عمادة الدراســات العليا

جامعة القدس

"واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة "

همـام سالم سمارة المصري

رسالة ماجستير

القدس – فلسطين

1441هـ - 2019م

واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة

إعداد

همام سالم سمارة المصري

بكالوريوس إدارة أعمال/ جامعة القدس المفتوحة– غزة– فلسطين.

المشرف: د. محمد عبد أبو سعدة

قدمت هذه الدراسة استكمالاً لمتطلبات درجة الماجستير في بناء المؤسسات وتنمية الموارد البشرية، من معهد التنمية المستدامة/ جامعة القدس– فلسطين.

1441 هـ / 2019 م

جامعة القدس
عمادة الدراسات العليا
برنامج ماجستير في بناء المؤسسات والتنمية البشرية

إجازة الرسالة

واقع تطبيق معايير أمن المعلومات (ISO-IEC 272002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة

اسم الطالب: همام سالم سمارة المصري
الرقم الجامعي: 21620442

المشرف: الدكتور محمد عبد أبو سعدة

نوقشت هذه الرسالة وأجيزت بتاريخ 2019/10/13 من قبل أعضاء لجنة المناقشة المدرجة أسماءهم وتواقيعهم:

١. رئيس لجنة المناقشة د. محمد عبد أبو سعدة التوقيع:.....
٢. ممتحناً داخليا: د. حسن خميس السعدوني التوقيع:.....
٣. ممتحناً خارجيا أ. د. ماجد محمد الفرا التوقيع:.....

القدس- فلسطين
2019م- 1441هـ

الإهداء

إلى من كان سبباً في وجودي.. إلى من أفنى عمره من أجلي ... والدي الغالي

إلى من أسير في الدنيا برضاها، إلى من أفنت زهرة حياتها من أجلي... أمي الحبيبة

إلى من أنارت لي طريقي وآزرتني... إلى رفيقة دربي.. زوجتي العزيزة أسماء

إلى أبنائي فلذة كبدي ونور عيني، سالم وأمير

إلى الذين أضاءوا بعلمهم عقول الآخرين... أساتذتي

إلى من ضحوا بحريتهم لأجل أن نعيش بحرية... أسرانا البواسل

أهدي هذا البحث المتواضع راجياً من المولى عز وجل أن يجد القبول والنجاح.

همام سالم سمارة المصري

إقرار

أنا الموقع أدناه أقر بأني معد هذه الرسالة، لتقديمها إلى جامعة القدس، لنيل درجة الماجستير، وأنها جاءت نتيجة أبحاثي الخاصة، باستثناء ما تم الإشارة إليه حيثما ورد، وأن هذه الرسالة أو أي جزء منها لم يقدم لنيل أي درجة علمية لأي جامعة أو معهد آخر.

التوقيع: .....

همام سالم سمارة المصري

التاريخ: 2019/10/13

شكر وعرفان

الحمد لله ذي المن والفضل والإحسان، حمداً يليق بجلاله وعظمته. وصَلِّ اللهم على خاتم الرسل، من لا نبي بعده. ولله الشكر أولاً وأخيراً، على حسن توفيقه، وكريم عونه، وعلى ما منَّ وفتح به عليَّ من إنجاز لهذه الدراسة، بعد أن يسّر العسير، وذلّل الصعب، وفرَّج الهم، وعلى تفضُّله عليَّ بوالدَين كريمين شقّا لي طريق العلم، وكانا خير سند لي طيلة حياتي الدراسية من تشجيع ودعاء وصبر وعطاء أمدَّ في عمرهما على عمل صالح، وأعانني على برهما.

كما أَدِينُ بعظيم الفضل والشكر والعرفان بعد الله سبحانه وتعالى في إنجاز هذا البحث وإخراجه بالصورة المرجوة إلى مشرفي على الرسالة الأستاذ الدكتور / محمد أبو سعدة الذي منحني الكثير من وقته، وجهده وتوجيهاته وآرائه القيمة، ومدَّ يد العون لي دون ضجر للسير قدماً بالدراسة نحو الأفضل سائلاً المولى القدير أن يجزيه عني خير الجزاء ويثيبه الأجر إن شاء الله.

كما وأشكر لجنة المناقشة والمكونة من الدكتور حسن سعدوني لقبوله لمناقشة هذه الدراسة بصفته مناقشاً داخلياً، والأستاذ الدكتور ماجد الفرا لقبوله مناقشة هذه الدراسة بصفته مناقشاً خارجياً، اللذين سيثريان الدراسة بعلمهما الكبير وملاحظاتهم القيمة.

والشكر موصول كذلك لأصدقائي الذين وقفوا معي من البداية للنهاية وأخص بالذكر الدكتور نضال المصري، والدكتور جهاد المصري، والأستاذ يوسف مطرية، ولا أنسى أن أتوجه بجزيل الشكر والتقدير لعائلة مكتبة القدس ممثلة بصاحبها الأستاذ محمد أبو زايد.

وأتوجه لكل من مدَّ لي يد العون ممن لم تسعفني الذاكرة بذكرهم بالشكر، فجزاهم الله عني خير الجزاء.

وختاماً أسال الله العلي القدير أن يكون هذا العمل خالصاً لوجهه، وأن يجعله علماً نافعاً، ويسهّل لي به طريقاً إلى الجنة.

مصطلحات الدراسة:

تبحث هذه الدراسة في واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة، وقد وردت مفاهيم ومصطلحات تخدم هذه الدراسة، ولهذه المفاهيم والمصطلحات تعريفات نظرية وأخرى إجرائية، وقد تم اعتماد التعريفات الآتية:

معايير أمن المعلومات:

يعرف المعيار بأنه مجموعة محددة مسبقاً من القواعد والشروط أو المتطلبات المتعلقة بتعريف المصطلحات، وتصنيف المكونات، وتحديد المواد، والأداء والإجراءات، وتخطيط العمليات، والقياسات الكمية أو الجودة لتوصيف المواد، والمنتجات، والأنظمة، والخدمات أو الممارسات (السالمي، 2001)

معيار (ISO27002):

يختص هذا المعيار بضوابط أمن المعلومات، ويمثل الموجه لتطبيق ضوابط أمن المعلومات في المؤسسة، وإنَّ سياسات أمن المعلومات تعتبر أحد مكونات هذا المعيار، ويشير المعيار أنه يجب على المؤسسات أن تعرف سياسات أمن المعلومات لديها لتوجه وترشد العاملين تجاه قضايا أمن المعلومات (العربي، 2014).

جودة الخدمات:

مجموعة الصفات والخصائص التي يتميز بها المنتج أو الخدمة، والتي تؤدي إلى تلبية حاجات المستهلكين والعملاء سواء من حيث تصميم المنتج أو تصنيعه أو قدرته على الأداء في سبيل الوصول إلى إرضاء هؤلاء العملاء وإسعادهم (الدهيمات، 2011).

ملخص الدراسة

هدفت هذه الدراسة إلى بيان واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة، ولتحقيق أهداف الدراسة تم استخدام المنهج الوصفي التحليلي، ومن أجل تلك الغاية تم تصميم استبانة للحصول على البيانات اللازمة لهذه الدراسة، وتم توزيعها على مجتمع الدراسة المكون من المدراء والإداريين والعاملين في الإدارة العليا والوسطى، ودوائر شبكات المعلومات، وتكنولوجيا المعلومات بالجامعات الحكومية والأهلية والخاصة في قطاع غزة (جامعة الأزهر، الجامعة الإسلامية، جامعة الأقصى، جامعة فلسطين) والبالغ عددهم (601). وتم اختيار عينة طبقية عشوائية تمثلت في (333) مفردة، وبعد جمع البيانات تم معالجتها إحصائياً من خلال برنامج الرزم الإحصائية للعلوم الاجتماعية (SPSS).

وتوصلت الدراسة إلى عدة نتائج أهمها:

أن مستوى تطبيق معايير أمن المعلومات في الجامعات الفلسطينية كان بدرجة كبيرة وبنسبة (70.75%)، وكان مستوى جودة الخدمات في الجامعات الفلسطينية بدرجة كبيرة وبنسبة (70.49%)، كما توصلت الدراسة إلى وجود علاقة طردية قوية بين تطبيق معايير أمن المعلومات، وجودة الخدمات المقدمة في الجامعات الفلسطينية.

وكانت أهم التوصيات، ضرورة الاهتمام بمستوى تطبيق معايير أمن المعلومات في الجامعات الفلسطينية وذلك لعلاقتها وأثرها الواضح على جودة الخدمات التي تقدمها للطلبة، والعمل على زيادة جودة الخدمات التي تقدمها الجامعات الفلسطينية إلى الطلاب؛ وذلك حتى تكون عنصر جذب للطلاب إلى الجامعات الفلسطينية في ظل المنافسة الشديدة التي يشهدها قطاع التعليم العالي في ظل الظروف الاقتصادية الصعبة التي يمرُّ بها طلاب القطاع.

الكلمات الدالة: أمن المعلومات، الجامعات الفلسطينية، جودة الخدمات.

"The reality of the application of information security standards (ISO-IEC 27002) in Palestinian universities and their relationship to the quality of services provided"

Prepared by: Humam Salem Smara El masri

Supervisor: Mohammed Abed Abo Seda

Absract:

The aim of this study was to demonstrate the Reality of the Application of Information Security Standards (ISO-IEC 27002) in Palestinian Universities and Their Relation to The Quality of Services Provided. To achieve the objectives of the study, the analytical descriptive method was adopted. To this end, a questionnaire was designed to obtain the necessary data for this study. Distributed to the population of the study which consists of managers, administrators and employees of the senior and middle management, the information networks and information technology in public and private universities in the Gaza Strip. A random sample of 333 individuals was selected. After the data were collected, they were processed statistically through the Statistical Packages for Social Sciences (SPSS) program.

The results of the study indicate that:

The level of application of information security standards in the Palestinian universities was significantly by (70.75%). The quality of services in the Palestinian universities was significantly by (70.49%). In addition, a strong correlation between the application of information security standards and the quality of services provided in Palestinian universities.

The key recommendations include paying attention to the level of application of information security standards in Palestinian universities because of their relationship and its obvious impact on the quality of services provided to students. In addition, there is a need to promote the quality of services provided by Palestinian universities to students in order to attract students in light of the serious competition in the higher education sector in light of the difficult economic conditions experienced by students in Gaza strip.

Keywords: Information Security, Palestinian Universities, Quality of Services.

الفصل الأول

خلفية الدراسة

1.1 مقدمة الدراسة

يعد معيار أمن معلومات الموارد البشرية من أهم معايير أمن المعلومات المعروفة اختصاراً بـ (ISO-IEC..27002)، وذلك لأهمية العنصر البشري باعتباره أحد وأهم عناصر الإنتاج في أي منظمة، واعتماد كل المعايير الأخرى على مدى الكفاءة في تحقيق أمن هذا المعيار، ولكن لتحقيق التكامل في الوظيفة الأمنية للمعلومات وجب الاهتمام بكل معايير أمن المعلومات (السالمي، 2001).

فتزداد أهمية البيانات والمعلومات في الشركات والمؤسسات نتيجة دقة المنافسة، وحاجتها للوصول لمعلومات سريعة، وخالية من الاختراق أو لضمان سلامة المعلومات باعتبارها أحد أهم أصول المنظمة الحديثة، ولهذا يجب وضع كافة الإجراءات والتدابير اللازمة للمحافظة على أصول المنظمة؛ وذلك من خلال المحافظة على الأجهزة والبرامج والأفراد من الاختراق (المصري والأغا، 2018).

وتواجه منظمات الأعمال العديد من التحديات المرتبطة بازدياد المنافسة في جميع المجالات، والتي كان من أهم أسباب ظهورها ما يسمى بالعولمة والتطور التكنولوجي، اللذين ساهما بدورهما في إزالة الحواجز والحدود بين منظمات الأعمال من جهة والعملاء من جهة أخرى، حيث أصبحت الحدود بين الدول آخر ما يعيق المنظمة في تحقيق أهدافها في الانتشار حول العالم.

وبما أنَّ الفضاء الإلكتروني فضاءٌ عالميٌ وسريعُ التغير، ويصعب إحكام السيطرة عليه؛ فقد كثرت الأخطار التي تهدد أمن شبكات الحاسوب والبرامج المتصلة بالإنترنت، وغدت سلامة البيانات المحتضنة في خزائنها عرضة للانتهاك والقرصنة والتعديل والتزوير، والإصابة بالفيروسات والبرامج الضارة والتعرض لمحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث (عمار والكبيسي، 2012).

ولأهمية أمن المعلومات لكل من المؤسسات الحكومية والخاصة، والذي أصبح من الضرورة عدم الاستغناء عنها في ظل التطور المستمر في تقنيات المعلومات وما صاحبه من تطور في اختراق البيانات والمعلومات، لذا حرصت كثير من المنظمات العالمية وعلى رأسها المنظمة الدولية للتوحيد القياسي (أيزو) على وضع معايير لضبط أمن المعلومات بالمؤسسات والمنظمات، وهي منظمة تعمل على وضع المعايير وتضم عدة ممثلين من عدة منظمات قومية للمعايير، وهي تعتبر أحد أهم وأقوى المنظمات غير الحكومية بسبب أن معظم معاييرها تحولت إلى قوانين وفق معاهدات ومعايير قومية (العربي، 2015).

كما ويحظى موضوع الجودة حالياً باهتمام من قبل جميع المؤسسات التعليمية في جميع أنحاء العالم المتقدم والنامي على السواء، بعد أن انتبهت تلك المؤسسات إلى أهمية تطوير وتحسين الأداء كمدخل أساسي لمواجهة التحديات الداخلية والخارجية خاصة بعد التطورات التكنولوجية والاتجاه نحو العولمة (الحدابي وقشوة، 2009).

وتعدُّ الجامعات من المؤسسات الرئيسة والحساسة، والتي يجب أن تكون السباقة في تطبيق أفضل المعايير؛ لأنها وجدت للبناء والتنمية وتخريج طلبة ذوي كفاءة عالية لخدمة المجتمع، وتنشئة أجيال صالحة؛ فالجامعات لها علاقاتها التبادلية مع المجتمع (الكسر، 2018).

من هنا جاءت فكرة دراسة واقع معايير أمن المعلومات (ISO-IEC..27002) وهي بمسمى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات في الجامعات الفلسطينية، وعلاقتها بجودة الخدمة المقدمة للطلبة، لنحاول الوصول إلى نموذج تستفيد منه الجامعات والباحثون.

2.1 مشكلة الدراسة

حظي موضوع جودة التعليم العالي باهتمام واسع في أدبيات الدراسة ذات الصلة بجودة مخرجات التعليم الجامعي، كما أن الكثير من الدراسات اتجهت إلى قياس رضا الطلاب عن جوانب كثيرة مما تقدمه الجامعة كمدخل من المداخل لتحسين جودة التعليم العالي ومخرجاته (بن جمعة، 2015).

كما أن اختراق أنظمة المعلومات، ونظم الشبكات والمواقع المعلوماتية أصبح خطراً كبيراً يثير قلق الكثير من المنظمات في السنوات الأخيرة، ومع مرور الزمن نجد أنه على الرغم من سبل الحماية المتبعة في المنظمات، إلا أنَّ هناك ارتفاعاً واضحاً في معدل الاختراقات مع تنوع الوسائل المستخدمة في الاختراق، ومن هذه المخاطر التي تحيط بالمنظمات سرقة المعلومات أو إدخال الفيروسات، وهي التي تعتبر أشد خطراً وضرراً على المعلومات، كما أنه من الصعب التنبؤ بالمخاطر والدوافع العدائية للأشخاص، كما أن هناك بعض الأخطار المتمثلة بالأخطاء البشرية والكوارث الطبيعية (العربي، 2015).

