعتماد في تحليل البيانات الاستبانة على برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS و كانت أهم النتائج المتوصل إليها هي : تتعرض المؤسسات إلى عدة مخاطر تهدد أمن نظم المعلومات الإلكترونية، فاعلية السياسات الأمنية و ضوابط للموظفين داخل المؤسسة من شأنه ضمان الحد من مخاطر استخدام تكنولوجيا المعلومات والاتصال بالإضافة الى أن عملية التكوين في مجال الأمن الكتروني في المؤسسات به عدة اختلالات ونقائص انطلاقا من تحديد الاحتياجات التكوين في حد ذاته، وأخيرا ليزال موظفي المؤسسات محل الدراسة يعانون من نقص على مستوى الثقافة التكنولوجية، اضافة الى عدم وجود صرامة بشأن احترام القواعد واللوائح القانونية المتعلقة بنظام الأمن الالكتروني.

الكلمات المفتاحية: تكنولوجيا المعلومات والاتصال، نظام الحماية الالكتروني، سياسات الأمنية، مخاطر تكنولوجيا المعلومات والاتصال.

تصنيف JEL : M15

Abstract:

The aim of this study is to assess the extent to which the electronic protection system contributes to the reduction of information and communication technology risks with a comparative study of a sample of institutions in the state of Ouargla. The present study relied on the descriptive method using both the interview tool and the questionnaire. The study sample was consisted of three institutions Algeria Telecom, Sonelgaz, and Lindh Gas, in which 228 questionnaires were addressed to the information and communication technology managers and users in these institutions, and the response rate was 97%. The analysis of the questionnaire data was also based on the SPSS program and the most important results are: firstly, the institutions are exposed to several risks threaten the security of the electronic information systems. Then, the effectiveness of security policies and the controls of staff within the institution will ensure the reduction of the risk of the information and communication technology use; in addition, the process of training in the field of electronic security in the institutions has several imbalances and imperfections from the needs identification of the formation itself. Finally, the staff of the institutions concerned are still deficient in the level of technological culture, in addition to the lack of rigor regarding respect of the rules and regulations concerning the electronic security system.

Keywords: Information and communication technology, information systems security, security policies, information and communication technology risks.

(JEL) Classification: M15

* **المؤلف المرسل: الإيميل:** tahaer.benamara@gmail.com

DOI : 10.12816/0052776

I- تمهيد:

ان استخدام تكنولوجيا المعلومات والاتصال وفر الكثير من الوقت والجهد للعاملين، إلى أنه أدى إلى زيادة مخاطر أنظمة المعلومات، من هنا كان على المؤسسات أن تشدد من إجراءاتها الأمنية لحماية أنظمتها المعلوماتية، ومن هذا المنطلق سعت المؤسسات إلى تصميم وبناء نظام حماية إلكتروني للحد من مختلف المخاطر المحيطة بنظام المعلومات المتمثلة في مخاطر تتعلق بالأفراد، اخرى تتعلق هجمات الكترونية من طرف قراصنة، وصولى الى مخاطر تتعلق بمراحل النظام، بناءا عليه يمكن صياغة الاشكالية الاتية:

ما مدى فعالية نظام الحماية الالكتروني في الحد من مخاطر تكنولوجيا المعلومات والاتصال في عينة الدراسة؟

1. فرضيات الدراسة:

- تتميز نظم المعلومات في عينة الدراسة بالكفاءة من خلال المكونات (المادية والبرمجيات).
- لدى المؤسسات محل الدراسة نظام امن الكتروني يشمل كل عناصر الأمن الالكتروني لحماية أنظمتها من كل أنواع الاختراق.
- تحيط بأنظمة معلومات المؤسسات محل الدراسة مجموعة من المخاطر تتعلق بإدخال البيانات، والتشغيل ومخاطر تتعلق بالمخرجات وأخرى ذات علاقة بالبيئة.
- هناك تفاوت في فعالية نظام الحماية الالكتروني في الحد من ا لمخاطر بين المؤسسات محل الدراسة، مرتبطة بقلة الخبرة والوعي بالأمن الإلكتروني لدى موظفي المؤسسة بالإضافة إلى عدم الاعتماد على سياسات واضحة وصرامة في تطبيق الإجراءات الرقابية والالتزام باللوائح القانونية من طرف إدارة المؤسسة.

2. الدراسات السابقة:

- دراسة (أيمن محمد فارس الدنف 2013) بعنوان: "واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها" وهدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، وأستخدم الباحث المنهج البحثي الوصفي التحليلي، وتكون مجتمع الدراسة من العاملين على نظم المعلومات في الكليات التقنية وجمعت أدوات الدراسة بين الاستبانة والمقابلة ، وتوصلت الدراسة إلى مجموعة من النتائج أهمها، أن تتوفر البنية التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة، وأن تدرك الإدارات العليا للكليات التقنية أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة،تتفاوت الكليات التقنية مجتمع الدراسة في درجات استخدام تعهد نظم معلوماتها،وان توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة.
- دراسة (حرية شعبان محمد الشريف 2006) بعنوان "مخاطر نظم المعلومات المحاسبية الإلكترونية دراسة تطبيقية على المصارف العاملة في قطاع غزة" تهدف هذه الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر حيث استعانت الباحثة بما تناولته الدراسات السابقة والأبحاث التي اهتمت في هذا المجال، كذلك تم التعرف على الإجراءات والوسائل الرقابية المتبعة من قبل المصارف العاملة في قطاع غزة لمواجهة تلك المخاطر التي قد تواجه نظم معلوماتها المحاسبية الالكترونية وبناء على ذلك تم استخلاص بعض النتائج التي تسهم في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية

DOI : 10.12816/0052776

الالكترونية في المصارف العاملة في قطاع غزة، وتقديم التوصيات في هذا المجال كما استخدمت الدراسة المنهج الوصفي التحليلي في الوصول لنتائج الدراسة، حيث تم توزيع استبانه على المصارف العاملة في قطاع غزة وفروعها وقد تم استخدام برنامج التحليل الإحصائي(SPSS) للعلوم الإنسانية والاجتماعية لمعالجة البيانات باستخدام التكرارات والنسب المئوية، والمتوسطات الحسابية، واختبار الإشارة إلي معلمي (Sign Test)وقد تم التوصل إلى مجموعة من النتائج أهمها ،أوضحت الدراسة قلة عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة حيث يعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفين المختصين يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية ، وأن الإدارة الجيدة تستطيع أن تقلل أو تحد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف ، وأن تطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية.

