LJAST
Libya n Journal for
Applied Science & Technology
مجلة ليبيا للعلوم التطبيقية والتقنية

Volume 9 Issue 1
September 2021

واقع إدارة أمن المعلومات للمراكز البحثية في حماية البنية التحتية لنظم المعلومات وسياسة أمن المعلومات

أحمد دخيل [1] ، سعد طلحة [2] ، عزالدين بن ضو [3]

المركز المتقدم للتقنية، مكتب التوثيق والمعلومات / طرابلس [1]
هيئة البحث العلمي والتعليم التقني والفني،/ طرابلس [2]
كلية التقنية الالكترونية،/ طرابلس [3]

الملخص

يعتبر أمن المعلومات ضروري لحماية وتأمين الموارد المستخدمة، حيث أنه يعمل على سريتها وسلامتها ففي حالة غياب أمن المعلومات أو نقصه أو عدم الاستفادة منه، يؤدى ذلك إلى وجود ثغرات مثل الوصول أو الاستخدام الغير مصرح به، أو ربما الكشف والتعطيل والتعديل أو التخريب، ولهذا يعد أمن المعلومات من الركائز الضرورية في حماية الأفراد والمؤسسات من الأضرار الناتجة لضمان أمن المعلومات هناك عدة طرق دقيقة وملائمة وموثوقة تستخدم لعدم إفشاء البيانات والمعلومات المخزنة التي تؤثر على سير أداء المراكز البحثية.

تهدف هذه الدراسة إلى معرفة واقع أمن المعلومات في المراكز البحثية، بحيث يكون لدينا في المستقبل خطة معلوماتية تتناسب مع هذه المراكز حيت ستساهم هذه الدراسة في إنشاء حكومة الكترونية يكون لديها توصيف يتوافق مع هذه المراكز البحثية مستقبلا، كما تهدف الدراسة إلى نشر الوعي بثقافة أمن المعلومات للعاملين بهذه المراكز.

تتمحور الدراسة حول عينة من المراكز البحثية التابعة للهيئة الليبية للبحث العلمي، حيث تم استخدام استبيان كوسيلة لجمع المعلومات ولاختبار فرضيات الدراسة، تم استخدام برنامج التحليل الإحصائي SPSS للوصول إلى نتائج ومن تم التوصل إلى مجموعة من الاستنتاجات والتوصيات التي تؤدي الى اتخاذ كافة التدابير الضرورية لنشر ثقافة أمن المعلومات على مختلف المستويات الإدارية والفنية بالمراكز عن طريق إعداد برامج تدريبية وورش عمل توعوية.

الكلمات الافتتاحية

أمن نظم المعلومات، سياسة أمن المعلومات، الاستبيان، برنامج الحزمة الإحصائية للعلوم الاجتماعية

1. المقدمة

تعد المعلومات في وقتنا الحاضر أحد أهم مقومات إدارة الأعمال في المؤسسات الحكومية والغير الحكومية ، ومع ازدياد أهمية المعلومات والإيمان بأهميتها يزداد الاهتمام بكيفية الحفاظ عليها وحمايتها مما أدى إلى ظهور علم مختص يسمى علم أمن المعلومات ، ولا يعد أمن المعلومات عملية تقنية يقوم بها المختصون فقط وإنما هو نتاج تعاون بين جميع العاملين بالمؤسسة، بحيث تتوزع الأدوار والمسؤوليات بما يخدم مصالح المؤسسة وبالتالي فإن أي خطة تضعها المؤسسة بخصوص أمن المعلومات لابد من احتواؤها على عناصر وبنود شاملة لكل العمليات والسياسات المتعلقة بالنواحي التقنية والبشرية، بحيث يجب **أن** تشتمل خطة أمن المعلومات في المؤسسات والمراكز البحثية على كل الأوجه الحساسة للمعلومات لضمان سرية وسلامة بياناتها وتوافرها، والتي تعرف بأنها نهج أمني مستمر ومنظم لإدارة حماية معلومات المؤسسة من التعرض للخطر من قبل الأطراف غير المسئولة ولضمان بقاء سرية المعلومات أمن[1] ، وذلك بتوعية العاملين بها بالمخاطر والهجمات الممكنة ومسئولياتهم في حفظ المعلومات، كما يجدر التنويه على ان أمن المعلومات يمثل مجموعة من المقاييس المختلفة على كافة المستويات الطبيعية المتعلقة بالأفراد أو المقاييس الإدارية لمستويات نظام المعلومات. كما ان الامتثال لمعايير امن المعلومات سيؤثر على افاق اعمال المؤسسات والمنظمات وهو احد الطرق الفعالة لإدارة امن المعلومات [2].