ولهذا فإنَّ الجامعات تقدم مجموعة واسعة من الخدمات، تسعى أن تكون هذه الخدمات مرضية، وعند النظر إلى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات والأهمية التي توليها المنظمات لها، وعلى الرغم من أن الجامعات الفلسطينية تضع معايير لأمن المعلومات الا أنه هناك حالات اختراق لأنظمتها الامر الذي يثير القلق تجاه هذه المعلومات.

لكل ما تقدم فلقد بات من الضرورة أن يتم معالجة هذا الضعف في الأداء؛ لذلك جاءت هذه الدراسة لمحاولة الاجابة عن السؤال الرئيسي الآتي:

ما أثر تطبيق معايير أمن المعلومات (ISO-IEC 27002) على جودة الخدمات المقدمة في الجامعات الفلسطينية ؟

3.1 مبررات الدراسة

تعتبر هذه الدراسة استكمالاً لما بدأه الآخرون في موضوع أمن المعلومات، ويعتبر من الموضوعات المهمة جداً في ظل التطور الرهيب للتكنولوجيا بشكل عام، وتكنولوجيا المعلومات بشكل خاص، كما أن الجامعات تعتبر من المؤسسات المهمة على صعيد الوطن والمواطن، وبالتالي فإن أي شيء يمكن أن يؤثر على الجامعة له من التأثير الكبير على مستوى الوطن ككل، وقد أتت هذه الدراسة للتأكيد على أهمية أمن المعلومات في الجامعات الفلسطينية، ومدى إمكانية ارتباط أمن المعلومات بجودة الخدمات التي تقدمها الجامعات للطلبة.

4.1 أهداف الدراسة

تسعى هذه الدراسة للخروج بإطار نظري يساهم في معرفة واقع قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية، ومدى ارتباطها بجودة الخدمات المقدمة للطلبة كهدف رئيسي يتفرع منه مجموعة من الأهداف الفرعية:

1- الكشف عن أهم مقومات إدارة أمن المعلومات (ISO-IEC 27002).
2- التعرف على واقع إدارة أمن المعلومات (ISO-IEC27002) في الجامعات الفلسطينية.
3- بيان مستوى جودة الخدمات المقدمة للطلبة من قبل الجامعات الفلسطينية.
4- إبراز طبيعة العلاقة بين أبعاد إدارة أمن المعلومات (ISO-IEC27002)، وجودة الخدمات المقدمة للطلبة من قبل الجامعات الفلسطينية.
5- التعرف على مقدار التغير في جودة الخدمات المقدمة في الجامعات الفلسطينية نتيجة التغير في إدارة أمن المعلومات (ISO-IEC 27002).
6- التعرف على دلالة التفاوت بين استجابات المبحوثين حول واقع معايير أمن المعلومات (ISO-IEC27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة للطلبة وفق خصائص المبحوثين الديموغرافية.

5.1 أسئلة الدراسة:

1- ما مستوى كل من (أمن الموارد البشرية، وتقييم المخاطر ومعالجتها، والسياسة الأمنية، وتنظيم أمن المعلومات، والأمن المادي والبيئي، والاتصالات وإدارة العمليات) في الجامعات الفلسطينية؟

2- ما مستوى جودة الخدمات المقدمة للطلبة في الجامعات الفلسطينية من وجهة الإدارة؟

3- ما هي طبيعة العلاقة بين معايير أمن المعلومات (ISO-IEC..27002)، وجودة الخدمات المقدمة للطلبة في الجامعات الفلسطينية؟

4- هل يوجد أثر ذو دلالة إحصائية لإدارة أمن المعلومات على جودة الخدمات المقدمة للطلبة في الجامعات الفلسطينية؟

5- هل يوجد فروق ذات دلالة إحصائية بين استجابات العاملين حول "قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC..27002)" تُعزى للمتغيرات الديمغرافية (الجنس، والجامعة، والمؤهل، والمسمى الوظيفي، والتخصص)؟

6.1 فرضيات الدراسة ومتغيراتها:

أولاً: فرضيات الدراسة:

1- تتوفر قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات في الجامعات الفلسطينية (ISO-IEC 27002) بمستوى لا يقل عن (60%).

2- لا تقل مستوى جودة الخدمات المقدمة للطلبة في الجامعات الفلسطينية عن (60%).

3- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لأبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC..27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، ويتفرع منها ما يلي:

- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين أمن الموارد البشرية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.
- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تقييم المخاطر ومعالجتها في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.

- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين السياسة الأمنية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.
- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تنظيم أمن المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.
- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين الأمن المادي والبيئي في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.
- توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين الاتصالات وإدارة العمليات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.

4- يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لأبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية على جودة الخدمات المقدمة للطلبة.

5- توجد فروق ذات دلالة إحصائية في استجابات العاملين حول "مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC..27002)" تُعزى للمتغيرات الديموغرافية (الجنس، والجامعة، والمؤهل، والمسمى الوظيفي، والتخصص).

ثانياً: متغيرات الدراسة:

- **المتغير المستقل: معايير أمن المعلومات(ISO-IEC 27002) وأبعادها تشمل:**
  - سياسات أمن المعلومات
  - تنظيم أمن المعلومات
  - أمن الموارد البشرية
  - ادارة الأصول
  - التحكم في الوصول
  - التشفير
  - الأمن المادي والبيئي

- أمن العمليات
- أمن الاتصالات
- اكتساب النظام وتطويره وصيانته
- علاقات الموردين
- ادارة حوادث أمن المعلومات
- جوانب أمن المعلومات في ادارة استمرارية الأعمال
- الامتثال

- **المتغير التابع: جودة الخدمات المقدمة للطلبة**

7.1 حدود الدراسة

الحد المكاني: الجامعات الأهلية في قطاع غزة (جامعة الأزهر، الجامعة الإسلامية)، والجامعات الخاصة (جامعة فلسطين)، والجامعة الحكومية (جامعة الأقصى).

الحد الزماني: السنة الدراسية 2018 / 2019.

الحد البشري: العاملون في الإدارة العليا والوسطى، ودوائر شبكات المعلومات، وتكنولوجيا المعلومات بالجامعات المذكورة.

الحد الموضوعي: سيتم دراسة لأنظمة إدارة أمن المعلومات في الجامعات الفلسطينية المذكورة، وعلاقتها بمستوى جودة الخدمات المقدمة للطلبة.

8.1 مجتمع الدراسة:

يتكون مجتمع الدراسة من المدراء، والإداريين، والعاملين في الإدارة العليا والوسطى ودوائر شبكات المعلومات، وتكنولوجيا المعلومات بالجامعات الأهلية في قطاع غزة (جامعة الأزهر، الجامعة الإسلامية)، والجامعات الخاصة (جامعة فلسطين)، والجامعة الحكومية (جامعة الأقصى).

9.1 محددات الدراسة ومعوقاتها:

- لا تشمل هذه الدراسة جميع الجامعات الفلسطينية، وتشمل الجامعات الأهلية في قطاع غزة (جامعة الأزهر، والجامعة الإسلامية) والجامعات الخاصة(جامعة فلسطين)، والجامعة الحكومية (جامعة الأقصى).
- ندرة الدراسات السابقة التي تناولت المعيار (ISO-IEC 27002) بالتحديد.
- صعوبة الحصول على المعلومات حيثُ أنَّ بعض المعلومات تصنف تحت بند المعلومات الخاصة والسرية.

10.1 هيكل الدراسة

جاءت هيكلية الدراسة مقسمة الى ستة فصول كالآتي:

- **الفصل الأول** (خلفية الدراسة): وفيه يتم تعريف مشكلة الدراسة ومبرراتها، ويتم تحديد أهمية الدراسة، والهدف الرئيسي لهذه الدراسة، والأهداف الفرعية، ويتم تحديد السؤال الرئيسي والأسئلة الفرعية بالإضافة لتحديد فرضيات هذه الدراسة، وتحديد هيكلية الدراسة بشكل كامل.
- **الفصل الثاني** (الإطار النظري): وينقسم إلى أربعة مباحث:
  - **المبحث الأول:** ويتحدث عن أمن المعلومات، ومعايير أمن المعلومات والتركيز على المعيار (ISO-IEC 27002).
  - **المبحث الثاني:** يسلط الضوء على جودة الخدمات التي تقدمها الجامعات الفلسطينية.
  - **المبحث الثالث:** يتضمن الحديث عن الجامعات في قطاع غزة.
  - **المبحث الرابع** (الدراسات السابقة):

سوف يتم تلخيص الدراسات السابقة التي تم طرحها وتناولها بالدراسة، ويتم التأكد من أن هناك فجوة علمية فعلاً حول موضوع الدراسة، بالإضافة لصياغة جدول مقارنة بين هذه الدراسات لتسليط الضوء على أهداف ونتائج وتوصيات كل دراسة، ومقارنتها مع الدراسة الحالية.

- **الفصل الثالث** (منهجية الدراسة وإجراءاتها):

وفي هذا الفصل يتم تحديد منهج الدراسة؛ وهو المنهج الوصفي التحليلي، ويتم وضع خطة لآلية جمع البيانات الخاصة بالدراسة، وذلك من خلال المراجع والدراسات والأبحاث السابقة، والتقارير الصحفية والمقالات ذات العلاقة، ويتم جمع البيانات من خلال أداة جمع البيانات وهي الاستبانة، لذا سيتم تصميم استبانة تساعد في جمع البيانات من خلال توزيعها على المبحوثين بعد أن يتم تحديد عينة الدراسة، ثم تعبئته من خلال العينة المحددة.

- **الفصل الرابع** (النتائج ومناقشتها): في هذا الفصل يتم تفريغ الاستبانة باستخدام برنامج التحليل الإحصائي (SPSS) ويتم أخذ نتائج التحليل الإحصائي التي ستتم ترجمتها إلى نتائج واضحة ومقروءة، ونسب ذات علاقة بأسئلة وفروض الدراسة.
- **الفصل الخامس** (الاستنتاجات والتوصيات): في هذا الفصل ثم تحديد الاستنتاجات التي استنتجت من خلال الدراسة، ويتم تنفيذ إجراءاتها ومنهجيتها، وتم وضع التوصيات التي ساعدت على حل المشكلة الأساسية للدراسة، ووضع العديد من التصورات لبحوث مستقبلية تساهم في معالجة مشاكل لها علاقة وثيقة بموضوع الدراسة.

❖ وأخيرا تم الحاق الفصول بقائمة أهم المراجع والملاحق:

- **المراجع:** هنا يتم تحديد جميع المراجع التي ساهمت في إخراج هذه الدراسة بالشكل العلمي الصحيح.
- **الملاحق:** يتم وضع الملاحق كالتقارير، والاستبانة، والصور، وأي ملاحق أخرى تم استخدامها خلال عملية الدراسة.

الفصل الثاني

الإطار النظري والدراسات السابقة

1.2 المبحث الأول: أمن المعلومات

1.1.2 مفهوم أمن المعلومات:

يقصد بأمن المعلومات مجموعة العمليات والإجراءات والأدوات، التي تتخذها القطاعات، أو المنظمات لتأمين وحماية معلوماتها وأنظمتها ووسائطها من وصول غير المصرح لهم، سواء من هم من داخل القطاع أو خارجه (الأبروي، 2010).

ويرى بعضهم أنها الحفاظ على سرية وتوفر وسلامة المعلومات كأصل، في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية، وذلك من خلال تعزيز الوعي والتعلم والتدريب (Whitman & Mattord, 2011).

كما وتعتبر مجموعة الإجراءات المستخدمة لتوفير سلامة وسرية وتوفر المعلومات حين طلبها وفق صلاحية دخول لنظام المعلومات معروفة مسبقاً وموافقاً عليها (الدنف، 2013).

لقد أخذ بعضهم مفهوم أمن المعلومات من زاوية قانونية، وذلك بوجوب وضع التشريعات والقوانين لحماية المعلومات، وبعضهم الآخر أخذه من زاوية تقنية بوضع الأدوات والوسائل لحماية المعلومات، ولكون أمن المعلومات أحد عناصر البنية الأساسية التي يجب أن تتاح لأمن نظام المعلومات الخاص بالمؤسسة فعند التخطيط له يجب توازن قيمة المعلومات لإدارة المؤسسة مع الحجم النسبي لأنواع المعلومات في مواجهة حد الأمن المتوسط في الأساس، وفي كثير من المؤسسات، والأجهزة الحكومية تتوافر منظومات أمن صارمة لمعالجة وتخزين واسترجاع المعلومات ونقلها بطريقة تحمي سريتها وسلامتها في مستودعاتها المقروءة آلياً (عبد الكريم والربيعي، 2013).

ويرى (علي، 2017) بأن أمن المعلومات هو حماية البيانات ونظم المعلومات من الوصول، أو الاستخدام، أو الإفصاح، أو التعطيل أو التعديل أو التدمير غير المصرح به. ويتحقق أمن المعلومات من خلال ضمان سرية المعلومات، وسلامتها وتوافرها.

وهو مجموع الإجراءات والتدابير المستخدمة في المجالين: الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمداً عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير وافية، والمستخدمة من إدارة هذه المصادر (مقراني، 2016).

وهو السيطرة والتحكم في البيانات، ونقلها، ونشرها، وحمايتها من المخاطر الداخلية والخارجية التي تهددها، ومن أنشطة الاعتداء عليها (الحانوتي، 2014).

كما أنها الطرق والوسائل المعتمدة للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من السرقة، والتشويه، والابتزاز، والتلف، والضياع، والتزوير، والاستخدام غير الشرعي المرخص، وغير القانوني.

وهو كذلك حماية جميع أنواع المعلومات ومصادر الأدوات التي تتعامل معها وتعالجها، من منظمة وغرفة تشغيل أجهزة، والأجهزة ووسائط التخزين والأفراد من السرقة والتزوير والضياع والاختراق، وذلك باتباع إجراءات وقائية وضوابط محددة (حمودة، 2014).

وتعرف أمن المعلومات على أنها حماية المعلومات من الوصول غير المسموح به (القحطاني، 2015).

وقد أشار كل من (Calder& Watkins, 2012) أن أمن المعلومات يعنى بحماية موارد المعلومات من مختلف التهديدات من أجل ضمان استمرارية الأعمال، وتقليل المخاطر، وتعظيم العائد من الاستثمارات والفرص.

ويرى (البكري، 2017) أن أمن المعلومات هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها، ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية؛ فإنَّ أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات، ومكافحة أنشطة الاعتداء عليها واستغلال نظمها في ارتكاب الجريمة (جرائم الكمبيوتر والإنترنت).

إنَّ أمن المعلومات عبارة عن مجموعة من الإجراءات الإدارية والتقنية التي يتم اتخاذها لضمان توفير الحماية اللازمة للمعلومات من التهديدات الداخلية أو الخارجية (عبد الواحد، 2015).

ويرى (عبد الجابر، 2013) بأن أمن المعلومات يتمثل في درجة الثقة بالأمن والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام.

ومفهومه بشكل أوسع وأشمل يعني حماية المعلومات وعناصرها المهمة والأساسية، ومن بينهم تلك الأنظمة والأجهزة وجميع المستلزمات التي تستخدم هذه المعلومات وتخزنها وترسلها (Sharma, 2015).

يشتمل مفهوم أمن المعلومات على المحاور الآتية (القحطاني، 2015):

1. حماية المعلومات من الضرر بأشكاله كافة، سواء كان مصدره أشخاصاً أو برامج.
2. حماية المعلومات من الوصول غير المصرح به، أو السرقة، أو الالتقاط.
3. حماية قدرة المنشأة على الاستمرار وأداء أعمالها على أحسن وجه.
4. تمكين أنظمة تقنية المعلومات والبرامج التطبيقية لدى المنشأة من العمل بشكل آمن.