3. تكنولوجيا المعلومات و الاتصال: TIC : تم تعريفها و النظر إليها على أنها كل ما ترتب على الاندماج بين تكنولوجيا الحاسب الالكتروني و التكنولوجيا السلكية واللاسلكية و الالكترونيات الدقيقة و الوسائط المتعددة من أشكال جديدة لتكنولوجيا ذات قدرات فائقة على إنتاج المعلومات و جمعها و تخزينها و معالجتها و نشرها و استرجاعها، بأسلوب غير مسبوق يعتمد على مجموعة من مؤثرات الاتصال التفاعلي الجماهيري و الشخصي معا ،أي هي مجموعة التكنولوجيات المستخدمة في معالجة وتحرير وتبادل المعلومات، و أكثر تحديداً البيانات الرقمية، و ظهور تكنولوجيا المعلومات والاتصالات يرجع أساسا إلى التقارب و المزج الذي تم بين المعلوماتية والاتصالات السلكية و اللاسلكية، و السمعي البصري[1].

4. نظام المعلومات الالكتروني: يمكن تعريف نظام معلومات فنيا كمجموعة من المكونات المترابطة تهدف إلى جمع ومعالجة وتخزين وتوزيع المعلومات لدعم القرار والتحكم في المنظمة وبالإضافة إلى دعم عملية صنع القرار، التنسيق، والسيطرة، فان نظم المعلومات تساعد أيضا الإدارة العليا على تحليل المشاكل والموضوعات المعقدة.[2]

5. نظام الحماية الالكتروني (الامن الالكتروني): أمن نظام المعلومات هو جميع الطرق والتقنيات ووسائل الأمن والحماية لموارد نظام المعلومات، ويمثل الهدف من أي برنامج امن يعد لنظام المعلومات حماية المنظمة وذلك بتقليل المخاطر التي تؤثر على توافر المعلومات وسريتها وسلامتها بمستوى مقبول ومحدد[3]، وعليه يجب على المؤسسة وضع قواعد السلامة وإتباع السياسات الأمنية وفق المعايير المتعارف عليها لضمان السير السليم للنظام[4]، وينبغي ان يتضمن التخطيط والرقابة الإدارية على امن النظام ما يلي[5]:

- تحديد الأهداف والتي تعتبر بمثابة معايير لتقييم امن النظام فيما بعد، وتتمثل هذه الأهداف في حماية مكونات النظام؛
- تقدير الاحتمالات والتكاليف المرتبطة بمخاطر امن تشغيل البيانات؛
- إعداد خطة تضمن مستوى مقبولا من الأمن وبتكلفة معقولة، وتصف هذه الخطة كافة الإجراءات الرقابية التي سيتم تطبيقها وأهداف هذه الإجراءات، هذا وينبغي إن يتم فحص الخطة والتصديق عليها قبل وضعها موضع التنفيذ؛
- تحديد المسؤوليات عن امن النظام؛

DOI : 10.12816/0052776

- اختبار إجراءات الرقابة على امن النظام، وذلك للتحقق من مدى فعاليتها في تحقيق أهدافها المرجوة.

6. عناصر الأمن الالكتروني: من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنفت تلك العناصر إلى خمسة عناصر وهي[6]:

- **التحقق من المستعمل:** التأكد من هوية الشخص الذي يستخدم المعلومات، عن طريق فحص الصلاحيات الالكترونية لكل مستخدم.
- **سلامة المحتوى:** أي التأكد من أن محتوى المعلومات صحيح ولم يحرف، ولتفادي ذلك يجب على المؤسسة تأمين سلامة المحتوى من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات والفيروسات.
- **استمرارية توفر المعلومات أو الخدمة:** سلامة وامن التخزين والاسترجاع تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل وتقديم الخدمات لمستخدمين المرخص لهم بها، ومنع استخدامها أو الوصول إليها بطرق غير مشروعة.
- **المسؤولية:** إمكانية تتبع الأثر في حالات التغيير والتحريف والحذف. ويقصد به ضمان توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص في وقت معين.
- **السرية أو الموثوقية:** أي التأكد من أن المعلومات لا يمكن الاطلاع عليها من قبل أشخاص غير مصرح لهم.

7. متطلبات أمن نظم المعلومات: تعتبر مسألة حماية أمن نظم المعلومات من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات:[7]

- وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المنشأة؛
- يجب على الإدارة العليا في المنشأة دعم أمن نظم المعلومات لديها؛
- يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين؛
- تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة؛
- تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية؛
- الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن؛
- تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط؛
- تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

8. مخاطر نظام المعلومات الالكتروني: وتعرف مخاطر تكنولوجيا المعلومات بصفة خاصة على أنها " كل ما ينتج عنه وجود خطأ أو خلل في تكنولوجيا المعلومات تؤدي إلى تأثير سلبي على أعمال المنظمة، ولقد جاء تعريف جمعية مراجعة ومراقبة نظم المعلومات ISACA لمخاطر نظم المعلومات متسقاً مع ما سبق، وعرفتها على أنها:

DOI : 10.12816/0052776

" احتمال حدوث تصرف ما أو حدث ما له تأثير سلبي على المنظمة وعلى نظم المعلومات الخاصة بها ، أي احتمال أن يحدث استغلال لنقاط الضعف في الأصل أو مجموعة من الأصول فيسبب خسائر أو أضرار للأصول "[8]

ويتطلب الكشف عن الأبعاد المختلفة لمخاطر نظم المعلومات تناول المقومات الأساسية لأي نظام معلومات وهي:[9]

- **الأفراد:** وهم الذين يقومون بتشغيل النظام، وأداء الوظائف المختلفة.
- **الإجراءات:** تتضمن تلك الإجراءات سواء في النظام اليدوي أو النظام الآلي تجميع وتشغيل وتخزين البيانات عن أنشطة المنظمة.
- **البيانات :** وهي تتعلق بالعمليات التي تقوم بها المنظمة.
- **البرامج :** وهي التي تستخدم في تشغيل بيانات النظام.
- **البنية التحتية لتكنولوجيا المعلومات** : وهي تشمل أجهزة الكمبيوتر، وملحقاتها، ووسائل اتصالات الشبكات.