2.أسباب الدراسة :

يتمحور سبب الدراسة في عدم إعطاء الأهمية اللازمة من قبل أغلب المراكز البحثية لاستخدام وتطبيق سياسات أمن المعلومات لحماية مواردها المادية والمعنوية، وحيث انه لا يمكن تحقيق حماية نظام المعلومات إلا من خلال إدارة فعالة لأمن المعلومات وتنفيذ خطة أمنية كاملة عليه يمكن طرح التساؤلات الأتية:

- هل يوجد إدارة لأمن المعلومات بالمراكز البحثية؟
- هل تتأثر هذه المراكز البحثية بوجود أمن المعلومات أو غيابه؟
- ما هي سبل تطوير إدارة أمن المعلومات في المراكز البحثية؟

3. أهمية الدراسة

تنحصر الدراسة على أهمية إدارة أمن وسرية المعلومات وما مدى تأثيرها على أداء هذه المراكز البحثية، كما أنها ستعطي للمراكز البحثية أهمية كبيرة باعتبار بياناتها ومعلوماتها الرقمية متصلة بالعالم الخارجي وذات أهمية حيوية وفعالة في بلادنا.

4. أهداف الدراسة

1. تسليط الضوء على الإجراءات اللازمة لأمن وسرية المعلومات وكيفية الاستفادة منها في المراكز البحثية.
2. حماية وتوفير أمن وسرية لشبكة المعلومات في المراكز البحثية من أي اعتداء أو تطفل أو عبث وكذلك من الحوادث والكوارث الطبيعية.
3. معرفة تأثير أمن وسرية المعلومات على أداء المركز البحثية.
4. نشر الوعي وثقافة أمن المعلومات للعاملين بهذه المراكز.
5. تقديم مقترح لتحسين نظام إدارة أمن المعلومات في المراكز البحثية.

5. منهجية الدراسة

سيتم استخدام أسلوب المنهج الوصفي للإجابة على التساؤلات وإثبات فرضيات الدراسة من خلال أدوات البحث والمتمثلة في:

- المقابلات الشخصية : وذلك بإجراء مقابلات شخصية مع مدراء الإدارات والعاملين بأقسام تقنية المعلومات.
- استمارة الاستبيان : استخدمت الاستمارة كأداة لجمع البيانات الرئيسية من جميع العاملين بأقسام نظم المعلومات في المراكز البحثية.

فرضيات الدراسة

الدلالة الإحصائية هي وصف لنتائج تجارب أجريت على القيمة الاحتمالية (p-value) أقل من مستوى الدلالة، وعند القيام بدراسة علمية فإنه غالبا ما يتم اختبار مستوى الدلالة قبل جمع البيانات وغالبا ما يكون هذا المستوى 0.05، وإسنادا لما سبق وضعت الفرضية الرئيسية الاتية :

- عدم توفر سياسة لأمن المعلومات يؤثر على إدارة أمن ونظم المعلومات في المراكز البحثية بصورة إيجابية عند مستوى الدلالة الإحصائية.
- هل توجد فروق ذات دلالة إحصائية في نتائج عينة الدراسة عند مستوى الدلالة الإحصائية حول واقع إدارة نظم المعلومات في المراكز البحثية؟

6. الدراسة النظرية

يتناول الجانب النظري من الدراسة التعرف على مفهوم ومكونات أمن المعلومات :

6.1 مفهوم أمن المعلومات

يعرف أمن المعلومات بأنه السياسات والإجراءات والمقاييس التي تتخذها المؤسسات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها من وصول الأفراد الغير مصرح لهم سواء من هم داخل المؤسسة ومن خارجها، وتعتبر هده العمليات مستمرة وتتطلب استمرارية في التطوير ومتابعة للمستجدات وكذلك مراقبة وافتراض المخاطر وابتكار الحلول لها.

بناءاً على ما سبق فإن المنظمات لا توصف بأن لها نظام معلوماتي أمني حقيقي وفعال حتى يحقق نظام تطوير مستمر للعمليات الأمنية والبشرية والتقنية من أجل تقليل واحتواء المخاطر المفترضة أو المتوقعة [3].