ويرى الباحث أن كل مؤسسة تحتاج الى أحد أهم الوظائف التي حددها العالم هنري فايول والتي تتعلق بحماية وأمن المؤسسة وهي الوظيفة الأمنية، وهي ضمن ستة وظائف أساسية للمنظمة، وتمثل الوظيفة الأمنية حماية الممتلكات والأصول للمنظمة، وتعتبر في الوقت

الحالي المعلومات أهم الأصول المعنوية للمنظمة، فالحفاظ عليها من سرقة أو وصول الأشخاص غير المصرح لهم سواء من داخل المؤسسة أو من خارجها.

ولحماية أمن المعلومات لابد من حماية الأجهزة والبرامج والتأكد من المستخدمين وسلامة تعاملهم مع البرامج.

2.1.2 أهمية أمن المعلومات:

لقد أصبح لأمن المعلومات أهمية كبيرة وضرورة لا غنى عنها في ظل التطور المستمر والسريع في تقنيات المعلومات، والذي يؤدي بدوره إلى تطور مستمر وسريع في أساليب اختراق البيانات والمعلومات، لذا تكمن أهمية أمن المعلومات في (المصري والأغا، 2018):

- تعمل على تقليل المخاطر التي قد تؤثر على توافر المعلومات وسريتها وسلامتها، بمستوى مقبول ومحدد.
- أمن المعلومات لم يعد قضية يتولاها فنيون وتكنوقراط داخل المنظمات كل على حدة بشكل مجزأ، بل أصبحت من القضايا التي يتولاها سياسيون، واستراتيجيون، وصناع قرار يترجمونها في صورة سياسات، واستراتيجيات تعمل ضمن منظومة واحدة متكاملة بما يكفل ضبط العلاقة ما بين نظام أمن المعلومات وأمن المنظمة، وتوجهها في مسارها الصحيح.
- تعتبر جزءاً أساسياً من عمليات الإدارة الناجحة.
- تساعد على خفض المخاطر إلى الحد الأدنى.

ويرى الباحث أن أهمية أمن المعلومات تنبع من أهمية المعلومات في الوقت الحالي، حيث تعتبر جزء أساسي من المنافسة ومن تحديد احتياجات ورغبات المستخدمين.

3.1.2 أهداف أمن المعلومات:

إن الهدف المرجو من أمن المعلومات هو حماية المعلومات الخاصة بالمنظمة من العبث أو الفقدان، مع مراعاة الحيلولة دون تحقيق أهداف وتطلعات المنظمة، حيثُ أنَّ الهدف من أمن المعلومات يجب أن تتفق مع أهداف المنظمة، وذلك من خلال تحقيق الأمور الآتية (الأبروي، 2010):

1. الخصوصية أو السرية: وهي خصوصية المعلومات المتعلقة بالعملاء أو بالمنظمة، بحيث تكون بعيد عن وصول غير المصرح لهم بالاطلاع عليها.

2. السلامة للمعلومات والأنظمة: إنَّ البيانات لا يمكن أن يحدث لها استحداث أو تغيير أو حذف من غير تصريح، وكذلك تعني أن البيانات المخزنة في أحد أجزاء جداول قواعد البيانات متوافقة مع ما يقابلها من البيانات المخزنة في جزء آخر من قواعد البيانات.
3. التوفر بشكل دائم: حيث تكون متوفرة عند الحاجة لها.
4. الوعي الأمني للمعلومات: ويقصد به ضرورة وجود وعي ببرامج التجسس أو الفيروسات، لتقليل تعرض البيانات من خطر التلف أو السرقة أو العبث.

كما يرى (Whitman & Mattord, 2011) أن أي مؤسسة تهدف إلى إدارة أمن المعلومات لا بُدَّ من توفر المكونات الآتية:

1. الأمن المادي: ويشمل المصادر والممتلكات والمباني لمنع الوصول غير المشروع.
2. أمن الأفراد: لحماية الأفراد والمجموعات الذين لهم حق الوصول للمعلومات.
3. أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون.
4. أمن الاتصالات: لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى.
5. أمن الشبكات: لحماية مكونات الشبكة والتراسل والمحتويات.
6. أمن البيانات: لحماية سرية وسلامة وتوافر المعلومات.

ويذكر (عبد الكريم والربيعي، 2013) أن الأهداف قد تكون عامة، وقد يكون بعضها خاصة، فمنع حصول الاختراقات الأمنية قدر الإمكان، من خارج أو حتى من داخل الشركة الواحدة للأشخاص غير المصرح لهم، والحد من مهاجمة الفيروسات للبنية التحتية، والتقليل أو حتى منع وصول الرسائل الإلكترونية غير المرغوب فيها، هذه الأهداف وما شابهها عامة ومشتركة.

وترى (يونس، 2017) أن المنظمات إذ تسعى لتحقيق أمن نظم المعلومات فإن غايتها تحقيق الثالوث المسمى (CIA Triangle) ويعني السرية والخصوصية (Confidentiality)، التكاملية والسلامة (Integrity)، والتوفر والإتاحة (Availability).

4.1.2 مخاطر تهدد أمن المعلومات:

صنفها الحانوتي (2014) إلى صنفين رئيسيين:

1. مخاطر داخلية: وتشمل موظفي المؤسسة، والمتدربين، والموظفين المؤقتين، والتابعين لشركات أخرى تعمل داخل المؤسسة، والمستشارين، والمقاولين، وشركاء العمل، حيث تعتبر التهديدات الداخلية أشد خطورة من الخارجية أنها تحدث ضرراً أكبر من الخارجية.
2. مخاطر خارجية: ومن أمثلتها: محترفي أنظمة المعلومات، والجواسيس والمتطفلين، كما أن الفيروسات وملفات الكوكيز وغيرها من الملفات المستخدمة في عمليات التجسس والاختراق تحت صنف التهديدات الخارجية.

إن الاعتقاد السائد أن الجزء الأعظم من تهديدات أمن المعلومات يأتي غالباً من المصادر الخارجية، ولكن على النقيض من ذلك؛ فإنَّ الأشخاص الذين منحوا حق الوصول المعتمد للنظام يكونون أكثر فتكاً بأمن المعلومات أيضاً، فعلى الرغم من أنهم قد يكونون مؤتمنين أو عاملين من ذوي النوايا الحسنة، فإنهم ربما بفعل التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعالاً غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات المهمة للمنظمة (شبلي والنسور، 2009).

وقد ذكر (الدنف، 2013) تهديداً آخر وهو تهديد نقص التدريب والتوعية، حيث إن هذا النقص سوف يؤدي إلى الجهل بنظام المعلومات، ونقص الدورات التدريبية تجعل الكثيرَ من العاملين والمستخدمين جهلة بأغراض الأضرار التابعة من سوء استخدام النظام، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلى ممارسات وأفعال تعود بالإساءة لأمن نظم المعلومات.

كما صنفها بعضهم من حيث نية الشخص بالتهديد للمنظمة إلى نوعين:

1. مخاطر متعمدة: وهي إذا تم تهديد أمن المعلومات من قبل شخص بغرض العداء للمؤسسة، ضمن محاولة مقصودة للإضرار بأنظمة المؤسسة سواء كان هذا الشخص من داخل المؤسسة أو من خارجها.
2. مخاطر غير متعمدة: وهي المخاطر التي تأتي من قبل أشخاص نتيجة سوء التصرف أو الإهمال في تطبيق الأنظمة، ومثال ذلك ترك باب الغرفة مفتوحاً، وإعطاء كلمة السر الخاصة بموظف له صلاحيات كبيرة لموظف آخر لمساعدته في العمل.

5.1.2 طرق انتهاك أمن المعلومات:

يمكن تصنيف أشكال وطرق انتهاك أمن المعلومات إلى ثلاثة أنواع (الحانوتي، 2014):

1. الاشتراك بالأجهزة: ويقصد به اشتراك أكثر من شخص بالعمل على نفس الجهاز، الأمر الذي يتيح لشخص لديه خبرة بالحاسوب من تتبع نشاط أي شخص يستخدم الجهاز، والاطلاع على جميع الملفات قد تكون بعضها سرية لا سيما إذا كان هناك صور شخصية، ولعل أكبر مثال على مثل هذا النوع هو مقاهي الإنترنت، ومختبرات الحاسوب بالمؤسسات التعليمية.
2. برامج تجسس إلكترونية: وتعتبر أكثر الطرق شيوعاً، وتعتمد على القيام بزرع برامج معينة على أجهزة الحاسوب، تهدف إلى البحث عن معلومات معينة وإعادة إرسالها إلى الجاني، أو أي جهة أخرى، ويتم ترويج هذه البرامج من خلال الإعلانات، والحملات الترويجية التي تناسب اهتمامات المستخدم.
3. اعتراض البيانات: وهي الطريقة الأقل شيوعاً بسبب حاجتها إلى تقنيات عالية وأشخاص محترفين للقيام بهذه المهمة، كما أن الطريقة تستخدم عادة لمهمات محددة، وتقوم هذه الطريقة على مراقبة شبكات الاتصالات، ونقل البيانات وعمل تصفية للبيانات التي تمر عبر هذه الشبكات بحثاً عن نوع معين من المعلومات.

ويمكن تصنيف طرق اختراق أمن المعلومات كالآتي (الطائي، 2004):

1. التجسس التنافسي: وهي عملية الدخول غير المشروع إلى معلومات المؤسسة بسبب زيادة حدة التنافس، وانخفاض هامش الربح، من خلال التنصت، والتفتيش الدقيق في نفايات الشركة، والالتقاط الذهبي للمعلومات من شاشة الحاسوب.
2. سوء استخدام المعلومات: ويقصد بها إساءة استخدام المعلومات من قبل الأشخاص المخولين بالاطلاع على المعلومات لأهداف شخصية أو لتحقيق مبالغ مالية من المنافسين.
3. الإهمال: وهو التهاون وضعف الإدراك لأهمية الاحتفاظ بسرية المعلومات، أو عدم معرفتهم المعلومات التي تحتاج للحماية، ومن يمتلك الدافع لسرقتها سواء من داخل المؤسسة أو من خارجها.
4. تدمير المعلومات: وتتم عن طريق استخدام الفيروسات التي تعمل على إتلاف البرامج والمعلومات، وحذفها وتحريفها وإعادة تسميتها، أو تغيير تواريخ تخزينها.

6.1.2 عناصر أمن المعلومات:

تعرف عناصر أمن المعلومات على أنها: مجموعة العناصر الواجب توافرها لحماية المعلومات الثابتة والمنقولة؛ بحيث يغطي كل عنصر من هذه العناصر جانباً من جوانب الحماية المطلوبة، ولقد أظهرت التقنيات الحديثة الحاجة إلى عنصرين مهمين من عناصر أمن المعلومات قد لا يكون لهما مقابل في حال الرسائل التقليدية، وهما (القحطاني، 2015):

1. عنصر التوفر.
2. عنصر التدقيق أو المتابعة.

صنفها الحانوتي (2014) إلى:

1. **عناصر خارجية:** وتتمثل في جميع الضوابط والإجراءات التي تحدد وتؤثر على أمن المعلومات وتتمثل في :
   - إجراءات ضبط الدخول إلى الموقع.
   - وجود حراس أمن على الأماكن الحساسة.
   - سجل حركات الدخول لغير الموظفين بالتاريخ والوقت.
   - إشارات تمييز للموظفين.
   - تواجد مركز أمن المعلومات الخاص بالجامعة بموقع مناسب وآمن.
   - نظام رقابة مركزي ومرئي من خلال كاميرات مراقبة وتسجيل.
2. **عناصر داخلية:** وتتمثل في:
   - مواقع الأماكن التي تحتوي على المعلومات الحساسة.
   - جاهزية المبنى لمقاومة الحريق.
   - أجهزة الكشف عن الدخان والحرائق.
   - مصادر خاصة للطاقة لمركز المعلومات لضمان أمنها.
   - نظام إضاءة خاص بحالات الطوارئ.
   - تسليم المفاتيح والإشارات الخاصة بالموظفين.
   - إعادة أجهزة الحاسوب أو أي أجهزة أخرى.
   - التوقيع على تعهد.
   - تغيير الأقفال.

- إلغاء أو إيقاف الحساب المستخدم للولوج إلى أجهزة الحاسب الآلي.

ويمكن استخدام معيار أو أكثر للتحقق من الهوية حسب درجة قوة التحقق المطلوبة، فيمكن التحقق باستخدام معيار واحد أو معيارين أو ثلاثة معايير كما يلي (القحطاني، 2015):

- باستخدام معيار واحد وهو "ماذا تعرف؟" كاستخدام كلمات المرور أو أرقام التعريف الشخصية.
- باستخدام معيارين؛ وذلك يتم من خلال استخدام معيار "ماذا تعرف؟" بالإضافة إلى معيار آخر وهو "ماذا تملك؟".
- باستخدام ثلاثة معايير، ويتم ذلك باستخدام معيار "ماذا تعرف؟" ومعيار "ماذا تملك" بالإضافة إلى معيار ثالث وهو "من أنت؟".

وتتمثل أهم وسائل تحقيق عناصر أمن المعلومات في ثلاث تقنيات رئيسة يمكن استخدامها كوحدات بناء أساسية لتحقيق بعض عناصر أمن المعلومات وهي:

1. التشفير بنوعيه المتناظر، وغير المتناظر.
2. التصديق الرقمي.
3. البصمة الرقمية.

أولاً: التشفير

وهو تحويل النص من مقروء ومفهوم إلى نص غير مقروء وغير مفهوم، وبطريقة لا يستطيع أحد معرفتها سوى الأطراف المتعارف عليها، وتحول النص غير المفهوم إلى نص مفهوم (السويل، 2007).

ثانياً: التصديق الرقمي

ويعتمد التصديق الرقمي بدرجة أساسية على الرسالة نفسها بالإضافة إلى توقيع الشخص المخول بالتصديق الرقمي من أجل إنتاج بصمة خاصة لكل رسالة؛ وبهذه الطريقة تكون هناك بصمة فريدة لكل رسالة بحيث لا تنطبق بصمتان لرسالتان مختلفتان حتى لو صدرت من الشخص نفسه.

ثالثاً: البصمة الرقمية

هي سلسلة قصيرة وثابتة الطول من البتات (Bits) تشكل بصمة فريدة لكل رسالة.

والسياسة الأمنية تعتبر أهم عنصر من عناصر أمن المعلومات، حيث يجب مراعاة الأمور والمتطلبات الآتية لتحقيق السياسة الأمنية (داوود، 2004):

1. التكلفة المناسبة والمعقولة.
2. توافقها مع أسلوب أداء العاملين واتصالها بالعالم الخارجي.
3. تلبي المتطلبات القانونية في بيئة المؤسسة.
4. تراعي العوامل الإجرائية لضمان سير العمل.
5. معقولية القيود وعدم تحجرها.

كما أن هناك عناصر لأمن المعلومات الحديثة وهي سبعة عناصر يمكن اختصارها كالآتي (القحطاني، 2015):

1. التحقق من الهوية:

تعني الخدمة التي يمكن من خلالها التحقق من هوية الشخص (أو الجهة)، وأنه الشخص المعني لا غيره، وفي حال النقل فإنه يجب التحقق من هوية المرسل لضمان أن المعلومة قادمة من مصدرها الحقيقي، وكذلك يجب التحقق من هوية المستلم لضمان أن المعلومة ذاهبة إلى وجهتها الصحيحة؛ لذلك يجب أن تتوافر في طريقة تحديد الهوية المعايير الآتية:

أ. أن تكون الهوية فريدة؛ أي أن تكون غير قابلة للتكرار.

ب. أن تكون غير مفصحة عن معلومات المستخدم، ووظيفته، والغرض من وصوله إلى المعلومة.

ت. أن لا تكون مشتركة بين المستخدمين.