وتتسم أسباب مخاطر تكنولوجيا المعلومات والآثار الناتجة عنها بالتعقيد، وبصفة خاصة في المنظمات كبيرة الحجم، ويمكن تقسيم أسباب مخاطر تكنولوجيا المعلومات إلى أسباب خارجية وأسباب داخلية بالإضافة إلى مخاطر ناتجة عن مراحل النظام مثل مخاطر المدخلات، مخاطر التشغيل، مخاطر المخرجات.[10]

II ـ الطريقة والأدوات :

1. **عينة وأدوات الدراسة**: تتمثل عينة الدراسة في مستخدمي ومسيري نظام المعلومات في المؤسسات الثلاث (اتصالات الجزائر، سونلغاز، ليند غاز)، اذ اعتمدنا على المقابلة مع مسيري ومهندسي نظام المعلومات، اضافة الى توزيع استبيان على عينة من مستخدمي نظام المعلومات قدرت بـ 228 مستخدم في المؤسسات الثلاث.

ولقد تم تقسيم الاستبيان الى:

- **المحور الأول: المعلومات العامة:** ويتضمن المعلومات الشخصية والمتكون من 08 فقرات
- **المحور الثاني. مخاطر نظم المعلومات:** ويتضمن المخاطر المتعلقة بالمكونات والعناصر نظم المعلومات ويحتوي على 14 فقرة اذ اعتمدنا على المقياس " **لم يحدث أبدا " "أحيانا " "يحدث دائما".**
- **المحور الثالث: نظام الأمن الكتروني في المؤسسة:** وتم تقسيمه إلى ثلاثة الأبعاد: **البعد الأول** السياسات والإجراءات يحتوي على 11 فقرة، أما **البعد الثاني** إجراءات امن المعلومات المتعلقة بالعاملين يحتوي على 7 فقرات، وتكون **البعد الثالث** إجراءات امن المعلومات المتعلقة بالعتاد والبيانات ويحتوي على 10 فقرات وأما بالنسبة للإجابات على فقرات هذا المحور **"غير موافق" محايد" " موافق".**

DOI : 10.12816/0052776

III. النتائج ومناقشتها :

1. ثبات الدراسة: وفق الجدول رقم (01) تبين القيم المتحصل عليها على ثبات الأداة، وكانت قيمة الفا كرونباخ الاجمالي 0,86، حيث قدر الفا لمؤسسة اتصالات الجزائر 0,920 ، سونلغاز 0,878 وتأتي ليند غاز بقيمة 0,782.

2. نتائج اجابات العينة للمحور الثاني: مخاطر نظم المعلومات

1.2. بالنسبة لمؤسسة سونلغاز: وفقا للجدول رقم (02) يمكن تلخيص التعليق وفق مايلي:

- كانت العبارة الأولى التي تنص على " الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين " أكثر العبارات "أحيانا " من طرف العينة، إذا سجل 67,5 بالمائة ومتوسط المرجح 1,88 اذ يتفقون على أن المؤسسة تعاني من مشكل الإدخال غير المتعمد (غير المقصود) بواسطة الموظفين و أصبح يؤرق الادارة اذ يتسبب في عدة اختلالات وكثير من الأحيان يصعب اكتشافه.

- كانت عبارة السادسة التي تنص على " المرور غير الشرعي (غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة" أكثر العبارات "لم يحدث أبدا "، إذا سجل 87,8 بالمائة ومتوسط المرجح 1,29.

- كانت العبارة السابعة التي تنص على " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات" أكثر العبارات " يحدث دائما "، إذا سجل نسبة 41,3 بالمائة وهذا دليل على إن المؤسسة وإفرادها يتفقون أن الأجهزة تتعرض دائما إلى الفيروسات بطريقة او بأخرى.

2.2. بالنسبة لمؤسسة اتصالات الجزائر: وفقا للجدول رقم (02) يمكن تلخيص التعليق وفق مايلي:

- إن العبارة الأولى التي تنص على " الإدخال غير المتعمد (غير المقصود)للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "أحيانا " من طرف العينة، إذا سجل نسبة 80,8 بالمائة ومتوسط المرجح 1,91 وكان الانحراف المعياري 0,430 ويتفقون على إن المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود)للبيانات بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه مثل مؤسسة سابقة .

- العبارة السادسة التي تنص على " المرور غير الشرعي (غير المرخص به)للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة" أقل العبارات "أحيانا " من طرف العينة، إذا سجل نسبة 20,8 بالمائة، وعليه أفراد العينة يتفقون على أن المؤسسة لا يوجد بها مخطر المرور غير شرعي للبيانات أو النظام من خارج المؤسسة.

- وكانت العبارة السابعة التي تنص على " تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات" أكثر العبارات " يحدث دائما " من طرف العينة، إذا سجل نسبة 70 بالمائة بمتوسط حسابي 2.17 وهذا دليل على أن المؤسسة تتعرض أجهزتها وبرامجها دائما إلى الفيروسات وهذا من شانه يرفع من حدوث مخاطر نظم المعلومات.

- إن العبارة العاشرة التي تنص على " سرقة البيانات / المعلومات." أكثر العبارات "لم يحدث أبدا " من طرف العينة، إذا سجل نسبة 65,8 بالمائة ومتوسط المرجح 1,42 يبرهن أن أفراد العينة يتفقون على أن المؤسسة لا تتعرض لسرقة البيانات والمعلومات لا من داخل أو خارج المؤسسة.

3.2 بالنسبة لمؤسسة ليند غاز: وفقا للجدول رقم (03) يمكن تلخيص التعليق وفق مايلي:

- بالنسبة العبارة الأولى التي تنص على " الإدخال غير المتعمد (غير المقصود)للبيانات غير سليمة بواسطة الموظفين" أكثر العبارات "أحيانا " من طرف العينة، إذا سجل ما نسبته 72,2 بالمائة ويتفقون على إن المؤسسة تعاني من

DOI : 10.12816/0052776

الإدخال غير المتعمد (غير المقصود)للبيانات بواسطة الموظفين ، ويوجد السؤال رقم أربعة عشرة الذي ينص على "تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية "بالنسبة 66,7 وثم السؤال الثالث و ينص "التدمير غير المتعمد(الحذف) للبيانات بواسطة الموظفين" بالنسبة 61,1.

- بالنسبة العبارة الرابعة التي تنص على " التدمير **المتعمد** (الحذف) للبيانات بواسطة الموظفين " والسؤال السادس "المرور غير الشرعي (غير المرخص به) للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة" أقل العبارات "أحيانا " من طرف العينة ، إذا سجل نسبة 5,6 بالمائة تصريح واضح من العينة أقل وقوع ولم يحدث أبدا .
- بالنسبة للعبارة السادسة إلى غاية أخر عبارة في الاستبيان اتفق كل المستجوبين أن" يحدث دائما " أقل النسبة 0 بالمائة وهذا يفسر أن المؤسسة لا تواجه إي نوع من المخاطر التي تم ذكرها في الاستبيان.