6.2- مكونات أمن المعلومات

- ✓ السرية : وتعني الحفاظ على سرية المعلومات والمعاملات والإجراءات التي تضمن التأكد من حماية الموارد من الأفراد الغير مخولين بذلك .
- ✓ سلامة المحتوى : التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به.
- ✓ استمرارية توفر المعلومات : التأكد من استمرار عمل النظام ألمعلوماتي واستمرار القدرة على التفاعل مع المعلومات والمستخدمين لتقديم الخدمة لمواقع المعلوماتية وصمان ان المعلومات لن يتعرض إلى منع استخدامه لها أو الدخول إليها.
- ✓ عدم الإنكار : يقصد به ضمان عدم إنكار المستخدم الذي قام بتصرف ما, بحيث تتوفر قدرة الإثبات أن التصرف حدث من مستخدم معين في وقت محدد [4].

6.3 مكونات نظام أمن المعلومات

- ✓ العمليات : تعتبر العمليات مهمة وجوهرية لأي نظام فهي عبارة عن مجموعة من المعايير الدولية ذات طبيعة مستمرة للحماية من الأخطاء والمخاطر[5].
- ✓ الموظفين : جميع العاملين في مجال تقنية المعلومات والاتصالات ذات الخبرات والمهارات المناسبة , يقومون بإنجاز كل العمليات والخدمات.
- ✓ التكنولوجيا : هي جميع الأجهزة الحديثة التي تساعد على توفير وحفظ أمن المعلومات في المؤسسات والجهات العامة ويجب تحديثها حسب المتطلبات.
- ✓ الثقافة : ترتبط بطبيعة ثقافة العاملين في المؤسسات والجهات العامة والخاصة ويجب العمل على رفعها باستمرار.

7. الدراسات السابقة

ظهرت العديد من الدراسات السابقة التي تناولت
موضوع أمن المعلومات ومن بينها :

7.1 الدراسات العربية

1. دراسة (رؤى يونس، 2017)[6] بعنوان "واقع إدارة أمن المعلومات في المؤسسات السورية "، توصلت الدراسة إلى ضرورة بناء سياسات أمن نظم المعلومات والعمل على نشرها واستخدام الحوافز المادية والمعنوية لتشجيع المبدعين في مجال أمن المعلومات والحرص على استخدام البرمجيات الاصلية، كما أوصت الدراسة إلى الاعتناء بتدريب العاملين وزيادة الموازنات المالية لضمان أمن المعلومات والاهتمام بالبنية التحتية.
2. دراسة (رضا ابراهيم، 2020)[7] بعنوان " أثر ادارة امن المعلومات على نجاح برنامج نظم المعلومات " هدفت هذه الدراسة الى الحد من المخاطر التي تتعرض لها نظم المعلومات من خلال المعايير الدولية، وتوصلت الدراسة الى وجود العديد من المخاطر التى تتعرض لها نظم المعلومات وذلك لعدم وجود سياسات وبرامج لأمن المعلومات داخل المؤسسات والمنظمات.
3. دراسة (عرفان وآخرون، 2010)[8] بعنوان" دراسة عملية حول أمن المعلومات فى المنظمات السعودية "، هدفت هذه الدراسة الى تحقيق فهم أكثر حول أمن المعلومات داخل المؤسسات السعودية، وتوصلت الدراسة إلى أهمية تطبيق سياسة أمن المعلومات في المؤسسات العاملة، بالإضافة إلى أن هناك العديد من الحلول التي تمكن المؤسسات من الحفاظ على سرية المعلومات، وإرساء الوعى الأمني بين العاملين داخل المؤسسات من خلال التدريب.