ث. اتباع معايير التسمية المعتمدة عند المنشأة عند إنشاء حسابات المستخدمين.

2. التحكم بالوصول:

هو طرق أو وظائف الحماية التي تتحكم بوصول المستخدمين أو الأنظمة إلى موارد المنشأة، فتلك الطرق هي التي تحمي الأنظمة، وموارد المنشأة المختلفة من الوصول غير الشرعي، وكما أنها تساعد في تحديد مستوى التخويل المصرح به بعد نجاح عملية التحقق من الهوية.

3. السرية:

ويمكن أن يطلق على هذا العنصر أيضاً الخصوصية؛ وهي تعني الحفاظ على المعلومات من أن يطلع عليها ويقرأها غير الأشخاص المصرح لهم فقط، وهناك العديد من الطرق لتوفير السرية تتراوح بين حجب المعلومة يدوياً وعدم تسليمها إلى للأشخاص المصرح لهم فقط، إلى طرق التشفير الحديثة التي تعتمد على الخوارزميات الرياضية المعقدة، والتي يصعب فكها، ومن هنا يمكن القول: إنَّه يمكن توفير عنصر السرية من خلال تشفير البيانات سواء أكانت ثابتة أم منقولة، وتطبيق سياسة صارمة للتحكم بالوصول وتصنيف المعلومات وتدريب العاملين على أنظمة وسياسات أمن المعلومات تدريباً جيداً.

وقد أورد في هذا المجال عدة طرق لإحباط فعالية عنصر السرية؛ ومن أهمها:

- مراقبة الشبكة.
- هجوم التسلل من فوق الكتف.
- الهندسة الاجتماعية.
- غياب الحس الأمني لدى المستخدم.

4. سلامة المعلومة وتكاملها:

وتعني الخدمة التي يمكن من خلالها الحفاظ على سلامة المعلومة من التعديل أو الحذف أو الإضافة أو إعادة التوجيه، ويهتم هذا العنصر بعملية كشف عدم سلامة المعلومة وتكاملها أكثر من اهتمامه بعملية منع التعديل على المعلومة أو تصحيح ذلك التعديل.

5. عدم الإنكار:

وهي الخدمة التي من خلالها يمكن من أي شخص أو جهة من إنكار أي عملية قاموا بها وكشفهم، ويلعب هذا العنصر دوراً رئيساً في إثبات وقوع العمليات التفاعلية (بين طرفين) كالعمليات المالية وعمليات الحكومة الإلكترونية.

6. توافر المعلومة:

ويقصد بها أن تكون قابلة للوصول إليها، أو أن يتم استخراجها وقراءتها حين الطلب من قبل أي شخص، وفي أي وقت.

ويمكن القول: إنَّ خدمة التوافر هي الخدمة التي تحمي النظام ليبقى متاحاً دائماً (ومن هنا يطلق عليها أحياناً الديمومة)، حيثُ إنَّ الهدف العام من عنصر توافر المعلومة هو أن تكون الشبكة والأجهزة والأنظمة والبرامج والخدمات متاحة في جميع الأوقات التي يحتاج إليها المستخدم.

7. المتابعة أو التدقيق:

ويطلق عليها أحياناً المحاسبة، وتهدف إلى متابعة عمليات المستخدمين والتحقق من فرض سياسات أمن المعلومات وأنها تطبق بشكل صحيح ودقيق، وهناك أسباب عديدة وراء ضرورة إجراء عمليات التدقيق والمتابعة على موارد الشبكة ومستخدميها، ونجملها فيما يلي:

- التحقق من أن الأجهزة والأنظمة والبرامج تعمل بشكل طبيعي وصحي.
- مراقبة العمليات الضارة التي يقوم بها المستخدمون عمداً كان أو خطأً.
- الكشف عن عمليات التطفل والاختراقات.
- المساعدة على استعادة الأحداث ومعرفة متطلبات الأنظمة وإعداداتها.
- تشكل مصدراً قانونياً رسمياً للمنشأة لإثبات الأحداث أو نفيها.
- تشكل مصدراً من مصادر التقارير الرسمية للمنشأة عن أنشطتها والمشاكل التي قد تقع فيها.

ولابُدَّ من مراعاة أمور عدة عند إجراء عمليات التدقيق والمتابعة، وتتمثل في (القحطاني، 2015):

1. حفظ وثائق المتابعة كسجلات الأحداث في مكان آمن.
2. استخدام أدوات المتابعة المناسبة التي تؤدي إلى نتائج أفضل بحجم أقل من المعلومات.
3. يجب المحافظة على معلومات المتابعة وسجلات الأحداث من التغيير غير الشرعي.
4. يجب تدريب العاملين في حقل المتابعة ومراجعة وثائق المتابعة جيداً.
5. حصر صلاحية حذف وثائق المتابعة وسجلات الأعمال في مديري الأنظمة الموثوق بهم فقط.
6. لابُدَّ أن تشمل المتابعة جميع الأحداث بما في ذلك الأحداث الخاصة بذوي الصلاحيات العليا.

وإنَّ أهم الأحداث التي يجب أن تدخل تحت مظلة المتابعة والتدقيق:

1. الأحداث على مستوى الأنظمة.
2. الأحداث على مستوى البرامج التطبيقية.

3. الأحداث على مستوى المستخدمين.

كما أنه لابُدَّ من وجود مجموعة من الإجراءات المضادة للمخاطر والضوابط اللازمة وهي (حمودة، 2014):

1. ضوابط التوجيه، مثل: وضع سياسات، والمطالبة بالعمل بها.
2. ضوابط وقائية: وهي تحمي نقاط الضعف، وتجعل الهجوم فاشلاً أو تحد من آثاره، وتحتاج إلى الرقابة المستمرة لعناصر النظام.
3. ضوابط الكشف: وهي تؤدي لاكتشاف الهجمات.
4. ضوابط تصحيحية: تقلل من تأثير هجوم وتمنعه.
5. ضوابط الإنعاش: ترتبط غالباً باستمرارية الأعمال والتعافي من الكوارث.

7.1.2 معايير أمن المعلومات:

يعرف المعيار بأنه مجموعة محددة مسبقاً من القواعد والشروط أو المتطلبات المتعلقة بتعريف المصطلحات، وتصنيف المكونات، وتحديد المواد، والأداء والإجراءات، وتخطيط العمليات، والقياسات الكمية أو الجودة لتوصيف المواد، والمنتجات، والأنظمة، والخدمات أو الممارسات.

ويرى (السالمي، 2001) أن المعايير جاءت لكي تصنف درجات ومستويات الأمن، والتي من أهمها:

1. أمنية المعلومات ودرجة السرية.
2. صعوبة استرجاع المعلومات.
3. تكاليف استثمار الأجهزة والبرمجيات وجمع البيانات.
4. أهمية الأنظمة والتطبيقات المنفذة ودرجة اعتمادية العمل عليها.
5. أسلوب تناقل المعلومات ضمن منطقة الحاسوب ونوعية الشبكات المستخدمة.

8.1.2 علاقة (ISO27002) بسياسات أمن المعلومات:

يختص هذا المعيار بضوابط أمن المعلومات، ويمثل الموجه لتطبيق ضوابط أمن المعلومات في المؤسسة، وإنَّ سياسات أمن المعلومات تعتبر أحد مكونات هذا المعيار، ويشير المعيار أنه يجب على المؤسسات أن تعرف سياسات أمن المعلومات لديها لتوجه وترشد العاملين تجاه قضايا أمن المعلومات، ومن أهم عوامل نجاح نظام أمن المعلومات ما يلي (عبد الواحد، 2015):

1. وجود سياسات أمن المعلومات متوافقة مع أهداف المؤسسة.

2. دعم والتزام جميع المستويات الإدارية بأمن المعلومات، ولاسيما الإدارة العليا.
3. التوعية الفعالة والبرامج التدريبية حول أمن المعلومات، لإعلام العاملين، وكل الجهات المعنية بأمن المعلومات وسياسات أمن المعلومات وتحفيزهم للتعامل معها.

9.1.2 سياسات أمن المعلومات ومعاييره وتوجيهاته وإجراءاته:

يجب أن يشتمل برنامج أمن المعلومات على الأمور الآتية (القحطاني، 2015):

أولاً: السياسات الأمنية

هناك ثلاثة أنواع لسياسات أمن المعلومات؛ وهي:

1. سياسات أمن معلومات عامة.
2. سياسات أمن معلومات موضوعية.
3. سياسات أمنية للأنظمة.

وتعرف السياسة الأمنية على أنها الطريقة أو الخطوات المكتوبة التي تحددها الإدارة العليا للمنشأة لتحديد كيفية أداء الأعمال ذات العلاقة بأمن المعلومات، وكيف تعالج أي نشاط يخص المعلومة أو الأنظمة، والأشخاص المعالجين لها؛ ويمكن القول: إنَّ السياسات الأمنية هي بمنزلة قانون للمنشأة وذلك لابُدَّ أن تكون واضحة ودقيقة.

وتكمن أهمية السياسة الأمنية في البنود الآتية:

1. تحديد موارد المنشأة الرئيسة التي تُعدُّ ذات قيمة كبيرة للمنشأة.
2. بموجب السياسة الأمنية يخول فريق أمن المعلومات بممارسة مهامه.
3. تشكل مرجعاً رئيسياً وموحداً للرجوع إليه عند تعارض المهام الخاصة بأمن المعلومات مع بعضها ببعض.
4. تحدد أهداف المنشأة المتعلقة بأمن المعلومات.
5. توضح مسؤوليات الموظفين وتحددها.
6. تساعد في منع حدوث المفاجآت في الإجراءات أو أحداث العمل اليومية.
7. تحدد نطاق عمل فريق أمن المعلومات ومهامه.
8. توضح مسؤولية الاستجابة للأحداث التي تقع، والتي تخص أمن المعلومات.
9. توضح استجابة المنشأة ومسؤولياتها تجاه القوانين والمعايير العامة والخاصة.

10.1.2 أنواع السياسات الأمنية:

1. **السياسة الأمنية العامة:** إن للسياسة الأمنية العامة معايير ومميزات يجب فهمها وتطبيقها، وتتمثل في (القحطاني، 2015):
   - إنشاء السياسة الأمنية وتطبيقها وفق أهداف المنشأة العامة.
   - يجب أن تكون سهلة الفهم وواضحة المعاني، ومرجعاً أساسياً لموظفي المنشأة وإداريها كافة.
   - يجب أن تعد بطريقة يتم فيها تضمين أمن المعلومات في جميع إجراءات المنشأة.
   - يجب أن تعد بالاستناد إلى القوانين والتشريعات والقواعد المطبقة على المنشأة.
   - يجب أن تراجع وتحدث دورياً.
   - يجب أن يجري إصدار أو تحديث السياسة على شكل إصدارات أو طبعات مؤرخة.
   - أن تكون قابلة للتطبيق لعدة سنوات.
   - غالباً ما تكون السياسة الأمنية العامة ثابتة، قليلة تكرار التحديث.

هناك عدة خصائص لوثيقة السياسة الأمنية العامة تتمثل في:

   - أن تكون منظمة ومرتبة ومبوبة وفق مهام المنشأة الأساسية.
   - أن تكون مكتوبة بلغة واضحة سهلة الفهم والتطبيق.
   - أن تحدد فيها المسؤوليات والصلاحيات بكل دقة.
   - تحديد الإجراءات التي يجب إتباعها عند ظهور أي مشكلة بشكل تفصيلي.

2. **السياسة الأمنية الموضوعية:** إن للسياسة الأمنية الموضوعية معايير ومميزات يجب فهمها وتطبيقها، وتتمثل في:
   - أنها تركز على تقنية محددة كالبريد الإلكتروني مثلاً.
   - تحتاج إلى التحديث بشكل مستمر وبتكرار أكثر من السياسة العامة.
   - يجب أن تحتوي النصوص اللازمة لتحديد موقف المنشاة من موضوعات محددة.

ومن الأمثلة على السياسات الأمنية الموضوعية: السياسة الأمنية للبريد الإلكتروني، والسياسة الأمنية لاستخدام شبكة الإنترنت.

3. **السياسة الأمنية للأنظمة:** من أهم مهام هذه السياسة أن توضح ما يلي:

- القائمة المعتمدة بالبرامج التطبيقية لدى المنشأة، والمسموح باستخدامها على أجهزة المنشأة.
- كيفية حماية قواعد البيانات واستخدامها.
- شروط استخدام الأجهزة الطرفية كالحاسبات الآلية والطابعات وغيرها.

ومن الأمثلة على السياسة الأمنية للأنظمة: السياسة الأمنية لكلمات المرور.

ثانياً: المعايير القياسية

هي الأنشطة والأعمال واللوائح الإلزامية التي يجب التقيد بها في جميع أنشطة المنشأة، وقد تكون هذه المعايير داخلية المنشأ والتطبيق، وقد تكون خارجية المنشأ داخلية التطبيق، ومن المعايير التي يتم استخدامها داخل المنشأة (Harris & Foreword, 2001):

1. يجب أن يقوم الموظف بإبراز بطاقة التعريف الخاصة به.
2. يجب تشفير وترميز البيانات السرية داخل المنشأة.
3. أن يستخدم الموظف الخصائص الحيوية كبصمة الأصبع.
4. إلزام الموظف بتحديث معلوماته وعنوانه دورياً.

ثالثاً: الخطوط الأساسية

هي الحد الأدنى من الحماية المطلوبة، وتُعدُّ مرجعاً يتم الرجوع إليه لقياس مدى القرب أو البعد منه قبل وقوع الخطر وبعده، ومن ثم معرفة ما يمكن القيام به لتجاوز هذا الخطر، ومن الأمثلة عليها عملية تركيب أنظمة تشغيل جديدة وتفعيلها، أو برامج تطبيقية جديدة أو تحديثات جديدة، قد يترتب عليها النزول دون الحد الأدنى من الحماية(حمودة، 2014).

رابعاً: التوجيهات

هي مجموعة الأعمال المستحسنة، والتوجيهات التشغيلية الموجهة للمستخدمين، والمشغلين، والمختصين في تقنية المعلومات، وتشمل طرق الاستخدام للتقنيات المتاحة في المنشأة، والتي تساعد المستخدمين على التعامل مع تلك التقنيات بشكل جيد (عبد الواحد، 2015).

خامساً: الإجراءات

هي الخطوات التفصيلية المطلوب القيام بها لتحقيق هدف معين، والذي يقوم بها المستخدمون أو المختصون بتقنية المعلومات، أو المشغلون، أو غيرهم، حسب طبيعة الهدف المراد تحقيقه، وهناك أمثلة عدة على الإجراءات تتمثل في (Tipton& Nozaki, 2007):

1. الخطوات التفصيلية لتنصيب نظام التشغيل.
2. الخطوات التفصيلية لتغيير إعدادات أنظمة الحماية وآلياتها.
3. الخطوات التفصيلية لتطبيق قوائم التحكم بالوصول.
4. الخطوات التفصيلية لتعريف مستخدمين جدد إلى الشبكة.
5. الخطوات التفصيلية لمنح الصلاحيات على الأجهزة.

سادساً: التدريب والتوعية بأمن المعلومات

إن الهدف الرئيسي من التدريب والتوعية بأمن المعلومات، هو إيصال مفهوم أمن المعلومات والسياسات الأمنية العامة لكل موظف بالمنشأة، والتأكد من أن كلاً من السياسات الأمنية الموضوعية أو المختصة بأنظمة محددة قد وصلت بالصورة الصحيحة لكل شخص يتطلب عمله فهمها وتطبيقها والتعامل معها.