3. نتائج اجابات العينة بالنسبة للمحور الثالث: نظام الامن الالكتروني

1.3. نتائج البعد الأول: السياسات والإجراءات الأمنية

1.1.3 بالنسبة لمؤسسة سونلغاز: وفقا للجداول رقم (03،04،05) يمكن تلخيص التعليق وفق مايلي:

- كانت نتائج السؤال الثامن (أنظر جدول 03) الذي ينص على" يتم تجديد العتاد دوريا" حصل على اتفاق العينة بالنسبة 40 في المائة على عبارة "غير موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 1,95 وهذا دليل على إن المؤسسة تحتفظ بالعتاد لفترة يعتبرها الأفراد طويلة.
- كانت نتائج السؤال الثالث عشر (أنظر جدول 04) الذي ينص على" تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة " حصل على اتفاق العينة بالنسبة 31,3 في المائة على عبارة "غير موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,01.
- كانت نتائج السؤال العشرون (انظر جدول رقم 05) الذي ينص على" يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها" حصل على نسبة 42,5 في المائة بمتوسط المرجح 1,91 وهذا دليل على عدم وجود البديل لطاقة وهذا تم إثباته في المقابلة مع رئيس المصلحة المعلوماتية.
- وتحصلت العبارة السادسة عشر في البعد الثاني (انظر الجدول رقم 04) بنص "هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات" بالنسبة 43,8 لمتوسط الحسابي بالقيمة 2,06 يعني أن المؤسسة تضع سجل رقابي على حوادث أمن المعلومات كما ثبت في المقابلة.
- نلاحظ أن السؤال الحادي عشر في البعد الثاني (تنظر الجدول رقم03) الذي ينص على" تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها " حصل على اتفاق العينة بالنسبة 72,5 في المائة على عبارة "موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,55 وهذا ما أثبتناه بالمقابلة.
- وتحصل السؤال الثامن عشر في البعد الثاني (انظر الجدول رقم 04) بنص " لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا " بالنسبة 61,3 لمتوسط الحسابي بالقيمة 2,48 يعني أن المؤسسة تخول صلاحيات لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا.
- كما تحصلت عباراتي الواحد وعشرون و الخمسة والعشرون (انظر الجدول رقم 05) على التوالي" يمنع الموظف الغير المختص من أجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات " و" توفر الأنظمة المستخدمة

DOI : 10.12816/0052776

خدمة النسخ الاحتياطي للبيانات و في مكان امن" على اكبر نسبة في البعد الثالث (انظر الجدول رقم 05) 58,8 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة على التوالي 2,40 و2,42 بالانحراف معياري مقدر على التوالي 0,789 و 0,759 هذه نتيجتين جيدة لهذا البعد والذي شملت النسخ الاحتياطية و عدم إجراء تعديلات في المكونات المادية في نظم المعلومات وهذا من شانه تقليل المخاطر المترتبة عنه.

- بالنسبة للسؤال العشرون (انظر الجدول رقم 05) الذي ينص على" يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها." حصل على نسبة 42,5 في المائة بمتوسط المرجح 1,91 وانحراف معياري 0,789 وهذا دليل على عدم وجود البديل لطاقة وهذا تم إثباته في المقابلة مع رئيس المصلحة المعلوماتية.
- كما تحصلت السؤال الاثنان والعشرون (انظر الجدول رقم 05) بنص "كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها" على أكبر نسبة في البعد الثالث 30 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,33، هذه النتيجة المتوسط تميل ميل كبير وتقسم الإجابة مع الموافقة دليل ذ أن المؤسسة لا تتعرض لمخطر العبث بكوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم نظم المعلومات.
- حققت العبارة لرقم الحادي والعشرون في البعد الأول (انظر الجدول رقم 03) التي تنص على" تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها " حصل على اتفاق العينة بالنسبة 72,5 في المائة على عبارة "موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,55.
- كما تحصلت عباراتي الواحد وعشرون و خمسة والعشرون (انظر الجدول رقم 05) و ينص على التوالي" يمنع الموظف الغير المختص من أجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات " و" توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن" على اكبر نسبة في البعد الثالث 58,8 في المائة حصل على مجموع الكي لمتوسط الحسابي بالقيمة على التوالي 2,40 و 2,42 بالانحراف معياري مقدر على التوالي 0,789 و 0,759 هذه نتيجتين جيدة لهذا البعد والذي شملت النسخ الإضافية و عدم إجراء تعديلات في مكونات المادية في نظم المعلومات ومن شانه تقليل مخاطر المترتبة عنها.

2.1.3 بالنسبة لمؤسسة اتصالات الجزائر: تحصلت العبارة التاسعة في البعد الأول (انظر الجدول رقم 03) التي تنص على" يفرض على الموظفين تغيير كلمة المرور دوريا " حصل على اتفاق العينة بالنسبة 23,3 في المائة على عبارة "غير موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,17 أن المؤسسة تفرض على الموظفين تغيير كلمة المرور دوريا لكن الاشكال انه لا توجد صرامة في متابعة ذلك.

- كانت الاجابات المتعلقة بالسؤال الثامن (انظر الجدول رقم 03) الذي ينص على" يتم تجديد العتاد دوريا " حصل على اتفاق العينة بالنسبة 50 في المائة على عبارة "محايد " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,22 وهذا دليل على أن المؤسسة تجدد العتاد دوريا لكن ليس بالشكل المطلوب.
- وتحصلت العبارة السادس عشر في البعد الثاني (انظر الجدول رقم 04) بنص "هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات" بالنسبة 41,7 في المائة بالمتوسط الحسابي بالقيمة 2,32 بالانحراف معياري مقدر 0,698 يعني إن المؤسسة تضع السجل رقابي على حوادث الأمن المعلومات كما ثبت في المقابلة.

DOI : 10.12816/0052776

◆ وتحصلت عبارة الرابع والعشرون في البعد الثالث (انظر الجدول رقم 05) بنص " توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات وفي مكان امن." بالنسبة 41,7 في المائة بالمتوسط الحسابي بالقيمة 2,42 بالانحراف معياري مقدر 0,669.

◆ تحصلت العبارة الثانية عشر (انظر الجدول رقم 03) " تدرك الإدارة أهمية سياسات أمن المعلومات" حصل على اتفاق العينة بالنسبة 67,5 في المائة على عبارة "موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 2,62 بالانحراف معياري مقدر 0,597 هذا الجواب جوهري ومهم لأن سياسات الأمنية لا تطبق إلا بدراية الإدارة العليا بأهمية نظم المعلومات.