7.2 الدراسات الأجنبية

1. دراسة ((Zammani, M and Razali, R, (2016)[9] بعنوان " دراسة تجريبية لعوامل نجاح إدارة أمن المعلومات" تهدف هذه الدراسة إلى تخفيف التهديدات الأمنية ونقاط الضعف التي تعصف بالعديد من المؤسسات من خلال وضع مجموعة من العوامل الرئيسية لإدارة أمن المعلومات، توصلت هذه الدراسة الى مجموعة من النتائج أهمها عدم وجود سياسات وبرامج لأمن المعلومات داخل المؤسسات.
2. دراسة ("MWITA SIMION MAROA, 2015)[10] بعنوان " العوامل المؤثرة على فاعلية أمن المعلومات في جامعة نيروبي" عالجت هذه الدراسة العوامل المؤثرة على أمن نظم المعلومات، كما توصلت هذه الدراسة الى مجموعة من النتائج أهمها دعم الإدارة العليا والسياسات الأمنية لنظم المعلومات، وتدريب المستخدمين وزيادة الوعي.
3. دراسة (Takemura ,2010)[11] بعنوان: " مدى إدراك العاملين في اليابان لأمن المعلومات " توصلت الدراسة إلى العديد من النتائج كان أبرزها ضرورة تعزيز تعليم أمن المعلومات وتقديم نظام للمنظمات الحكومية والغير حكومية.

8. مجتمع وعينة الدراسة

اقتصرت هذه الدراسة على الأفراد العاملين ضمن نظم المعلومات في المراكز البحثية، وقد بلغ حجم العينة 70 وتم توزيع الاستبيان على جميع أفراد العينة، حيث تم استرداد 62 استبان، وبعد مراجعة الاستبيانات تم استبعاد 6 منها نظرا لعدم تحقق الشروط المطلوبة للإجابة، وكانت الاستبيانات المستوفاة الشروط 56 استبان، والجدول (1) يوضح مجتمع الدراسة وحجم العينة لكل مركز بحثي.

اسم المركز	الموزع	المسترجع	الفاقد	نسبة
المركز المتقدم	10	10	0	%100
مركز تقنيات	10	7	3	%70
مركز اللدائن	10	6	4	%60
مركز البحوث	10	9	1	%90
مركز التدريب	10	8	2	%80
مركز المنظومات	10	10	0	%100
مركز الاستشعار	10	6	4	%60

جدول رقم (1) يوضح مجتمع الدراسة وحجم العينة لكل مركز بحثي

استبان الدراسة

يتناول واقع أمن نظم المعلومات في المراكز البحثية وينقسم إلى محورين :

- **المحور الأول** : حماية البنية التحتية لنظم المعلومات ويتفرع منه ثلاثة محاور فرعية وهي:
  - الحماية المادية Hardware Security
  - الحماية البرمجية Software Security
  - حماية الأفراد Human Resource Security
- **المحور الثاني :** سياسة أمن المعلومات Information Security Policy

9. تحليل ومناقشة نتائج الدراسة

9.1 المعالجات الإحصائية

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية في تحليل البيانات لغرض الوصول الى دلالات ذات قيم ومؤشرات تدعم موضوع الدراسة:

1.تم حساب مقياس ليكرت الخماسي (حيث كانت الدرجة "5" تعنى موافق بشدة والدرجة "1" تعنى غير موافق بشدة) ولتحديد طول فترة مقياس ليكرت الخماسى (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1=4)، ثم تقسيمه على عدد فقرات المقياس الخمسة للحصول على طول الفقرة أي (4/5=0.08)، بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس وهى (الواحد الصحيح) وذلك لتحديد الحد الأعلى للفترة الأولى كما هو موضح بالجدول رقم (2).

الفترة	1.80-1	2.60-1.80	3.40-2.60	4.20-3.40	5.0-4.20
التصنيف	غير موافق تماما	غير موافق	محايد	موافق	موافق تماما
الدرجة	1	2	3	4	5

جدول رقم (2) لأطوال الفقرات

2. استخدام طريقة ألفا كرونباخ لقياس ثبات الاستبانة لجميع محاور الدراسة.
3. اختبار كولمجروف Kolmogorov-Smirnov Test لاختبار ما كانت البيانات تتبع التوزيع الطبيعي أو لا.

4. حساب المتوسط الحسابي Mean والوزن النسبي لمعرفة ارتفاع أو انخفاض استجابات أفراد الدراسة عن كل فقرة من فقرات الاستبيان .
5. اختبار t.test لمتوسط العينة الواحدة ولمعرفة الفرق بين متوسط الفقرة والمتوسط الحيادي.