حيث يشتمل كل من التدريب والتوعية بأمن المعلومات سواء أكان يتم التعامل معها كوحدة واحدة أم منفصلين عن بعضهما ببعض على ثلاثة مستويات:

1. المستوى الأعلى: وهو مستوى عام شامل يحتوي مواد تدريبية وتوعوية قصيرة المدة عامة المفاهيم، ويستهدف المستويات العليا من إدارة المنشأة.
2. المستوى المتوسط: متوسط الشمولية، يحتوي مواد تدريبية توعوية متوسطة المدة، ومتوسطة في التفاصيل، وتستهدف المهندسين والاستشاريين ورؤساء الأقسام.
3. المستوى الأدنى: وهو مستوى تفصيلي يحتوي مواد تدريبية وتوعوية طويلة المدة، تحتوي معلومات تفصيلية عن كيفية تطبيق السياسات الأمنية والمعايير القياسية، والتوجيهات والإجراءات خطوة بخطوة على أرض الواقع، ويستهدف الأفراد والجهات التنفيذية من فنيين ومستخدمين ومستفيدين (القحطاني، 2015).

يجب أن يكون كل من التدريب والتوعية بأمن المعلومات مستمرين طوال العام، وبصفة دورية، وأن يتما على كل مستوى من المستويات الثلاثة لمرة واحدة على الأقل في كل سنة.

11.1.2 معيار (ISO27002) لتكنولوجيا المعلومات – تقنيات أمن المعلومات– قانون الممارسة لإدارة أمن المعلومات:

هو أحد سلسلة معايير أيزو (27000) الصادرة عن المنظمة العالمية للتوحيد القياسي (ISO)؛ والذي يهدف إلى إنشاء نظام إدارة أمن المعلومات، ويستخدم في المؤسسات لتحديد الأهداف والمطالب الأمنية، والتوافق مع التشريعات والقوانين، ووضع إجراءات جديدة لإدارة أمن المعلومات وتحديد المسؤوليات والضوابط وإدارة أصول المنشأة (العربي، 2014).

وقد قام الباحث بالرجوع إلى المعيار الرئيسي، والنسخة الثانية المحدثة (الإصدار الثاني للمعيار)، وقام الباحث بتلخيص وترجمة المعلومات الخاصة بالمعيار كما يلي من المعيار نفسه (ISO/IEC 27002, 2013)، حيثُ أنَّ المعيار في إصداره الأول كان يضم (11) بنداً للتحكم في أمن المعلومات و(39) معياراً أساسياً، وقد حدثت تغييرات عدة على المعيار من إضافات وتعديلات كما يلي:

يحتوي هذا المعيار على (14) بند للتحكم في الأمان تحتوي بشكل جماعي على ما مجموعه (35) معياراً أساسياً و(111) ضابطاً فرعياً أو معايير فرعية، كما هو مبين في الجدول (1.2) (ISO/IEC 27002, 2013):

جدول (1.2): بنود معيار ISO27002

اسم المعيار	المصطلح	عدد
سياسات أمن المعلومات	Information security policies	1
تنظيم أمن المعلومات	Organizing Information Security	2
أمن الموارد البشرية	Human Resources Security	3
إدارة الأصول	Asset Management	3
التحكم في الوصول	Access Control	4
التشفير	Cryptography	1

2	Physical and Environmental Security	الأمن المادي والبيئي
7	Operations security	أمن العمليات
2	Communications security	أمن الاتصالات
3	System acquisition، development and maintenance	اكتساب النظام وتطويره وصيانته
2	Supplier relationships	علاقات الموردين
1	Information Security Incident Management	إدارة حوادث أمن المعلومات
2	Information security aspects of business continuity management	جوانب أمن المعلومات في إدارة استمرارية الأعمال
2	Compliance.	الامتثال
35	**إجمالي عدد المعايير الرئيسة لكل بند من بنود الأمان**	

ويبين الجدول (2.2) تفصيل المعايير الرئيسة المنبثقة من بنود المعيار الأربعة عشر، كما يلي:

جدول (2.2): المعايير الرئيسة للمعيار ISO27002

Information security policies	سياسات أمن المعلومات
Policies for information security	سياسات لأمن المعلومات
Organization of information security	تنظيم أمن المعلومات
Internal organization	التنظيم الداخلي.
Mobile devices and teleworking	أجهزة المحمول والعمل عن بعد
Human resource security	أمن الموارد البشرية
Prior to employment	قبل العمل
During employment	أثناء العمل
Termination and change of employment	إنهاء وتغيير العمل
Asset management	إدارة الأصول
Responsibility for assets	المسؤولية عن الأصول
Information classification	تصنيف المعلومات

Media handling	التعامل مع وسائل الإعلام
Access control	التحكم في الوصول
Business requirements of access control	متطلبات الأعمال من التحكم في الوصول
User access management	إدارة وصول المستخدم
User responsibilities	مسؤوليات المستخدم
System and application access control	التحكم في الوصول إلى النظام والتطبيق
Cryptography	التشفير
Cryptographic controls	ضوابط التشفير
Physical and environmental security	الأمن المادي والبيئي
Secure areas	المناطق الآمنة
Equipment	المعدات
Operations security	أمن العمليات
Operational procedures and responsibilities	الإجراءات والمسؤوليات التشغيلية
Protection from malware	الحماية من البرامج الضارة
Backup	النسخ الاحتياطي
Logging and monitoring	التسجيل والمراقبة
Control of operational software	التحكم في البرامج التشغيلية
Technical vulnerability management	إدارة الضعف التقني
Information systems audit considerations	اعتبارات تدقيق نظم المعلومات
Communications security	أمن الاتصالات
Network security management	إدارة أمن الشبكات
Information transfer	نقل المعلومات
System acquisition، development and maintenance	اكتساب النظام وتطويره وصيانته
Security requirements of information systems	المتطلبات الأمنية لنظم المعلومات

Security in development and support processes	الأمن في عمليات التطوير والدعم
14.3 Test data	بيانات الاختبار
Supplier relationships	علاقات الموردين
Information security in supplier relationships	أمن المعلومات في علاقات الموردين
Supplier service delivery management	إدارة تسليم خدمات الموردين
Information security incident management	إدارة حوادث أمن المعلومات
Management of information security incidents and improvements	إدارة حوادث أمن المعلومات والتحسينات
Information security aspects of business continuity management	جوانب أمن المعلومات في إدارة استمرارية الأعمال
Information security continuity	استمرارية أمن المعلومات
Redundancies	التكرار
Compliance	الامتثال
Compliance with legal and contractual requirements	الامتثال للمتطلبات القانونية والتعاقدية
Information security reviews	مراجعات أمن المعلومات

أولاً: معيار سياسات أمن المعلومات

يتكون هذا البند من معيار رئيسي واحد، وهو سياسات أمن المعلومات، ويهدف إلى توجيه إدارة المؤسسة ودعمها في طريقة تعاملها مع أمن المعلومات والتوافق مع القوانين واللوائح ذات الصلة (ISO/IEC 27002, 2013).

ويشتمل على معيارين فرعيين (العربي، 2013):

1. الوثيقة العامة لسياسة أمن المعلومات.
2. المراجعة لسياسة أمن المعلومات.

ومن أهم توجيهات التطبيق التي وردت تحت هذين المعيارين:

- إجازة وثيقة أمن المعلومات من الإدارة العليا للمؤسسة، وتعميمها على كل المنسوبين والجهات الخارجية ذات العلاقة.

- ضرورة أن تنص وثيقة سياسة أمن المعلومات على موافقة الإدارة العليا، وأن تضع رؤية المنظمة في إدارة أمن المعلومات.
- إذا حدث توزيع لوثيقة أمن المعلومات خارج المنظمة، فيجب الانتباه لعدم احتوائها على معلومات حساسة عن المنظمة.

ثانياً: معيار تنظيم أمن المعلومات

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى إنشاء إطار إدارة لبدء ومراقبة التنفيذ وتشغيل أمن المعلومات داخل المنظمة، كما يجب تحديد جميع مسؤوليات أمن المعلومات وتخصيصها، كما ينبغي تحديد أنشطة إدارة المخاطر وخصوصاً فيما يتعلق بقبول المخاطر المتبقية (ISO/IEC 27002, 2013).

حيث يتم تنظيم وإدارة أمن المعلومات داخل المؤسسة تبعاً لأمور عدة منها: موافقة الإدارة العليا على وثيقة أمن المعلومات، وأيضاً تحديد الأدوار والمسؤوليات وتنسيق ومراجعة تطبيق الأمن في جميع إدارات المنظمة (العربي، 2013).

ثالثاً: معيار أمن الموارد البشرية

يتكون هذا البند من (3) معايير رئيسة، ويهدف إلى ضمان فهم الموظفين والمتعاقدين لمسؤولياتهم ومناسبة للأدوار التي يتم النظر فيها، كما يجب إجراء فحوصات التحقق من الخلفية على جميع المرشحين للعمل وفقاً لهذه المعايير مع القوانين واللوائح والأخلاقيات ذات الصلة، ويجب أن تكون متناسبة مع متطلبات العمل، وكذلك يجب تصنيف المعلومات التي يجب الوصول إليها والمخاطر المتصورة (ISO/IEC 27002, 2013).

رابعاً: معيار إدارة الأصول

يتكون هذا البند من (3) معايير رئيسة، ويهدف إلى تحديد الأصول التنظيمية، وتحديد مسؤوليات الحماية المناسبة، كما يجب تحديد الأصول المرتبطة بمرافق معالجة المعلومات، ومعلومات جرد هذه الأصول ينبغي وضعها وصيانتها، كما يجب أن تتضمن دورة حياة المعلومات الإنشاء، المعالجة، التخزين، النقل، الحذف، ويجب الاحتفاظ بالوثائق في قوائم جرد مخصصة أو حالية حسب الحاجة (ISO/IEC 27002, 2013).

خامساً: معيار التحكم في الوصول

يتكون هذا البند من (4) معايير رئيسة، ويهدف إلى الحد من الوصول إلى المعلومات، ومرافق معالجة المعلومات، وينبغي وضع سياسة للتحكم في الوصول وتوثيقها ومراجعتها استناداً إلى الأعمال التجارية ومتطلبات أمن المعلومات، كما يجب على مالكي الأصول تحديد قواعد التحكم في الوصول المناسبة وحقوق الوصول والقيود المفروضة (ISO/IEC 27002, 2013).

سادساً: معيار التشفير

يتكون هذا البند من معيار رئيسي واحد، ويهدف إلى ضمان الاستخدام السليم والفعال للتشفير لحماية سرية أو صحة أو سلامة المعلومات، ينبغي وضع وتنفيذ سياسة بشأن استخدام ضوابط التشفير لحماية المعلومات (ISO/IEC 27002, 2013).

وعند وضع سياسة تشفير، يجب مراعاة ما يلي:

1. نهج الإدارة نحو استخدام ضوابط التشفير عبر المنظمة، بما في ذلك المبادئ العامة التي ينبغي بموجبها حماية المعلومات التجارية.
2. استناداً إلى تقييم المخاطر، ينبغي تحديد مستوى الحماية المطلوب مع مراعاة ذلك نوع وقوة وجودة خوارزمية التشفير المطلوبة.
3. استخدام التشفير لحماية المعلومات المنقولة بواسطة الوسائط المتنقلة أو الوسائط القابلة لإزالة الأجهزة أو عبر خطوط الاتصالات.
4. نهج الإدارة الرئيسة، بما في ذلك طرق التعامل مع حماية التشفير.
5. الأدوار والمسؤوليات، على سبيل المثال من المسؤول عن:

- تنفيذ السياسة.
- الإدارة الرئيسة.
- المعايير التي يجب اعتمادها للتنفيذ الفعال في جميع أنحاء المنظمة.
- تأثير استخدام المعلومات المشفرة على أدوات التحكم التي تعتمد على فحص المحتوى.

سابعاً: معيار الأمن المادي والبيئي

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى منع الوصول الفعلي غير المصرح به والضرر والدخول إلى المنظمة ومرافق المعلومات ومعالجة المعلومات، يجب تعريف حدود الأمان واستخدامها

لحمايـة المنـاطق التـي تحتـوي إمـا علـى حساسـية أو حرجـة مرافـق المعلومـات ومعالجـة المعلومـات (ISO/IEC 27002, 2013).

ويمكن تحقيق الحماية المادية عن طريق إنشاء حواجز فيزيائية واحدة أو أكثر حول المؤسسة المباني ومرافق معالجة المعلومات، ويوفر استخدام الحواجز المتعددة حماية إضافية، حيث لا يعني فشل حاجز واحد أن الأمان يتعرض للخطر على الفور، وقد تكون المنطقة الآمنة عبارة عن مكتب قابل للإغلاق أو عدة غرف محاطة ببدنية داخلية متواصلة حاجز الأمان، وقد تكون هناك حاجة إلى عوائق إضافية ومحيط للسيطرة على الوصول المادي للمناطق ذات المتطلبات الأمنية المختلفة داخل محيط الأمان.

ثامناً: معيار أمن العمليات

يتكون هذا البند من (7) معايير رئيسة، ويهدف إلى ضمان التشغيل الصحيح والآمن لمرافق معالجة المعلومات، كما يجب توثيق إجراءات التشغيل وإتاحتها لجميع المستخدمين الذين يحتاجون إليها(ISO/IEC 27002, 2013).

يجب إعداد إجراءات موثقة للأنشطة التشغيلية المرتبطة بالمعلومات، مثل: مرافق المعالجة والاتصالات، وإجراءات بدء التشغيل وإغلاق الكمبيوتر، والنسخ الاحتياطي، وصيانة المعدات، والتعامل مع وسائل الإعلام، وغرفة الكمبيوتر وإدارة التعامل مع البريد والسلامة.

كما يجب أن تحدد إجراءات التشغيل التعليمات التشغيلية، بما في ذلك:

1. تركيب وتكوين النظم.
2. معالجة المعلومات ومعالجتها آلياً ويدوياً.
3. نسخة احتياطية.
4. متطلبات الجدولة، بما في ذلك الاعتمادات المتبادلة مع النظم الأخرى ، وأقدم بداية عمل وآخر مواعيد إتمام العمل.
5. تعليمات للتعامل مع الأخطاء أو غيرها من الظروف الاستثنائية ، والتي قد تنشأ أثناء العمل.
6. جهات اتصال الدعم والتصعيد بما في ذلك جهات اتصال الدعم الخارجي.
7. الإرشادات الخاصة وإرشادات معالجة الوسائط.

8. إجراءات إعادة تشغيل النظام واستعادته للاستخدام في حالة تعطل النظام.
9. إدارة معلومات سجل التدقيق وسجل النظام.
10. إجراءات المراقبة.

تاسعاً: معيار أمن الاتصالات

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى ضمان حماية المعلومات في الشبكات ومرافق معالجة المعلومات الداعمة لها، كما يجب إدارة الشبكات والتحكم بها لحماية المعلومات في الأنظمة والتطبيقات(ISO/IEC 27002, 2013).

ينبغي تنفيذ الضوابط لضمان أمن المعلومات في الشبكات، وحماية الخدمات المتصلة من الوصول غير المصرح به، وعلى وجه الخصوص، ينبغي النظر في البنود الآتية:

1. ينبغي إنشاء مسؤوليات وإجراءات لإدارة معدات الشبكات.
2. يجب فصل المسؤولية التشغيلية للشبكات عن عمليات الحاسوب.
3. ينبغي إنشاء ضوابط خاصة للحفاظ على سرية وسلامة بيانات المرور عبر الشبكات العامة أو عبر الشبكات اللاسلكية وحماية الأنظمة المتصلة والتطبيقات.
4. ينبغي تطبيق التسجيل المناسب والرصد لتمكين تسجيل الإجراءات والكشف عنها قد تؤثر على أمن المعلومات أو تكون ذات صلة به.
5. ينبغي تنسيق أنشطة الإدارة عن كثب من أجل تحسين الخدمة ولضمان تطبيق الضوابط باستمرار عبر معالجة المعلومات.
6. ينبغي التصديق على الأنظمة الموجودة على الشبكة.
7. يجب تقييد اتصال الأنظمة بالشبكة.