◆ وتحصلت عبارة السابعة عشر في البعد الثاني (أنظر الجدول رقم 04) بنص " يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة " بالنسبة 62,5 لمتوسط الحسابي بالقيمة 2,52، يعني أن المؤسسة تهتم بالأمن المعلوماتي وتدرك العواقب إذا اختلت ومنه تفرض العقوبات على من ينتهك ويخالف الأوامر.

◆ وتحصلت العبارة العشرون في البعد الثالث (انظر الجدول رقم 05) بنص " يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها " بالنسبة 70 في المائة بالمتوسط الحسابي بالقيمة 2,63 وهذا ما ثبت في المقابلة.

3.1.3 بالنسبة لمؤسسة ليند غاز:

◆ تحصل السؤال الحادي عشر (أنظر الجدول رقم 03 الذي ينص على" تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها" حصل على اتفاق العينة بالنسبة 100 في المائة على عبارة "موافق " حصل على مجموع الكي لمتوسط الحسابي بالقيمة 3 هذا الجواب معبر على اتفاق كلي بان جميع العمليات في النظام تسجل أثناء المعالجة باسم الموظف الذي قام بها.

◆ وتحصلت عبارة الثامنة عشر في البعد الثاني (انظر الجدول رقم 04) بنص " لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا." بالنسبة 88,9 لمتوسط الحسابي بالقيمة 2,83.

◆ وتحصلت عبارة العشرون في البعد الثالث (انظر الجدول رقم 05) بنص " يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها " بالنسبة 94,4 في المائة بالمتوسط الحسابي بالقيمة 2,94 بالانحراف معياري مقدر 0,236 وتشير معطيات على عدم تشتت الإجابات يعني إن المؤسسة لديها مولد كهرباء ومخزن الطاقة كما ثبت في المقابلة أيضا.

◆ تساوي نسبة عباراتي الثالث عشر ورابع عشر والسادس عشر (انظر الجدول رقم 04) بنسبة 33,3 والذي يحتوي على ما يلي على توالي" تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه اتجاه أمن المعلومات في المؤسسة "" يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف".

DOI : 10.12816/0052776

4. نتائج اختبار علاقة الارتباط بين محاور الاستبيان (معامل سبيرمان): من خلال الجدول رقم (06) نجد النتائج الارتباط سبيرمان كالآتي:

- **بالنسبة لمؤسسة سونلغاز: تحصلنا** على القيمة الارتباط R =0.088 عند sig =0.436 وهي غير دالة إحصائيا إذ أنها يجب أن تكون أقل من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة سونلغاز لا يساهم في الحد من مخاطر نظم المعلومات، و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.
- **بالنسبة لمؤسسة اتصالات الجزائر:** تحصلنا على القيمة الارتباط R =0.063 عند sig =0.493 وهي غير دالة إحصائيا إذ أنها يجب أن تكون أقل من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة اتصالات الجزائر لا يساهم في الحد من مخاطر نظم المعلومات، و نستنتج انه لا توجد علاقة ذو دلالة إحصائية بين نظام الأمن الالكتروني و المخاطر.
- **بالنسبة لمؤسسة ليند غاز:** تحصلنا على القيمة الارتباط R =-0.55 عند sig =0.018 وهي دالة إحصائيا إذ أنها اصغر من 0.05، ومنه نستنتج إن نظام الأمن الالكتروني في مؤسسة ليند غاز يساهم في الحد من المخاطر. ونستنتج انه توجد علاقة ارتباط عكسية قوية ذو دلالة إحصائية بين نظام الأمن الالكتروني والمخاطر.

5. مناقشة النتائج:

1.5. مؤسسة سونلغاز: من خلال ما تم ملاحظته، وجمعه باستخدام كل من المقابلة والاستبيان، يتضح أن المؤسسة تمتلك الجانب البشري مؤهل على مستوى فرع ELIT بالجزائر العاصمة، المختص في إنجاز وتسيير وتطوير نظم المعلومات الإلكترونية، بالإضافة الى مستخدمي ومسيري النظام على مستوى المديرية بورقلة.

يحوي نظام معلومات المؤسسة على المكونات الأساسية من موارد بشرية، أجهزة وبرامج، شبكات بالإضافة الى السياسات الامنية، لكن لديهم مشكلة على مستوى البرامج اذ لم يتم استغلالهم كليا، اما بالنسبة للسياسات الامنية فيبقى وعي النوظفين بذلك اهم عائق تواجه المؤسسة. وعليه نستنتج ان نظام الأمن الالكتروني المعتمد في المؤسسة وفق نتائج الاستبيان والمقابلة مع مسؤولي النظام لا يساهم بكل فعال في الحد من مخاط نظم المعلومات.

2.5. اتصالات الجزائر: تمتلك المؤسسة الجانب البشري من إطارات ومهندسين تسهر على الاشراف على تسيير نظام المعلومات بصفة كاملة والمؤسسة حاليا تحدث بعض التغيرات من اجل تحسين البرنامج gaya 05 إلى نسخة 07 ، وانتقال عملية الإشراف على المستوى الخادم إلى الجزائر العاصمة وهذا لضمان التنسيق والترابط بين مختلف فروع المؤسسة وطنيا، كما اتضح لنا بالمقابلة بعض مميزات النظام كالسرعة تنفيذ المهام و المعالجة و التخزين و الاسترجاع، بالاضافة الى سهولة مراقبة سيرورة العمل كما يساعد على اتخاذ القرار من خلال تزويد المسؤولين بكل المعلومات الضرورية وفي والوقت المناسب وايضا يعتبر وسيط بين أجهزة الاتصالات والموظفين بوصول سريع وآمن للأجهزة كما لا يخلو من نقائص فمثلا لا يوجد نظام واجراءات وقوانين داخلية تتعلق بالأمن الالكتروني، وأن الإنقطاعات التي تحدث أحيانا على مستوى الوكالات التجارية سببها عادة خلل في الشبكة وليست الأجهزة ، مما سبق نستنتج أن للسياسات الأمنية دور كبير في استمرارية عمل نظام المعلومات، كما نشير

DOI : 10.12816/0052776

ان المؤسسة ايضا تعاني من مشكلة الوعي بأهمية السياسات الأمنية لنظم المعومات من طرف موظفيها، وعليه نستنتج أن نظام الأمن الالكتروني لا يساهم بشكل فعال في الحد من مخاطر نظم المعلومات.