9.1 ثبات الاستبيان

معامل الثبات يأخذ قيما تتراوح ما بين الصفر والواحد الصحيح، فإن لم يكن هناك ثبات في البيانات فإن المعامل يكون مساويا للصفر وإن كان هناك ثبات تكون قيمة المعامل الواحد الصحيح وكلما اقتربت قيمة البيانات من الواحد الصحيح كان الثبات مرتفعا وكلما اقتربت البيانات من الصفر كان الثبات منخفضا وقد تم استخدام طريقة ألفا كرونباخ لقياس ثبات الاستبانة لجميع محاور الدراسة، ومن الجدول رقم (3) يتضح أن معامل الاستبانة لكل المحاور اكبر من 78% وهى نسبة مرتفعة، مما يدل على درجة عالية من ثبات الاستبانة التي يمكن الاعتماد عليه في الدراسة.

رقم	عنوان المحور	عدد الفقرات	معامل الفا كرونباخ
1	حماية البنية التحتية لنظم المعلومات	17	0.935
2	سياسة أمن المعلومات	6	0.882
	جميع الفقرات	23	0.936

جدول (3) يبين ثبات الاستبانة بطريقة ألفا كرونباخ

9.3- اختبار التوزيع الطبيعي

تم استخدام اختبار كولمجروف Kolmogorov-Smirnov Test لاختبار ما كانت البيانات تتبع التوزيع الطبيعي من عدمه، ويوضح الجدول رقم (4) نتائج الاختبار حيث كانت ان القيمة الاحتمالية لكل محور اكبر من 0.05 وهذا يدل على ان البيانات تتبع التوزيع الطبيعي.

رقم	عنوان المحور	عدد الفقرات	قيمة Z	القيمة الاحتمالية
1	حماية البنية التحتية لنظم المعلومات	17	0.955	0.321
2	سياسة أمن المعلومات	6	0.863	0.476
	جميع الفقرات	23	0.919	0.423

جدول (4) يبين اختبار التوزيع الطبيعي بطريقة كولمجروف

9.4 تحليل فقرات ومحاور الدراسة

تساؤلات الدراسة : ما هو واقع إدارة أمن المعلومات في المراكز البحثية ؟ وما هي طرق تطويرها ؟
تم استخدام اختبار t.test للعينة الواحدة لتحليل فقرات الاستبانة، وتكون الفقرة إيجابية في حالة أفراد العينة يوافقون على محتواها إذا كانت قيمة t المحسوبة أكبر من t الجدولية والتي تساوى 1.98(أو القيمة الاحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أكبر من 60%)، وتكون الفقرة سلبية في حالة أفراد العينة لا يوافقون على محتواها إذا كانت قيمة t المحسوبة أصغر من t الجدولية والتي تساوى 1.98- (أو القيمة الاحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أقل من 60%)، وتكون أراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من 0.05.

10. اختبار فرضيات الدراسة

10.1 الفرضية الأولى : يؤثر حماية البنية التحتية لنظم المعلومات بصورة إيجابية، وتنقسم هذه الفرضية إلى الفروض الفرعية التالية :

10.1.1 . يؤثر توفير الحماية المادية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في فقرات الحماية المادية والنتائج موضحة في الجدول رقم (5).

	الفقرة	المتوسط الحسابي	المتوسط الحسابي	قيمة t	القيمة الاحتمال	الترتيب	اتجاه الفقرة
1	تستخدم المحيطات الأمنية (الجدران – الأبواب – الإقفال – كاميرات المراقبة –	3.76	75.2	2.31	0.0408	1	موافق
2	كوابل الكهرباء والاتصالات التي تنقل البيانات محمية من العبث بها أو اتلافها	2.80	56.00	3.470	0.1272	5	محايد
3	يوجد في المركز مصدر بديل للكهرباء (مولد ، خط ثاني ، UPS)	3.50	70.00	3.24	0.0158	3	موافق
4	يتم صيانة الأجهزة بشكل دوري لضمان استمرارية عملها وسلامتها	3.08	61.6	3.17	0.045	4	محايد
5	يمنع الموظف غير المختص من إجراء أي تعديلات مادية على الأجهزة الخاصة بنظم	3.57	71.40	2.96	0.0207	2	موافق
	جميع الفقرات	3.34	66.84	3.03	0.0499		

جدول (5) يبين اختبار t.test

نلاحظ من الجدول رقم (5) أن المتوسط الحسابي لجميع فقرات الحماية المادية Hardware Securityيساوى 3.34 ، وهو متوسط يقع ما بين (2.60 -3.40) وهو متوسط يقع في الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد)، ومن ثم فإن هذه الفقرات ذات أثر متوسط في زيادة أمن المعلومات، كما أن المتوسط الحسابي النسبي يساوى 66.84 وهو اكبر من المتوسط الحسابي النسبي المحايد 60% وقيمة t المحسوبة المطلقة تساوى 3.03 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98، والقيمة الاحتمالية (Sig') تساوى 0.0499 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفير الحماية المادية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

10.1.2 . يؤثر توفير الحماية البرمجية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية$\alpha \leq 0.05$.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في فقرات الحماية البرمجية والنتائج موضحة في الجدول رقم (6).