عاشراً: حيازة النظام وتطويره وصيانته

يتكون هذا البند من (3) معايير رئيسة، ويهدف إلى ضمان أمن المعلومات هو جزءٌ لا يتجزأ من نظم المعلومات عبر دورة حياة كاملة، وهذا يشمل أيضاً متطلبات نظم المعلومات التي تقدم الخدمات على الشبكات العامة (ISO/IEC 27002, 2013).

الحادي عشر: علاقات مع الموردين

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى لضمان حماية أصول المنظمة التي يمكن الوصول إليها من قبل الموردين، وكذلك التخفيف من المخاطر المرتبطة بوصول المورد إلى متطلبات أمن المعلومات (ISO/IEC 27002, 2013).

الثاني عشر: إدارة حوادث أمن المعلومات

يتكون هذا البند من معيار رئيسي واحد، ويهدف إلى ضمان اتباع نهج متسق وفعال حوادث أمن المعلومات، بما في ذلك التواصل حول الأحداث الأمنية ونقاط الضعف، وينبغي وضع مسؤوليات وإجراءات الإدارة لضمان سرعة وفعالية استجابة المنظمة لحوادث أمن المعلومات (ISO/IEC 27002, 2013).

الثالث عشر: جوانب أمن المعلومات في إدارة استمرارية الأعمال

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى أن تكون استمرارية أمن المعلومات مضمنة في أنظمة إدارة استمرارية الأعمال في المؤسسة، ويجب أن تحدد المنظمة متطلباتها لأمن المعلومات واستمرارية إدارة أمن المعلومات في المواقف المعاكسة، على سبيل المثال الأزمات والكوارث (ISO/IEC 27002, 2013).

الرابع عشر: الامتثال

يتكون هذا البند من معيارين رئيسيين، ويهدف إلى تجنب انتهاكات الالتزامات القانونية أو التنظيمية أو التعاقدية المتعلقة بأمن المعلومات وأي متطلبات أمنية، حيث يجب تحديد جميع اللوائح والمتطلبات التعاقدية وتحديثها باستمرار لتضمن بشكل صريح نظام معلومات كامل ومنظم (ISO/IEC 27002, 2013).

2.2 المبحث الثاني: جودة الخدمات

1.2.2 تمهيد:

مع تنامي حدة المنافسة بين جميع المنظمات، والتزايد المستمر في حجمها، وكذلك التغيرات التي مست جميع دول العالم قد فرضت الجودة نفسها بالاتجاه نحو التحسين المستمر والتفوق الدائم، فقد اتجهت جميع المنظمات ولاسيما الخدمية إلى الاهتمام بالجودة وذلك باعتبار أن قطاع الخدمات أصبح يمثل جزءاً كبيراً من الناتج الوطني الإجمالي للدول، وبمقارنة قطاع الخدمات بالقطاعات الأخرى الصناعية المنتجة للسلع المادية؛ فإنَّ الخدمة توفر فرصاً أكبر للعمل، وذلك بعد تطور مستوى معيشة الأفراد، وازدياد المتطلبات العصرية للحياة (دهليز، 2018).

ويحظى موضوع الجودة باهتمام متزايد في كل المنظمات، لاسيما بعدما تنبهت هذه المنظمات إلى أهمية تطوير وتحسين الجودة، وأصبح هذا المفهوم كمدخل أساسي لمواجهة التحديات الداخلية والخارجية التي بدأت في مواجهتها، بعد ظهور التكتلات الاقتصادية، فضلاً عن التطورات التكنولوجية المتلاحقة والاهتمام بقضايا البيئة، والتغير الحاصل في سلوك المستهلك الذي بدأ ينظر للجودة كمعيار أساسي لتقييم واختيار ما يشبع حاجاته ورغباته (زقاي وزاني، 2017).

2.2.2 مفهوم الجودة:

إن كلمة الجودة في اللغة تعني "الجيد نقيض الرديء، وجاد جودة: صار جيداً"، ويرجع أصل كلمة الجودة إلى الكلمة اللاتينية (Qualities) التي يقصد بها طبيعة الشخص أو الشيء ودرجة صلاحيته، وكانت تعني قديماً الدقة والإتقان (الدهيمات، 2011).

وتعني جودة الخدمة الفرق بين توقعات العملاء للخدمة وإدراكهم للأداء الفعلي لها (عودة، 2012).

وجودة الخدمات التي يتوقعها العملاء أو التي يدركونها فعلياً، هي المحدد الرئيس لرضا العملاء، وتُعدُّ في الوقت نفسه من الأولويات الرئيسة للمنظمات التي تريد تعزيز مزاياها التنافسية، أي أنَّ جودة الخدمة هي درجة تطابق الأداء الفعلي للخدمة مع توقعات العملاء (Kumar, 2006).

وتمثل الخدمة عملاً أو نشاطاً يمكن تقديمه من طرف لطرف آخر، وهي في الأساس غير ملموسة ولا ينتج عنها أيه ملكية، وأن إنتاجها أو تقديمها يكون مرتبطاً بمنتج مادي ملموس (Kotler & Armstrong, 2013).

وتعرف جودة الخدمات على أنها مجموعة الصفات والخصائص التي يتميز بها المنتج أو الخدمة، والتي تؤدي إلى تلبية حاجات المستهلكين والعملاء سواء من حيث تصميم المنتج أو تصنيعه أو قدرته على الأداء في سبيل الوصول إلى إرضاء هؤلاء العملاء وإسعادهم (الدهيمات، 2011).

ولكي تستطيع الجامعات أن تنافس بكفاءة في أسواقها، لابُدَّ من أن تتميز في تقديم خدماتها الطلابية لضمان رضا طلابها الحاليين، وضمان استقطاب أكبر عدد من الطلبة، وتقوم الجامعات باستخدام العديد من الاستراتيجيات من أجل تحسين مستوى أدائها، ومن أهم هذه الاستراتيجيات الاهتمام بالجودة بوصفها استراتيجية مهمة تساعد الجامعات وغيرها على توفير خدمات تشبع الرغبات الكاملة للطلاب، وتلبي متطلباتهم واحتياجاتهم وتوقعاتهم المعلنة وغير المعلنة سواء داخل الجامعة أو خارجها (السعافين، 2015).

وبناءً على ما سبق يعرف الباحث جودة الخدمات بأنها عبارة عن تكامل ما بين الملامح وخصائص المنتج أو الخدمة والتي تلعب دوراً مهماً في كسب رضا العميل وتحقيق رغباته.

أما الجودة في المجال العلمي فيعرفها الباحث على انها عبارة عن مجموعة من المعايير والاجراءات التي تهدف الى تحسين مستمر في المنتوج التعليمي، وتشير الى المواصفات والخصائص المتوقعة في هذا المنتوج وفي العمليات والأنشطة التي تتحقق من خلالها تلك المواصفات مع توفر أدوات وأساليب متكاملة تساعد المؤسسات التعليمية على تحقيق نتائج مرضية.

حيث أن أساس الجودة العلمية احترام خصوصية الطلاب، ومن هنا تأتي أهمية الدراسة في أمن المعلومات لدى الطلاب والخصوصية وهي حق أصيل لدى كل طالب.

3.2.2 أبعاد جودة الخدمات التعليمية:

قامت مجموعة كبيرة من الدراسات بتحديد مجموعة من الأبعاد التي تمثل جودة الخدمات، ومن أشهر أساليب قياس جودة الخدمات نموذج (SERVQUAL) الذي يستند على توقعات العملاء لمستوى الخدمة، وإدراكهم لمستوى الخدمة المقدمة بالفعل، وقد تم تحديد عشرة أبعاد لقياس جودة الخدمة؛ وهي: الاعتمادية، والأمان، وسهولة الوصول، وفهم المستهلك، والاتصال، والأشياء الملموسة، والجدارة، وسرعة الأداء، والتأهيل واللباقة، غير أن دراسة (Parasuraman, et. Al, 2002)، قامت بدمج هذه الأبعاد في خمسة أبعاد؛ هي:

4.2.2 العناصر المادية الملموسة (Tangibles):

وتتضمن هذه العناصر أربعة متغيرات، تقيس توافر حداثة الشكل في تجهيزات المنظمة، والرؤية الجذابة للتسهيلات المادية، والمظهر الأنيق لموظفيها، وتأثير المظهر العام للمنظمة.

- **الاعتمادية (Reliability):** وتتضمن خمسة متغيرات تقيس وفاء المنظمة بالتزاماتها التي وعدت بها عملاءها، واهتمامها بحل مشاكلهم، وحرصهم على تحري الدقة في أداء الخدمة، والتزامها بتقديم خدماتها في الوقت الذي وعدت فيه بتقديم الخدمة لعملائها، واحتفاظها بسجلات دقيقة خالية من الأخطاء.
- **سرعة الاستجابة (Responsiveness):** ويتضمن هذا البعد أربعة متغيرات تقيس اهتمام المنظمة بإعلام عملائها بوقت تأدية الخدمة، وحرص موظفيها على تقديم خدمات فورية لهم، والرغبة الدائمة لموظفيها في معاونتهم، وعدم انشغال الموظفين عن الاستجابة الفورية لطلباتهم.
- **الثقة والأمان (Assurance):** ويحتوي هذا البعد على أربعة متغيرات تقيس حرص الموظفين على زرع الثقة في نفوس العملاء، وشعور العملاء بالأمان في تعاملهم مع الموظفين، وتعامل الموظفين بلباقة معهم، وإلمامهم بالمعرفة الكافية للإجابة عن أسئلتهم.
- **التعاطف (Empathy):** ويشتمل هذا البعد على أربعة متغيرات تتعلق باهتمام موظفي المنظمة بالعملاء اهتماماً شخصياً، وتفهمهم لحاجاتهم، وملائمة ساعات عمل المنظمة لتناسب جميع العملاء، وحرص المنظمة على مصلحتهم العليا، والدراية الكافية باحتياجاتهم.

5.2.2 أهمية جودة الخدمة:

بسبب زيادة حدة المنافسة بين الشركات وزيادة التوجه نحو العولمة أصبحت الشركات تتجه نحو التميز في جودة منتجاتها لتحسين الربحية وزيادة الحصة السوقية؛ فالجودة تؤثر في حجم الطلبات على الخدمات وهي وسيلة لبناء مكانة تنافسية للمنظمة؛ لذلك؛ فإنَّ الجودة لم تعد ترفاً اختيارياً بل أصبحت التزاماً لا بديل عنه لاستمرار المنظمة ونجاحها فالاهتمام بالجودة يحقق للمنظمات مزايا عدة؛ منها (السر، 2014):

- تحسين سمعة المنظمة.
- تحسين الإنتاجية.
- تقليل الإهدار في الموارد.

- تقليل التكلفة.
- زيادة الحصة السوقية.
- تحسين الربحية.

6.2.2 خطوات تحسين الجودة:

ذكر جودة (2014) مجموعة من الخطوات لتحقيق الجودة في تقديم الخدمات؛ وهي:

1- جذب الانتباه وإثارة الاهتمام بالمستفيدين: إنَّ جذب انتباه المستفيدين، يتم من خلال المواقف الإيجابية التي يبديها مقدم الخدمة، مثل: الاستعداد النفسي والذهني لملاقاة المستفيد.

2- خلق الرغبة لدى المستفيد وتحديد حاجاتهم: إنَّ خلق الرغبة، وتحديد احتياجات المستفيد تعتمد على المهارات البيعية والتسويقية لمقدم الخدمة.

3- إقناع المستفيد ومعالجة الاعتراضات لديه: يتطلب من مقدم الخدمة العديد من الجهود السلوكية القادرة على خلق القناعة لدى المستفيد عند تقديم الخدمات وكذلك معالجة الاعتراضات التي يبديها المستفيد عند الشراء.

4- التأكد من استمرار المستفيدين بالتعامل مع المنظمة: تأتي من خلال بعض الخدمات البيعية والتسويقية التي تشكل ضماناً لولاء المستفيدين للمنظمة؛ ومنها: الاهتمام بشكاوى المستفيدين وملاحظاتهم، فتقديم هذه الخدمة بكفاءة يسهم استمرار المستفيدين مع المنظمة.

3.2 المبحث الثالث: نبذة عن الجامعات الفلسطينية في قطاع غزة

1.3.2 تمهيد:

لم تنشأ الجامعات الفلسطينية كاستجابة للتطور الحضاري فحسب، وإنما ضرورة لمواجهة الاحتلال الصهيوني أيضاً، وظلت الجامعات الفلسطينية تسعى إلى ترسيخ وجودها وكينونتها كي تتمكن من تحمل مسؤوليتها في ترسيخ الهوية الوطنية الفلسطينية التي شكلت التحدي الأهم في رسالتها إلى جانب اهتمامها بمرتكزات التعليم العالي والبحث العلمي وخدمة المجتمع. ولذلك كانت المهمة صعبة منذ البداية، وانعقدت المسؤولية بحجم المهمة. وإن أي تصدع في الأداء لمؤسسات التعليم العالي الفلسطيني، يعني انهيار صرح حضاري يشكل قلعة الصمود الوطني في وجه الاحتلال وسياسات طمس الهوية.

وتتميز جامعاتنا الفلسطينية عن غيرها من الجامعات المجاورة في وجود مفهوم الجامعة العامة، والتي ليست حكومية وليست خاصة، حيثُ إنَّها لا تهدف إلى الربح وتتمتع بالوقت نفسه باستقلالية في الإدارة والتعيين والتوظيف وتتحمل مسؤولية الرواتب والمصاريف التشغيلية الأخرى، وهذه الميزة انفردت فيها معظم الجامعات الفلسطينية بحكم نشأتها في ظل احتلال إسرائيلي، وغياب السلطة الوطنية الفلسطينية (وزارة التربية والتعليم العالي، 2018).

جدول (3.2): الجامعات ونوعها في الضفة وقطاع غزة

نوع الجامعة	الضفة الغربية	قطاع غزة	المجموع
حكومية	2	1	3
عامة	6	2	8
خاصة	1	2	3
تعليم مفتوح	1		1
المجموع	**10**	**5**	**15**

المصدر: (الكتاب الإحصائي السنوي لوزارة التربية والتعليم العالي، 2017/2016)

2.3.2 نبذة عن الجامعات العاملة في قطاع غزة

1- جامعة الأقصى:

جامعة الأقصى – بغزة مؤسسة أكاديمية فلسطينية مستقلة طبقاً لقانون الخدمة المدنية، وقانون التعليم العالي الفلسطيني رقم (11) للعام 1998م، لقد كانت بداية نشأتها في عام 1955م معهداً للمعلمين، ثم نمت وتطورت لتصبح كلية جامعية في العام 1991م وهي كلية التربية الحكومية، ثم تحولت الكلية إلي جامعة الأقصى في العام 2001م، تهدف الجامعة إلي إعداد الإنسان المزود بالمعرفة والمهارات والقيم النبيلة، ولديه القدرة علي التعلم المستمر، وتوظيف تكنولوجيا المعلومات من خلال برامج بناء القدرات والتعليم الجامعي والبحث العلمي وتنمية خدمة المجتمع. وأصبحت عضواً فاعلاً في اتحاد الجامعات العربية، واتحاد جامعات العالم الإسلامي، وعضواً في اتحاد جامعات الأورومتوسطة واتحاد جامعات الفرانكفونية وعضوا في مجلس التعليم العالي الفلسطيني، ساهمت الجامعة وعلى مر مراحل تطورها واتساعها في تهيئة الطلبة ليكونوا مواطنين فاعلين في مجتمعهم، قادرين على تحمل مسؤولياتهم تجاه دينهم ووطنهم ، إضافةً إلى تقوية صلتهم بمجتمعهم وتنمية روح التعاون فيما بينهم. وقد نهجت الجامعة نهجاً إسلامياً حيث غرست في طلابها الصبغة الإسلامية التي تعطي تصورها عن الإسلام الحنيف بصورته الوسطية المعتدلة الذي يحترم كافة الثقافات والحضارات، وتبين علاقة الفرد المسلم بربه، وعلاقته بمجتمعه ومن حوله، بل تؤهل طلابها وطالباتها على المزج بين روح الإسلام ومتطلبات الحياة بما لا يخدش قواعد الدين ، مبطلة بذلك كله مزاعم من قال إنَّه لا يمكن في عصرنا ممارسة الدين والدنيا، بل لابُد من الفصل بينهما، بدعوى أن المجتمع يتغير من وقت لآخر حسب ظروفه الاجتماعية والسياسية والاقتصادية، لقد لعبت الجامعة – منذ تأسيسها – دوراً محورياً في تأهيل وتنمية القدر الأكبر من موارد ومصادر المجتمع المحلية ولاسيما البشرية منها، وذلك عبر ما تقدمه الجامعة من برامج في مجال الدراسات الإسلامية، واللغة العربية، وفي برامج بحثية وتدريبية متخصصة في حقول العلوم الطبية وتكنولوجيا المعلومات والعلوم والآداب ، والإدارة والاقتصاد، وفي مجالات التربية والفنون وإعداد المعلمين ، وفي حقول الإعلام والرياضة. كل ذلك لخدمة المجتمع الفلسطيني والمساهمة في تطوره الاقتصادي والاجتماعي (http://www.alaqsa.edu.ps).