3.5. مؤسسة ليند غاز: من خلال النتائج توصلنا أن المؤسسة لديها كفاءات بشرية تتوافق وأهداف المؤسسة لتثبيت نظام معلوماتي فعال، بالاضافة الى توفر عنصر العتاد والبرامج المتطورة (ERP)، وتتكون قاعدة البيانات المؤسسة لنظام المعلومات من خادم من نوع Microsoft بسعة صغيرة تقدر بـ1.5 تيرا ولكن كافية لتخزين معلومات الوحدة وبدورها تنقل المعلومات لتخزينها على مستوى الجزائر العاصمة، وهذا الخادم تم تقسيمه إلى خادم ثلاثي افتراضية - نقطة توزيع- نقطة طباعة - نقطة الثالثةو تحتوي على البرامج وتحديثات ومضادات الفيروسات المرخصة فقط من طرف الشركة إلام، ولكن لوحظ غياب كاميرات المراقبة التي جاري توصيلها إلى المؤسسة، وكما تبين ان المؤسسة لا تملك نظام إطفاء الحرائق جيد هذا من شانه يرفع تهديدات المتعلقة بنظام المعلومات خاصة في ظل نوع نشاط المؤسسة لكونها مؤسسة تنتج الغازات، كما لاحظنا أن المؤسسة تولي اهتمام بالأمن الكتروني ولديها معرفة جيدة بذلك، ولكن توجد بعض النقائص والتي نراها خطر تهدد نظام منها الاستعانة بمؤسسات خارجية لتصليح، ومع هذه النقائص يعتبر نظام معلومات مؤسسة ليند غاز الاحسن في عينة الدراسة من حيث السياسات الأمنية المطبقة و الصرامة في متابعة تنفيذ كل الاجراءات و لالوائح، وعليه نستنتج ان نظام الأمن الالكتروني في مؤسسة ليند غاز يساهم في الحد من مخاطر نظم المعلومات.

IV- الخلاصة:

حاولنا من خلال هذه الدراسة توضيح مفهوم نظام المعلومات الالكتروني المبني على تكنولوجيا المعلومات والاتصال، كما تطرقنا الى نظام الحماية الالكتروني ومختلف مخاطر بيئة نظم المعلومات، اما في الدراسة الميدانية حاولنا تحليل واقع نظام الأمن الالكتروني في المؤسسات محل الدراسة وتوصلنا في الأخير الى تصنيف المخاطر الممكن حدوثها في كل مؤسسة بالنسبة لمدى فعالية نظام الحماية الخاص بها، ويمكن تلخيص النتائج في النقاط الآتية:

- كفاءة نظم معلومات المؤسسات من حيث المكونات المادية والبرمجية والبشرية؛
- لدى مؤسسة ليند غاز نظام حماية الكتروني يشمل كل العناصر؛
- يتميز نظام الأمن الالكتروني في مؤسستي سونلغاز واتصالات الجزائر بالنقص والضعف؛
- لدى مؤسسة ليند غاز نظام معلومات الكتروني فعال (erp)؛
- هناك تفاوت في إمكانية نظام الأمن الالكتروني في الحد من ا لمخاطر بين المؤسسات محل الدراسة؛
- انتشار الوعي بأهمية نظام الامن الالكتروني واحترام السياسات الأمنية لدى موظفي ليند غاز عكس المؤسستين الأخرتين؛
- عدم وضوح السياسات والإجراءات الرقابية المطبقة ومكتوبة في المؤسسات بما يتعلق بالأمن الالكتروني؛
- إدراك الإدارة العليا بأهمية النظام الأمن الكتروني من ناحية تكوين الأفراد في مجال الأمن الكتروني ومشاركتهم في فعالية نظام الحماية لدى مؤسسة ليند غاز؛
- عدم تطبيق إجراءات عقابية صارمة على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في مؤسستي سونلغاز واتصالات الجزائر.

DOI : 10.12816/0052776

ـ الملاحق:

الجدول رقم 01: يوضح ثبات استمارة الاستبيان حسب معامل" ألفا كرونباخ"

المؤسسة	حجم العينة	عدد الفقرات	معامل ألفا كرونباخ	نسبة ألفا كرونباخ٪
المؤسسة سونلغاز ورقلة	80	42	0,878	87.8
المؤسسة اتصالات الجزائر ورقلة	120	42	0,92	92
المؤسسة ليند غاز وحدة ورقلة	18	42	0,782	78.2

المصدر : من إعداد الباحثين بناءا على برنامج Spss

الجدول رقم 02: إجابات افراد العينة حول المحور الأول

المحور الأول: مخاطر نظام المعلومات	مؤسسة سونلغاز			مؤسسة اتصالات الجزائر			مؤسسة ليند غاز		
	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه
1.الإدخال غير المتعمد (غير المقصود) للبيانات غير سليمة بواسطة الموظفين.	1,9	0,56	أحيانا	1,9	0,43	أحيانا	2,28	0,461	أحيانا
2.الإدخال المتعمد) المقصود) للبيانات غير سليمة بواسطة الموظفين	1,5	0,55	لم يحدث أبدا	1,6	0,605	لم يحدث أبدا	1,33	0,594	لم يحدث
3.التدمير غير المتعمد(الحذف) للبيانات بواسطة الموظفين.	1,7	0,56	أحيانا	1,8	0,612	أحيانا	1,94	0,639	أحيانا
4.التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين.	1,4	0,59	لم يحدث أبدا	1,6	0,690،	أحيانا	1,5	0,857	لم يحدث أبدا
5.الوصول غير الشرعي للبيانات او للنظام من طرف موظفين غير مرخص لهم	1,6	0,6	أحيانا	1,7	0,657	لم يحدث أبدا	1,44	0,616	لم يحدث أبدا
6.الوصول غير الشرعي للبيانات او للنظام من طرف أشخاص من خارج المؤسسة.	1,3	0,6	لم يحدث ابدا	1,5	0,756	لم يحدث ابدا	1,06	0,236	لم يحدث ابدا
7.تعرضت اجهوة الحاسوب في المؤسسات الى الفيروسات.	2,3	0,6	أحيانا	2	0,541	أحيانا	2,17	0,383	أحيانا
8.تم تعديل بعض خصائص أو تدمير بنود معينة من المخرجات.	1,7	0,59	أحيانا	1,7	0,679	أحيانا	1,33	0,485	لم يحدث أبدا
9.خلق مخرجات زائفة / غير صحيحة.	1,5	0,64	أحيانا	1,6	0,681	لم يحدث أبدا	1,17	0,383	لم يحدث أبدا
10.سرقة البيانات / المعلومات.	1,5	0,64	لم يحدث أبدا	1,4	0,644	لم يحدث ابدا	1,11	0,323	لم يحدث أبدا
11.عمل نسخ غير مصرح وغير مرخص بها من المخرجات من طرف موظفين	1,5	0,63	لم يحدث أبدا	1,5	0,698	لم يحدث أبدا	1,22	0,428	لم يحدث أبدا
12.الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق. (أي اطلاع موظفين او اشخاص اخرين على مخرجات تم طبعها وهم غير مرخصين لذلك).	1,4	0,59	لم يحدث ابدا	1,6	0,725	لم يحدث أبدا	1,17	0,383	لم يحدث أبدا
13.تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.	1,3	0,59	لم يحدث أبدا	1,6	0,719	لم يحدث أبدا	1,22	0,428	لم يحدث أبدا
14.تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية.	1,7	0,64	أحيانا	1,9	0,593	أحيانا	1,67	0,485	أحيانا