	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب	اتجاه الفقرة
1	تستخدم آليات تشفير لحماية البيانات	3.07	61.40	6.34	0.0015	3	محايد
2	توفير أنظمة للنسخ الاحتياطي	3.32	66.40	3.51	0.1233	2	محايد

3	تتم حماية النظام وجميع البرامج المصدرية والتنفيذية عن طريق برامج مكافحة الفيروسات	3.85	77.00	1.90	0.0650	1	موافق
4	توجد برامج حماية فعالة لمنع الاختراق والتسلسل على نظام المعلومات Firewalls	2.92	58.40	4.53	0.0052	4	محايد
5	هناك معايير ولوائح لقبول أي أنظمة جديدة أو تعديلات	2.80	56.00	4.03	0.0078	5	محايد
جميع الفقرات		3.19	63.00	4.06	0.0405		

جدول رقم (6) تحليل الفقرات المتعلقة بالحماية البرمجية Software Security

نلاحظ من الجدول رقم (6) أن المتوسط الحسابي لجميع فقرات الحماية البرمجية Software Security يساوى 3.19، وهو متوسط يقع ما بين (2.60- 3.40) وهو متوسط يقع في الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد)، ومن ثم فإن هذه الفقرات ذات أثر متوسط في زيادة أمن المعلومات، كما أن المتوسط الحسابي النسبي يساوى 63.00 وهو اكبر من المتوسط الحسابي النسبي المحايد 60% وقيمة t المحسوبة المطلقة تساوى 4.06 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98، والقيمة الاحتمالية (Sig') تساوى 0.0405 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفير الحماية البرمجية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

10.1.3 . يؤثر توفير حماية الأفراد على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في فقرات حماية الأفراد والنتائج موضحة في الجدول رقم (7)

	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب	اتجاه الفقرة
1	يتوفر تدريب للموظفين على نظم المعلومات بشكل دوري لتطوير مهاراتهم المتعلقة بالمستجدات الأمنية	3.32	66.40	2.45	0.0352	2	محايد
2	تحتوى وثيقة الوصف الوظيفي للموظف على مسئولياته ومهامه تجاه أمن المعلومات في المركز	2.91	58.20	5.00	0.0037	4	محايد
3	يوجد رقابي سجل يتضمن أنشطة المستخدمين وحوادث أمن المعلومات	2.58	51.60	2.14	0.0492	7	غير موافق
4	تقيد جميع الموظفين بتطبيق السياسات والتعليمات الخاصة بأمن المعلومات	2.80	56.00	3.47	0.1272	6	محايد
5	هنالك تعريف واضح لمهام ومسئوليات كل موظف بالقسم	3.82	76.40	1.73	0.0790	1	موافق
6	يتم تطبيق إجراءات عقابية على الموظف في حالة انتهاك إجراءات وسياسات أمن المعلومات في المركز	3.25	65.00	3.28	0.0151	3	محايد
7	يطلب من الموظفين التوقيع على تعهد بعدم نشر أو الإفصاح على معلومات حساسة تخص المركز	2.89	57.80	4.12	0.0072	5	محايد
جميع الفقرات		3.08	61.60	3.17	0.0452		

جدول رقم (7) تحليل الفقرات المتعلقة بحماية الأفراد Human Resource Security

نلاحظ من الجدول رقم (7) أن المتوسط الحسابي لجميع فقرات حماية الأفراد يساوى 3.08، وهو متوسط يقع ما بين (2.60-3.40) وهو متوسط يقع في الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد)، ومن ثم فإن هذه الفقرات ذات أثر متوسط فى زيادة أمن المعلومات، كما أن المتوسط الحسابي النسبي يساوى 61.60 وهو اكبر من المتوسط الحسابي النسبي المحايد 60% ، وقيمة t المحسوبة المطلقة تساوى تساوى3.17 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98 والقيمة الاحتمالية (Sig') تساوى 0.0452 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفر حماية الأفراد على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

د . اختبار الفرضية الرئيسية الأولى : تؤثر حماية البنية التحتية لنظم المعلومات بصورة إيجابية على إدارة أمن نظم المعلومات عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$.