2- جامعة الأزهر:

جامعة الأزهر بغزة مؤسسة للتعليم العالي أُنشئت لتلبي طموحات الشعب الفلسطيني، ولتكون عنواناً لقدرة هذا الشعب على البذل والعطاء، وقد كان قرار سيادة الرئيس الشهيد ياسر عرفات رئيس دولة فلسطين بإنشاء هذه الجامعة هادفاً إلى غرس الشباب الفلسطيني في بلده ومد جذوره فيه، وقد نمت هذه الجامعة نمواً سريعاً يستحق كل الإعجاب والتقدير، تأسست الجامعة سنة 1991م، تتمثل رؤية الجامعة في أنها تسعى إلى التميز، والإبداع ، والرقمية؛ لتكون ضمن الجامعات المرموقة فلسطينياً وعربياً ودولياً، ولتكون مركزاً للإشعاع العلمي، والبحثي، والتنموي للمجتمع الفلسطيني المبني على الجودة الشاملة والتحسين المستمر، ورسالة الجامعة تكمن في أنها مؤسسة تعليم مستقلة غير ربحية، تهدف إلى تلبية احتياجات المجتمع الفلسطيني والعربي من الموارد البشرية المؤهلة في التخصصات المعرفية المختلفة، والبحوث العلمية التطبيقية، والتنمية المستدامة مع التركيز على توظيف تكنولوجيا المعلومات والاتصالات، والمحافظة على أصالة التراث العربي الإسلامي، والالتزام بمبادئ حقوق الإنسان التي تشمل العدالة والمساواة، والالتزام بحكم القانون والشفافية والتسامح والاحترام، وعدم التميز والتنوع والشراكة لأصحاب المصلحة (http://www.alazhar.edu.ps).

3- الجامعة الإسلامية:

الجامعة الإسلامية بغزة مؤسسة أكاديمية مستقلة من مؤسسات التعليم العالي، تعمل بإشراف وزارة التربية والتعليم العالي، وهي عضو في: اتحاد الجامعات العربية، ورابطة الجامعات الإسلامية، واتحاد الجامعات الإسلامية ، ورابطة جامعات البحر الأبيض المتوسط، والاتحاد الدولي للجامعات، وتربطها علاقات تعاون مع الكثير من الجامعات العربية والأجنبية، تأسست عام 1978م، تتمثل رؤيتها في أنها منارة علمية رائدة للمعرفة والثقافة وخدمة الإنسانية لإحداث نهضة مجتمعية شاملة، **وتكمن رسالتها في أنها** مؤسسة أكاديمية تسعى للنهوض بالمستوى العلمي والثقافي والحضاري، تعمل على مواكبة الاتجاهات الحديثة في التعليم العالي والتطور التكنولوجي، وتشجع البحث العلمي وتساهم في بناء الأجيال وتنمية المجتمع في إطار من القيم الإسلامية (http://www.iugaza.edu.ps).

4- جامعة فلسطين:

جامعة فلسطين مؤسسة أكاديمية من مؤسسات التعليم العالي الفلسطينية تأسست من أجل خدمة أبناء الشعب الفلسطيني في الداخل والخارج بشكل خاص والطلبة العرب والأجانب بشكل عام، أسست

جامعة فلسطين بمباركة من فخامة الرئيس الراحل ياسر عرفات – أبو عمار، وبدأت ممارسة دورها في المجتمع الفلسطيني جنباً إلى جنب مع نظيراتها من الجامعات المحلية في أوائل شهر مارس من عام 2005 في مدينة غزة، وذلك بتجهيز ملفات اعتماد الكليات والبرامج، تأسست عام 2003، تتمثل رؤيتها في أنها جامعة متميزة، تستند إلى البحث والمعرفة وتوظيف التقنيات الحديثة لإعداد الكوادر، في شتى المجالات ضمن معايير الجودة الشاملة لرسم شخصية فلسطينية مميزة واثقة منفتحة على حضارات العالم وعلومه، وتقوم رسالتها على أنها مؤسسة تعليم عالٍ فلسطينية، تهدف إلى إعداد كوادر مؤهلة علمياً ومهنياً قادرة على تلبية حاجات المجتمع، من خلال تهيئة البيئة الجامعية وفق متطلبات الجودة مع مواكبة المستجدات العلمية والتقنية وتعزيز دور البحث العلمي والتطور المعرفي، وذلك للمساهمة في دعم جهود التنمية المستدامة ومواكبة ركب الحضارة والمساهمة في صياغة خارطة المستقبل في إطار مبادئ وقيم حضارتنا العريقة (http://up.edu.ps).

4.2 المبحث الرابع: الدراسات السابقة:

سيتم استعراض مصادر الدراسات السابقة وتحليلها وذلك على النحو الآتي:

1.4.2 الدراسات العربية

1. دراسة (المصري والأغا، 2018)، بعنوان: "واقع العدالة التنظيمية كمصدر للتنافسية من خلال ممارسة الجامعات الفلسطينية لمعيار أمن المعلومات (ISO/IEC 27002) في ضوء التماثل التنظيمي: مقترح تطبيقي تنموي استراتيجي".

هدفت هذه الدراسة إلى تقديم إطار مقترح لتحقيق التنافسية للجامعات الفلسطينية، من خلال ممارسة الجامعات لمعيار أمن المعلومات (ISO/IEC..27002)، للتأثير على العدالة التنظيمية والتماثل التنظيمي، موظفاً المنهج الوصفي التحليلي، ولتحقيق أهداف البحث قام الباحثان باستخدام الاستبانة كأداة لجمع المعلومات، وتم تطبيقها على عينة مكونة من (214) موظفاً من موظفي الإدارة العليا والوسطى في الجامعات الفلسطينية في قطاع غزة.

وقد توصل البحث إلى نتائج عدة من أهمها: أن المتوسط الحسابي النسبي لجميع فقرات ممارسة معيار أمن المعلومات (ISO/IEC..27002) يساوي (84.37%)، والمتوسط الحسابي النسبي لجميع فقرات توافر التنافسية يساوي (85.74%)، والمتوسط الحسابي النسبي لجميع فقرات توافر العدالة التنظيمية يساوي (76.98%)، والمتوسط الحسابي النسبي لجميع فقرات تحقيق التماثل التنظيمي يساوي (88.41%)، كما أظهرت النتائج وجود علاقة طردية بين ممارسة معيار أمن المعلومات (ISO/IEC..27002) وتحقيق التنافسية وتحقيق العدالة التنظيمية، وبين توافر العدالة التنظيمية وتحقيق التماثل التنظيمي، وبين العدالة التنظيمية والتنافسية، وعدم وجود علاقة بين ممارسة معيار أمن المعلومات (ISO/IEC 27002) وتحقيق التماثل التنظيمي وبين التماثل التنظيمي والتنافسية.

وفي ضوء هذه النتائج أوصت الدراسة بضرورة أن تقوم الجامعات بوضع خطة استراتيجية متكاملة مرنة لممارسة معيار أمن المعلومات (ISO/IEC..27002) داخل الجامعات، يكون أحد أهم ركائزها تعزيز وتحقيق التنافسية.

2. دراسة (العميري وآخرون، 2017)، بعنوان: "واقع ممارسات أمن المعلومات في المكتبة الرئيسة بجامعة السلطان قابوس، ومدى توافقها مع المعيار الدولي لأمن المعلومات: دراسة حالة (ISO/IEC 27002)".

هدفت الدراسة إلى الكشف عن واقع ممارسات أمن المعلومات في المكتبة الرئيسة بجامعة السلطان قابوس، وتحديد مدى توافقها مع المعيار الدولي لأمن المعلومات الممارسات (ISO/IEC 27002)، والوقوف على جوانب الضعف في الأمنية واتخاذ التوصيات لتحسينها.

ركزت الدراسة على ثلاثة أبعاد، وهي: أمن الموارد البشرية، والأمن المادي والبيئي، وأمن التقنيات. واعتمدت الدراسة على منهج دراسة الحالة، باستخدام أساليب عدة تتمثل في: الزيارات الميدانية، والمقابلات الشخصية، وتتبع الوثائق والمواقع الإلكترونية، واستخدمت استمارة المراجعة أداة لجمع البيانات. تألف مجتمع الدراسة من كافة العاملين في الأقسام المسؤولة عن ممارسات أمن المعلومات بجامعة السلطان قابوس البالغ عددها (12) قسماً، وتم اختيار عينة قصدية من رؤساء الأقسام و/أو من ينوب عنهم في كل قسم.

كشفت نتائج الدراسة عن توافق أغلب ممارسات أمن المعلومات في المكتبة الرئيسة مع ممارسات المعيار الدولي لأمن المعلومات(ISO/IEC..27002)، فقد جاءت أعلى نسبة توافق لمعايير أمن الموارد البشرية بواقع (100%)، يليها معايير الأمن المادي والبيئي بدرجة توافق عالية بلغت (94.8%)، وأخيراً حققت معايير أمن التقنيات درجة توافق عالية كذلك بنسبة (90.5%).

خرجت الدراسة بمجموعة من التوصيات، أهمها: ضرورة الاستمرار في تدريب وتوعية المستفيدين في المكتبات حول الاستخدام الأمثل لمصادر وخدمات المعلومات، والعمل على تطوير سياسة أمنية بالمكتبات تستند على المعيار الدولي لأمن المعلومات، كما أوصت الدراسة بضرورة تخزين النسخ الاحتياطية للأنظمة والبرمجيات خارج مبنى المكتبة، وتوفير مصدر بديل للطاقة خاص بتشغيل المعدات الحاسوبية؛ لضمان استمرار العمل في حال انقطاع التيار الكهربائي بالمكتبة.

3. دراسة (زقاي، 2017) بعنوان: "مستوى جودة الخدمات التعليمية وأثرها في رضا الطلبة : دراسة تطبيقية على طلبة جامعة سعيدة – الجزائر".

هدفت الدراسة إلى تحديد أثر جودة الخدمات التعليمية التي تقدمها جامعة سعيدة في الجزائر، على رضا الطلبة، وذلك باستخدام مقياس الأداء (SERVPERF)، الذي يركز على قياس الأداء الفعلي للخدمة المقدمة، وقد تكونت عينة الدراسة من (370) طالب، ولمعالجة ذلك استخدمت استمارة اشتملت على (29) فقرة تم توزيعها على عينة الدراسة، وتم تفريغ البيانات وتحليل النتائج باستخدام البرنامج الإحصائي (SPSS).

وقد أظهرت النتائج أن درجة تقدير الطلبة لأبعاد جودة الخدمات التعليمية المقدمة في الجامعة جاء بدرجة متوسطة، حيث حصل على درجة كلية بلغت (57.4%)، وأظهرت النتائج كذلك أن مستوى رضا الطلبة على جودة الخدمات التعليمية في الجامعة جاء بدرجة متوسطة، حيث حصل على درجة كلية (54%)، وبينت النتائج كذلك على وجود أثر ذي دلالة إحصائية لجودة الخدمات التعليمية على رضا طلبة الجامعة محل الدراسة.

وفي ضوء هذه النتائج أوصت الدراسة بضرورة الاهتمام بالأساليب الحديثة في التعامل مع الطلبة، والاستماع إلى صوتهم، والتركيز عليهم لأنهم محور كل العمليات التعليمية.

4. دراسة (العربي، 2015)، بعنوان: "معيار المنظمة الدولية للتوحيد القياسي أيزو 27002: (ISO/IEC..27002) لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية".

هدفت الدراسة التعرف إلى تحليل معايير أيزو 27002 لإدارة أنظمة أمن المعلومات والصادرة عن المنظمة الدولية للتوحيد القياسي (آيزو)، والتعرف على السياسات والتوجيهات التي تتضمنها المعايير ومدى التزام أفضل الجامعات العربية بها.

واستخدم الباحث المنهج الوصفي التحليلي للتعرف على مكونات معايير آيزو 27002، ومدى تطبيقها في مواقع أفضل الجامعات العربية حسب تصنيف ويبومتركس لتقييم الجامعات والمعاهد (CSIC-Webometrics) عام 2012، بالإضافة إلى منهج تحليل المضمون لتحليل عناصر معايير 27002 الفرعية. وتم الاعتماد على قائمة مراجعة تضم عناصر معايير تقييم أمن المعلومات لتطبيقها على مواقع أفضل الجامعات العربية.

وتوصل الباحث إلى أن جميع جامعات الدراسة حرصت على تطبيق معايير فرعية في (11) معياراً أساسياً بنسبة (28.2)% من إجمالي معايير آيزو 27002، وكان معيار السياسات الأمنية هو أقل المعايير تطبيقاً بنسبة (19.05)% من الجامعات العربية موضوع الدراسة، وجاءت جامعة الملك عبد العزيز في المرتبة الأولى بتطبيق (95) معياراً بنسبة (71.43%) من إجمالي المعايير، تليها جامعة الملك فهد للبترول والمعادن بنسبة (58.65%)، ثم جامعة أم القرى بنسبة (52.63)%، ثم الجامعة الأردنية بنسبة (51.88%)، ووصلت نسبة الجامعات التي لم تحقق (50%) من المعايير الفرعية (80.95%) من إجمالي الجامعات العربية موضوع الدراسة.

وفي ضوء هذه النتائج أوصت الدراسة بضرورة تطوير سياسات لأمن المعلومات بالجامعات العربية، لتكون مرجعيتها معايير الآيزو 27001، و27002 واعتمادها من إدارة الجامعة ومراجعتها على فترات متقاربة.

5. دراسة (السعافين، 2015)، بعنوان: "استراتيجية مقترحة لتحسين مستوى جودة الخدمات الطلابية في الجامعات الفلسطينية".