المصدر: من اعداد الباحثين بناء على مخرجات spss

DOI : 10.12816/0052776

الجدول رقم 03: نتائج البعد الأول المتعلق بالسياسات الأمنية

	سونلغاز			اتصالات الجزائر			ليند غاز		
	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه
1.توجد في المؤسسة سياسات وإجراءات مكتوبة لأمن المعلومات.	2,34	0,779	موافق	2,26	0,728	محايد	2,11	0,832	محايد
2.تدرك الإدارة أهمية سياسات أمن المعلومات.	2,65	0,638	موافق	2,62	0,597	موافق	2,72	0,575	موافق
3.يتم مراجعة وتطوير سياسات أمن المعلومات بشكل دوري.	2,39	0,738	موافق	2,34	0,692	موافق	2,56	0,616	موافق
4.يتم إدخال المعلومات بعد مصادقة الرئيس المصلحة المباشر.	2,49	0,763	موافق	2,51	0,661	موافق	2,67	0,594	موافق
5.لا يسمح لغير المختصين بالوصول إلى الأجهزة والعتاد المحوسب.	2,49	0,763	موافق	2,57	0,645	موافق	2,83	0,514	موافق
6.يمنع الدخول لمواقع الانترانت بأجهزة الموصولة بالخادم المركزي.	2,51	0,729	موافق	2,24	0,733	محايد	2,33	0,84	محايد
7.لا يسمح بتثبيت البرامج غير الأصلية (الغير المرخصة) والمقرصنة.	2,49	0,779	موافق	2,15	0,729	محايد	2,39	0,85	موافق
8.يتم تجديد العتاد دوريا.	1,95	0,87	محايد	2,22	0,676	محايد	2,28	0,752	محايد
9.يفرض على الموظفين تغيير كلمة المرور دوريا	1,96	0,803	محايد	2,17	0,781	محايد	2,17	0,857	محايد
10.يتم التصريح بعناوين الحواسيب IP حتى يتم الدخول النظام	2,32	0,759	محايد	2,44	0,671	موافق	2,72	0,669	موافق
11.تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها	2,55	0,778	موافق	2,57	0,67	موافق	3	0	موافق
المجموع	2,37	0,763	موافق	2,37	0,689	موافق	2,52	0,645	موافق

الجدول رقم 04 : اجابات البعد الثاني المتعلق بإجراءات امن المعلومات المتعلقة بالعاملين

	سونلغاز			اتصالات الجزائر			ليند غاز		
	المتوسط ا لمرجح	الانحرا ف المعياري	الاتجاه	المتوسط ا لمرجح	الانحرا ف المعياري	الاتجاه	المتوسط ا لمرجح	الانحرا ف المعياري	الاتجاه
12.يستفيد العاملون من تدريب يتعلق بالأمن الالكتروني و نظام المعلومات	2,1	0,836	محايد	2,38	0,699	موافق	2,28	0,826	محايد
13.تدرج في بطاقة المنصب في المسؤوليات المتعلقة بالأمن المعلوماتي	2,01	0,803	محايد	2,33	0,7	محايد	2,11	0,832	محايد
14.يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف.	2,01	0,787	محايد	2,32	0,698	محايد	2,22	0,808	محايد
15.يطلب من الموظفين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.	2,26	0,791	محايد	2,36	0,683	موافق	2,56	0,784	موافق
16.هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.	2,06	0,752	محايد	2,24	0,71	محايد	2,22	0,808	محايد
17.يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات.	2,29	0,783	محايد	2,52	0,673	موافق	2,67	0,686	موافق
18.لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا.	2,48	0,729	موافق	2,53	0,635	موافق	2,83	0,514	موافق
المجموع	2,17	0,783	محايد	2,38	0,685	موافق	2,41	0,751	موافق

المصدر: من اعداد الباحثين بناء على مخرجات spss

DOI : 10.12816/0052776

الجدول رقم 05: نتائج البعد الثالث المتعلقة بإجراءات امن المعلومات المتعلقة بالعتاد والبيانات

	سونلغاز			اتصالات الجزائر			ليند غاز		
	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه	المتوسط المرجح	الانحراف المعياري	الاتجاه
19 ،تستخدم المؤسسة شتئ الوسائل (أبواب –أقفال – بطاقات دخول - كاميرات) لحماية مكونات نظم المعلومات.	2,33	0,808	محايد	2,43	0,682	موافق	2,67	0,767	موافق
20 ،يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها.	1,91	0,874	محايد	2,63	0,607	موافق	2,94	0,236	موافق
21 يمنع الموظف الغير المختص من أجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.	2,4	0,789	موافق	2,52	0,635	موافق	2,72	0,669	موافق
22 كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها.	2,33	0,776	محايد	2,55	0,62	موافق	2,67	0,594	موافق
23 تستخدم طرق تشفير لحماية البيانات.	2,41	0,758	موافق	2,42	0,62	موافق	2,56	0,705	موافق
24 توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات وفي مكان امن.	2,35	0,765	موافق	2,42	0,669	موافق	2,78	0,428	موافق
25 توجد برامج حماية لتتبع ومنع الاختراق والتسلل.	2,42	0,759	موافق	2,43	0,658	موافق	2,61	0,698	موافق
26 تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.	2,25	0,834	محايد	2,48	0,622	موافق	2,67	0,594	موافق
27 يتم تثبيت مضادات الفيروسات والتحديثات الدورية.	2.43	0,792	موافق	2,39	0,677	موافق	2,56	0,616	موافق
28 يتم صيانة الشبكة والعتاد دوريا.	2,22	0,826	محايد	2,49	0.661	موافق	2,61	0,698	موافق
المجموع	2,3	0,798	محايد	2,47	0,647	موافق	2,67	0,6	موافق