ر.ق	المحاور الفرعية	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب	اتجاه الفقرة
1	الحماية المادية Hardware Security	3.34	66.84	3.03	0.0499	1	محايد
2	الحماية البرمجية Software Security	3.19	63.00	4.06	0.0405	2	محايد
3	حماية الأفراد Human Resource Security	3.08	61.60	3.17	0.0452	3	محايد
4	جميع الفقرات	3.20	68.81	3.42	0.0452		

جدول رقم (8) المحاور الفرعية لحماية البنية التحتية لنظم المعلومات

نلاحظ من الجدول رقم (8) أن المتوسط الحسابي لجميع أفراد عينة الدراسة يساوى 3.20، وهو متوسط يقع ما بين (2.60-3.40) وهو متوسط يقع فى الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد)، ومن ثم فإن هذه الفقرات ذات أثر متوسط في زيادة أمن المعلومات، كما نلاحظ ان المتوسط الحسابي النسبي يساوى 68.81 وهو اكبر من المتوسط الحسابي النسبي المحايد 60% والقيمة t المحسوبة تساوى 3.42 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98 والقيمة الاحتمالية (Sig') تساوى 0.0452 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفير حماية البنية التحتية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

10.2. الفرضية الثانية : يؤثر توفير سياسة أمن المعلومات على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في فقرات سياسة أمن المعلومات والنتائج موضحة في جدول رقم (9).

	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب	اتجاه الفقرة
1	يوجد بالمركز سياسة مكتوبة لأمن المعلومات	2.69	53.80	5.81	0.0021	6	محايد
2	يعرف الموظف بسياسة أمن المعلومات	3.01	60.20	5.88	0.0020	5	محايد
3	توجد جهة مكلفة بالإشراف على متابعة سياسة أمن المعلومات	2.94	58.80	4.05	0.0076	3	محايد
4	يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري	3.26	65.20	5.70	0.0023	4	محايد
5	إدراك الجهة العليا في المركز أهمية سياسة أمن المعلومات	3.16	63.20	4.33	0.0061	1	محايد
6	يوجد إجراءات صارمة لحماية نظم المعلومات من أي تغييرات	3.10	62.00	3.88	0.0088	2	محايد
	جميع الفقرات	3.03	60.53	4.94	0.0048		

جدول رقم (9) تحليل الفقرات المتعلقة بسياسة أمن المعلومات Information Security Policy

نلاحظ من الجدول رقم (9) أن المتوسط الحسابي لجميع فقرات سياسة أمن المعلومات Information Security Policy يساوى 3.03 ، وهو متوسط يقع ما بين (2.60-3.40)) وهو متوسط يقع في الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد)، ومن ثم فإن هذه الفقرات ذات أثر متوسط في زيادة أمن المعلومات، كما أن المتوسط الحسابي النسبي يساوى 60.53 وهو اكبر من المتوسط الحسابي النسبي المحايد 60% وأن القيمة t المحسوبة تساوى 4.94 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98 والقيمة الاحتمالية (Sig') تساوى 0.0048 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفير سياسة أمن المعلومات على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

11. النتائج

1- لاحظ من خلال نتائج الدراسة عدم توفر حماية لأمن المعلومات في المراكز البحثية بصورة جيدة.
2- معرفة الجهات المسئولة للمراكز البحثية بأهمية سياسات أمن المعلومات، إلا انه لا يوجد في أي من المراكز المذكورة سياسات وإجراءات معمول بها ومطبقة على أسس واضحة.
3- هناك نقص في برامج التوعية والتدريب للعاملين في مجال أمن المعلومات.
4- عدم توفر سياسات امن المعلومات وعدم توفر الإجراءات الداعمة لها.
5- عدم توفر الكفاءات سواء من جانب مشغلي خدمات امن المعلومات أو من جانب الجهات المسئولة.
6- غياب الوعي بأمن المعلومات على جميع مستويات المراكز البحثية.
7- اعتقاد أن امن المعلومات يعتمد على بعض التقنيات كجدار الحماية أو مضاد الفيروسات وعدم التفكير في تبنى استراتيجيات لاحتواء الأحداث الأمنية بطرق مناسبة والعمل على معرفة أسباب حدوثها.

12. التوصيات

في ضوء النتائج السابقة نوصى بالتالي :

1-زيادة الاهتمام بتوعية العاملين بالمراكز البحثية بأهمية استخدام المعايير والسياسات الأمنية وإقامة دورات تدريبية وورش عمل.
2-ضرورة قيام المراكز البحثية ببناء سياسات لأمن نظم المعلومات خاصة بها والعمل على نشرها وتطبيقها ، والقيام بتطويرها ومراجعتها وتقييم المخاطر بشكل دوري ووضع خطط لضمان أمن وسرية المعلومات.
3-تطبيق المعايير الدولية لأمن المعلومات يوفر ضمان الحماية لها في جميع المراكز البحثية .
4-التأكد من الالتزام بالسياسات والإجراءات الأمنية.
5-استخدام تقنيات تشفير البيانات والتأكد من امن كافة الأنظمة بشكل مستمر.
6-حماية شبكات المراكز وكافة الخوادم وأجهزة الحاسوب من خلال التحديث المستمر للبرامج الأصلية.
7-وضع نظام مجدول للنسخ الاحتياطي والعادي خاصة في ظل الظروف الحالية من ناحية التهديدات والانتهاكات اليومية من قبل المحترفين.
8-وضع سياسة مكتوبة لأمن المعلومات ومراجعتها بصورة دورية لمواكبة التطورات الحديثة.
9-تحديد المخاطر وتقييم الثغرات الأمنية التي يمكن أن تهدد امن المعلومات في هذه المراكز البحثية.

13. الخاتمة :-

إن تطبيق خطة إدارة امن المعلومات في المراكز البحثية يكون على عدة مراحل وتحتاج إلى مراجعة دورية ليتلاءم فعلها مع وجود التحديات والاختراقات الموجودة ، لذا يجب على الجهات المختصة إتباع كافة المعايير الأمنية، كما يجب ونشر الوعي بين العاملين تجاه حماية معلوماتهم ومعلومات الجهات التابعين لها، كما يجب تحديد الإجراءات والسياسات الأمنية لتفادى حدوث أي اختراقات او انتهاكات امنية داخل مؤسساتها، وفي الختام نأمل تطبيق سياسة أمل المعلومات في جميع المؤسسات الحكومية والغير حكومية.

14. المراجع

[1] Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", International Journal on Advanced Science Engineering information Technology, Vol. 6, No. 6.
[2] Micki Krause ; Harold F. Tipton , Information Security Management Hand book , Sixth Edition , Auerbach Publication , New York , 2008.

[3] Heru Susanto, Mohammad Nabil, Information Security Management, publisher Francis and Taylor, July 2020.
[4] Bel G. Raggad. 2010, "Information Security Management: concepts and practice ,page 23.
[5] Stair, Ralph M. &George W. Reynolds. (2010).Principles Of Information Systems, Course Technology. 9th Editions. NY: Mc-Graw-Hill
Straub, et.al. (1995). Measuring System.
[6] رؤى بن يونس، "دراسة واقع أمن نظم المعلومات في المؤسسات السورية"، مجلة البعث– المجلد 39 – العدد 31 لسنة 2017.
[7] رضا ابراهيم، أحمد عبد السلام "دراسة أثر ادارة امن المعلومات على نجاج برنامج نظم المعلومات" مجلة الدراسات التجارية المعاصرة، المجلد السادس، العدد العاشر، 2020
[8] عرفان نبي، عبد الرحمن مرزا، خالد الغنبر،"دراسة عملية حول أمن المعلومات في المنظمات السعودية، جامعة الملك سعود، مركز التميز لأمن المعلومات، لسنة 2010.
[9] Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", International Journal on Advanced Science Engineering information Technology, Vol. 6, No. 6.
[10] MWITA SIMION MAROA, « Factors affecting information systems security effectiveness in university of Nairobi »,Thesis of Master of science degree in information systems, Kenya,2015.
[11] Takemura, Toshihiko, (2010), "A Quantitative Study on Japanese Workers Awareness to Information Security Using the Data Collected by Web-Based Survey American Journal of Economics and Business Administration, Vol. 2, No.1: 20- 26.