المصدر: من اعداد الباحثين بناء على مخرجات spss

الجدول رقم 06: معامل الارتباط بين محاور الدراسة

	ليند غاز		اتصالات الجزائر		سونلغاز		
	المحور الثاني: مخاطر نظم المعلومات.	المحور الثالث: نظام الأمن الكتروني في المؤسسة	المحور الثاني: مخاطر نظم المعلومات.	المحور الثالث: نظام الأمن الكتروني في المؤسسة	المحور الثاني: مخاطر نظم المعلومات.	المحور الثالث: نظام الأمن الكتروني في المؤسسة	معامل الارتباط سبيرمان
المحور الثالث :	-0,550*	1	0,063	1	0,088	1	
نظام الأمن الكتروني	0,018		0,493		0,436		
المحور الثاني	1	-0,550*	1	0,063	1	0,088	
مخاطر نظم المعلومات.		0,018		0,493		0,436	

المصدر: من إعداد الباحثين بناء على مخرجات spss

DOI : 10.12816/0052776

الجدول رقم 07: المقارنة بين السياسات الأمنية المتبعة من المؤسسات عينة الدراسة

المؤسسة السياسات الأمنية	سونلغاز	اتصالات الجزائر	ليند غاز
مضادات الفيروسات	موجودة غير شاملة كل	موجودة غير شاملة كل الأجهزة	موجودة
عدم استعمال فلاش ديسك	غير مطبقة	غير مطبقة	مطبقة
كاميرات مراقبة	موجودة	موجودة	غير موجودة حاليا
تحديد الصلاحيات بدقة	مطبقة	مطبقة	مطبقة
كلمة السر شخصية لكل فرد	مطبقة	مطبقة	مطبقة
تغيير كلمة السر دوريا	مطبقة	مطبقة	مطبقة دوريا
الجدار الناري(العتاد)	موجود	موجود	موجود
مضادات الحرائق	موجودة	موجودة	غير موجودة
إنذارات السرقة	موجودة	غير موجودة	موجودة
إجراءات وسياسات أمنية مكتوبة	غير الموجودة	غير الموجودة	موجودة
الصيانة الدورية	موجودة	موجودة	موجودة
صيانة داخلية	داخليا	داخليا	داخليا وخارجية
دورات تحسيسية دورية في امن المعلومات	قليلة	متوسط	معتبرة
برامج حماية الشبكة	موجودة	موجودة	موجودة وفعالة
نسخ احتياطية	موجودة	موجودة	موجودة
نسخ احتياطية خارج المؤسسة	موجودة في ELIT	موجودة في المديرية	موجودة في المجمع
تشفير البيانات المهمة	مطبقة	مطبقة	مطبقة
مولد الكهرباء	غير موجود	موجود	موجود
مخزن ومعدل الكهرباء	موجود	موجود	موجود

المصدر: من إعداد الباحثين بناء على النتائج المقابلة والملاحظة

الجدول رقم 08: المقارنة مدى إمكانية حدوث مخاطر نظام المعلومات بين المؤسسات عينة الدراسة

المؤسسة / المخاطر	سونلغاز	اتصالات الجزائر	ليند غاز
المتعلقة بالمدخلات	متوسط	متوسط	منخفض
سرقة بيانات	منخفض	متوسط	منخفض
انتحال شخصية	منخفض	منخفض	منخفض
الفيروسات	مرتفع	مرتفع	منخفض
استعمال فلاش ديسك	مرتفع	مرتفع	متوسط
المخرجات زائفة	مرتفع	مرتفع	منخفض
مخطر اختراق الشبكة	منخفض	منخفض	منخفض
مخطر الانترانت في المؤسسة	منخفض	مرتفع	متوسط
مخطر انقطاع الكهرباء	مرتفع	منخفض	منخفض
عدم وجود أهداف ورؤية الإستراتجية أمن نظام المعلومات	مرتفع	مرتفع	منخفض
عدم وجود الإجراءات الأمنية	منخفض	مرتفع	منخفض
عدم وجود تدقيق في المجال الأمن نظام المعلومات	منخفض	متوسط	منخفض
غياب البنية الشبكة	منخفض	منخفض	منخفض
عدم توفير لوازم الأمنية لحفاظ على الخوادم ماديا	منخفض	منخفض	مرتفع

المصدر: من إعداد الباحثين بناء على النتائج المقابلة والملاحظة

DOI : 10.12816/0052776

ـ الإحالات والمراجع:

1. كاوجة بشير. (2013)، دور تكنولوجيا المعلومات و الاتصال في تحسين الاتصال الداخلي بالمؤسسات الاستشفائية العمومية الجزائرية، مذكرة ماجستير، جامعة ورقلة، ص24.

2 laudon & laudon-(2006)-management information systems-the digital firm , idition9, Pearson Education, USA, page50

3 Robert Longeon, Jean-Luc,(2009)Guide de la sécurité des systèmes d'information, Paris, France, , P10

4 Ayari amani"(2014) audit de sécurité du système informatique de MTIC " mémoire de mastere professionnel « Nouvelles Technologies des Télécommunications et Réseaux » Université virtuelle de tunis, p 14.

5. علوطي لمين. (2009). تحديات الامن الالكتروني في المؤسسة"، مجلة الابحاث الاقتصادية و الادارية- العدد السادس ديسمبر ،جامعة المدية، ص169.

6 Robert Longeon, Jean-Luc, (2009)(Guide de la sécurité des systèmes d'information, Paris, France, P12

7 . أمل ابراهيم أبو رحمة. (2005)، نظام معلومات الموارد البشرية وأ رها على فاعلية ادارة شؤون الموظفين في فلسطين، مذكرة ماجستير، ادارة الأعمال، غزة ص58.

8 . مصطفى فتحي. (2010) . **أمن المعلومات**، دورة علمية، المنظمة العربية للتنمية الإدارية، القاهرة، ص 10.

9 . نفس المرجع والصفحة

10 رجم خالد. (2016). محاضرات مراجعة نظام المعلومات، ماستر تدقيق ومراقبة التسيير، جامعة ورقلة، ص30.

كيفية الاستشهاد بهذا المقال حسب أسلوب APA :

الطاهر بن عمارة، خالد رجم، العربي عطية. (2018). أثر نظام الحماية الالكتروني في الحد من مخاطر تكنولوجيا المعلومات والاتصال، دراسة مقارنة لعينة من المؤسسات، مجلة رؤى اقتصادية، 08(02)، جامعة الوادي، الجزائر، ص.ص 135-150.