هدفت الدراسة التوصل إلى استراتيجية مقترحة لتحسين جودة الخدمات الطلابية في الجامعات الفلسطينية في محافظات غزة، وذلك من خلال التعرف إلى مستوى جودة الخدمات الطلابية في الجامعات الفلسطينية بمحافظات غزة من وجهة نظر الطلبة، ودراسة الفروق في متوسطات تقدي ارتهم لمستوى جودة الخدمات الطلابية في الجامعات الفلسطينية تبعاً للمتغيرات (الجنس، والجامعة، والتخصص). ولتحقيق أهداف الدراسة استخدمت الباحثة المنهج الوصفي التحليلي لملاءمته لموضوع الدراسة، وقامت الباحثة بتصميم الاستبانة كأداة للدراسة، وقد تكونت من (59) فقرة، وزعت على (5) أبعاد تتماشى مع مقياس جودة الخدمة الأداء الفعلي (Performance..Service). وقد تم عرض الاستبانة على (12) محكماً، وتم التحقق من صدق الاستبانة، وثباتها من خلال تطبيقها على عينة استطلاعية مكونة من (40) طالباً وطالبة، وذلك قبل تطبيقها على عينة الدراسة المكونة من (568) طالباً وطالبة من طلبة المستوى الرابع بالجامعات الثلاث (الإسلامية، والأزهر، والأقصى) في العام الدراسي 2015-2014 وقامت الباحثة باستخدام برنامج الرزم الإحصائية للدراسات

الاجتماعية (SPSS)، ولوضع الاستراتيجية المقترحة لتحسين مستوى جودة الخدمات الطلابية في الجامعات الفلسطينية قامت الباحثة باستخدام المنهج البنائي من خلال المجموعة البؤرية التي تكونت من عدد من الخبراء.

ومن خلال استجابات أفراد عينة الدراسة، توصلت الدراسة إلى عدة نتائج أهمها: أن مستوى جودة الخدمات الطلابية في الجامعات الفلسطينية متوسطاً، حيث كان الوزن النسبي للأبعاد الخمسة هو (53.84%). كما أظهرت النتائج أن بعد الموثوقية حصل على المرتبة الأولى بوزن نسبي (58.87%). وأظهرت النتائج أيضاً أن بعد الاستجابة حصل على المرتبة الثانية بوزن نسبي متوسطاً قدره (57.51%)، كما أظهرت النتائج أن بعد التعاطف الاجتماعي حصل على المرتبة الثالثة بوزن نسبي متوسطاً قدره (52.97%)، وأظهرت النتائج أن بعد العناصر المادية الملموسة حصل على المرتبة الرابعة بوزن نسبي منخفضاً قدره (51.38%).

وفي ضوء نتائج الدراسة أوصت الباحثة أن تتبنى إدارة الجامعات الفلسطينية جودة الخدمة الطالبية كاستراتيجية للمنافسة والتميز، وأن يكون تطوير وتحسين جودة الخدمات التي تقدمها من أولوياتها وبخاصة في ما يتعلق بالأبعاد (التعاطف الاجتماعي، والعناصر المادية الملموسة والاعتمادية).

6. **دراسة (الدنف، 2013)، بعنوان: "واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها".**

هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، واستخدم 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:

- تتوفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة.
- 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 تعهيد نظم معلوماتها.

- توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة.

وفي ضوء هذه النتائج فقد أوصى الباحث بالآتي:

- ضرورة الاستمرار بالاهتمام بالبنى التحتية لنظم المعلومات، وتطويرها لتجاري المستحدثات التكنولوجية السريعة.
- ضرورة أن تقوم الكليات التقنية ببناء سياسات أمن نظم المعلومات الخاصة بها، والعمل على نشرها وتطبيقها، والقيام بتطويرها ومراجعتها وتقييم المخاطر بشكل دوري للوقوف على ما يمكن عمله وايجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات.
- ينصح بأن تقوم الكليات التقنية بالاعتناء بدور أكبر بالتدريب، وزيادة الموازنات المالية المخصصة لعمليات أمن المعلومات.

7. دراسة (عبد الجابر، 2013)، بعنوان: "مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية".

هدفت الدراسة إلى السعي لاكتشاف مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية المستخدِمة لنظم المعلومات المحاسبية الإلكترونية، وتخفيض مخاطر أمن المعلومات لديها والمعوقات التي تؤثر على فاعلية هذه الاجراءات من خلال تحديد ثلاثة مخاطر تهدد أمن نظم المعلومات وهي مخاطر اختراق الشبكات ومخاطر الهندسة الاجتماعية وأخيراً مخاطر البرمجيات الضارة، كما غطت فاعلية الرقابة الداخلية في منع واكتشاف المخاطر وتصحيحها في حالة وقوعها. ولتحقيق هذا الغرض تم تصميم استبانة وقد تم توزيعها على عينة الدراسة المكونة من ثلاثين شركة صناعية عاملة في المملكة الأردنية الهاشمية تستخدم نظم المعلومات المحاسبية. ولتحليل البيانات قام الباحث باستخدام أساليب إحصائية تمثلت في المتوسطات الحسابية والإنحرافات المعيارية واختبار كروسكال والس واختبار مان وتن واختبار (One Sample t-test).

أظهرت نتائج التحليل الاحصائي فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع والاكتشاف

والتصحيح) من خلال اختبار ثلاثة أنواع من المخاطر التي تهدد أمن المعلومات الالكترونية وهي مخاطر اختراق الشبكات والهندسة الاجتماعية والبرمجيات الضارة، كما أظهرت النتائج فروق ذات دلالة إحصائية بين إجابات أفراد العينة تعود للخلفية الشخصية لكل منهم خاصة في مجالات طبيعة الدور الوظيفي وسنوات الخبرة وحيازة شهادات مهنية وحجم الشركة وكونها أجنبية أو محلية. أظهرت النتائج أيضاً وجود معوقات وتحديات تواجه تطبيق اجراءات رقابة داخلية فعالة؛ ومنها: عدم مواكبة التطور المتسارع لأساليب الاحتيال الإلكتروني، وأيضا عدم دعم الإدارة لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.

وفي ضوء هذه النتائج قدمت الدراسة مجموعة من التوصيات، منها: ضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة، وكذلك تحفيز العاملين في الشركات الصناعية للحصول على الشهادات المهنية ذات العلاقة.

8. دراسة (عمار والكبيسي، 2012)، بعنوان: "التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية : دراسة مسحية تحليلية".

هدفت هذه الدراسة إلى إيجاد حلول لتجنب الثغرات الأمنية الخطرة في شبكات الحاسوب المحلية وتحديد التدابير اللازمة لتجنب حصول الثغرات وإزالة الموجود منها، للوصول إلى أفضل حماية ممكنة بظروف وصول مرنة، وذلك بتطبيق الاستبانة كأداة لجمع البيانات على عينة الدراسة المتكونة من خبراء في تقنية المعلومات من أساتذة جامعات ومهندسين وفنيين ومدراء يعملون في إدارات تقنية المعلومات في المؤسسات التعليمية في الرياض،، حيث بلغ عدد الاستبانات القابلة للتحليل 105 استبانات.

وقد أظهرت نتائج التحليل الإحصائي عن وجود فروق ذات دلالة إحصائية بين درجة خطورة الثغرات الأمنية وبين التدابير الوقائية المتخذة لتجنبها، وذلك لصالح درجة خطورة الثغرات الأمنية، الأمر الذي يدل على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية.

وأوصت الدراسة بضرورة زيادة الاهتمام بالكادر البشري العامل في حماية الشبكات المحلية، من حيث الكفاءة وكفاية العدد والتدريب والتحفيز. لتمكينها من القيام بتدابير الحماية الفيزيائية وإعداد وتشغيل وتحديث أجهزة وبرامج الحماية، وكذلك تنفيذ الاختبارات دورية

لكشف الثغرات الأمنية، بالإضافة لضرورة توفير السياسات الأمنية اللازمة لتنفيذ أعمال الحماية.

9. **دراسة (سلمان، 2012)، بعنوان: "مستوى جودة الخدمات الجامعية كما يدركها طلبة جامعة الأقصى بغزة طبقاً لمقياس جودة الخدمة (SERVPERF)".**

هدفت الدراسة الحالية إلى قياس جودة الخدمات الجامعية كما يدركها طلبة جامعة الأقصى بغزة من خلال استخدام مقياس جودة الخدمة(Performance Service) أو الأداء الفعلي والذي يشار إليه اختصاراً (ServPerf)، وقد قام الباحث بتصميم مقياس خاص بقياس جودة الخدمة مكون من ستة أبعاد، ويشتمل على(40) فقرةً، وتم تطبيق المقياس على عينة من طلبة جامعة الأقصى مكونة من(380) طالب وطالبة، وقد تم معالجة المقياس بالطرق الاحصائية من خلال(spss).

وقد بينت نتائج الدراسة ما يلي:

1 – أن جودة الخدمات الجامعية كما يدركها طلبة جامعة الأقصى بين الضعيف والمتوسط في معظم أبعاد المقياس.

2 – وجود فروق ذات دلالة إحصائية تُعزى لمتغير الجنس بين الذكور والإناث ولصالح الإناث في مستوى جودة الخدمات الجامعية المدركة في جميع الأبعاد ما عدا بعد (الأمان).

3 – وجود فروق ذات دلالة إحصائية في الدرجة الكلية، وفي الأبعاد الآتية (العناصر الملموسة – الاستجابة) لصالح التخصصات التطبيقية، في حين لا توجد فروق ذات دلالة في الأبعاد الأخرى (الاعتمادية، الأمان، التعاطف، خصوصية الجامعة).

4 – عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (α= 0.05) في جودة الخدمات الجامعية المدركة تبعًا لمتغير المستوى الدراسي (المستوى الأول المستوى الرابع).

5 – وجود فروق ذات دلالة إحصائية في جودة الخدمات الجامعية المدركة تُعزى لمتغير فرع الجامعة (فرع غزة – فرع خانيونس) وذلك لصالح فرع الجامعة في خانيونس، وفي جميع الأبعاد والدرجة الكلية، ما عدا بعد (الأمان).

وقد أوصت الدراسة بضرورة العمل على الارتقاء بمستوى الخدمات الجامعية المقدمة للطلبة بجامعة الأقصى في أبعاد المقياس ككل مع ضرورة العمل الجاد على أن تكون خصوصية الجامعة مدخلاً لرضا الطلاب عن جودة الأداء المقدم فعلاً للطلبة.

10. دراسة (الحافظ والنعيمي، 2010)، بعنوان: "دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (أنموذج مقترح)".

هدفت هذه الدراسة إلى تسليط الضوء على دور (ISO..27001) في تعزيز دور إدارة دورة حياة المعلومات، وما سيسهم به من إتاحة فرص وقدرات وقابليات أكثر في التعامل مع المعلومات والبيانات التي تتسم بالتزايد المضطرد في منظمات الأعمال إنتاجية أو خدمية.

وقد استخلص البحث إلى أن وجود ندرة وانحسار في التأكيد على عمل إدارة دورة حياة المعلومات في ظل المواصفة (ISO..27001)، في حين يجب أن يعمل مفهوم إدارة دورة حياة المعلومات في ظل المواصفة (ISO..27001) لإعطائه الصفة النظامية والقانونية الموحدة.

وقد أوصت الدراسة بضرورة التركيز على المفاهيم الحديثة التي تسلط الضوء على كل ما له علاقة بدورة حياة المعلومات، والمواصفة (ISO..27001) إذ إنَّ المنظمات اليوم أصبحت منظمات تتسم بتزايد هائل في المعلومات، الأمر الذي يتوجب معه توجيه الأنظار نحو المفاهيم التي من شانها أن تسهل وتنظم التعامل مع هذه الزيادات في المعلومات.

2.4.2 الدراسات الأجنبية:

1. دراسة (Napitupulu, 2018)، بعنوان: " Analysis of Student Satisfaction Toward Quality of Service Facility ".

هدفت هذه الدراسة إلى تحديد مدى تأثير جودة الخدمات على رضا المستخدمين. ولتحقيق أهداف الدراسة استخدم الباحث استبيان مبني على الاستقصاء لقياس الإدراك والتوقعات، تكون مجتمع الدراسة من (842) طالباً وطالبة في كلية علوم الحاسوب في جامعة (XYZ)، وتم توزيعه على عينة عشوائية من (89) طالباً وطالبة، وقد استجاب (84).

أظهرت النتائج وجود فجوة بين الإدراك وتوقعات المستجيبين الذين لديهم قيمة سلبية لكل عنصر. وهذا يعني أن مرافق الخدمات في الجامعة لا تلبي في الوقت الحالي توقعات الطلاب. وكانت أقل ثلاثة

مرافق خدمات في الجامعة والتي لديها أدنى مؤشر على تصور المستجيبين هي المختبر (2.56) ، والكمبيوتر والوسائط المتعددة (2.63) وكذلك شبكة واي فاي (2.99). وقد أوضحت النتائج أن حجم العلاقة بين الارتياح بجودة مرافق الخدمة هو (0.725) مما يعني وجود علاقة قوية وإيجابية. كما أن تأثير جودة مرافق الخدمة بما يرضي الطلاب هو (0.525) مما يعني أن الجودة المتغيرة لمرفق الخدمات يمكن أن تفسر (52.5)٪ من الرضى لدى الطلاب.

وفي ضوء هذه النتائج قدمت الدراسة توصيات لإدخال تحسينات لتحسين جودة الخدمات في مرافق الجامعة.

2. دراسة (Yilmaz & Yalman, 2016)، بعنوان: " A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks".

هدفت هذه الدراسة إلى فحص البنية التحتية لنظام المعلومات في الجامعات الحكومية الرائدة، والمؤسسات الجامعية في تركيا، والإبلاغ عن حالات المخاطر لهذه الجامعات من خلال أداة تحليل مخاطر أمن المعلومات، وتفسير النتائج التي تم الحصول عليها، والمساهمة في تطوير أمن المعلومات والوعي حول أمن المعلومات في الجامعات.

كشفت نتائج الدراسة أنه من الممكن زيادة أمن المعلومات في الجامعات من خلال اتخاذ العديد من الاحتياطات، كما أوضحت النتائج أن كل جامعة من الجامعات التي تم تحليلها تمتلك فريقاً لتطوير التطبيقات، ولكنها تحتاج إلى اتخاذ الاحتياطات وتوفير التدريب لموظفيها من أجل إجراءات تطوير التطبيقات الآمنة، علاوة على ذلك لوحظ أن الجامعات لا تأخذ بعناية كافية تصنيف البيانات وتشفير البيانات المعرضة للهجوم.

كما توصلت الدراسة إلى أن العامل البشري يؤثر مباشرة في كل مرحلة من مراحل التحليل بالإضافة إلى ذلك فقد توصلت الدراسة إلى أن توثيق وتحديث البيانات هي المشاكل الشائعة للجامعات ويمكن التغلب على هذه المشكلات من خلال زيادة الوعي بأمن المعلومات بين الناس.

3. دراسة (Alnawaiseh, 2014)، بعنوان: " Security information system of the computer center in mu'tah university "

هدفت هذه الدراسة إلى التعرف على أهمية الأمن والحماية في مركز الكمبيوتر في جامعة مؤتة، وفي سبيل تحقيق أهداف الدراسة قامت الباحثة بتحليل الأسئلة الآتية: هل الأمن والحماية مطلب ضروري؟

ما هي الأداة التي المعتمدة في تأمين النظام؟ وما هي العوامل التي أثرت على أمن النظام؟ وأخيراً كيف يمكن تأمين النظام بعد بنائه؟ وما هي الطرق التي يمكن استخدامها لذلك؟ وقد تم جمع البيانات لهذه الدراسة من خلال استبانة لتحقيق أهداف الدراسة.

توصلت الدراسة إلى أنه لا يوجد وعي لدى الموظفين في جامعة مؤتة حول قضايا أمن المعلومات، كما توصلت الدراسة إلى عدم وجود التزام من قبل الموظفين للحفاظ على أنظمتهم من المخاطر الشخصية، كما بينت النتائج عدم وجود التزام من قبل الموظفين في جامعة مؤتة حول حماية النظام من المخاطر المادية. كما أظهرت النتائج عدم وجود علاقة بين الوعي حول أمن المعلومات والمتغيرات الشخصية (الجنس، والعمر، وسنوات الخبرة، والمؤهل العلمي).

وفي ضوء النتائج التي توصلت لها الدراسة أوصت الدراسة بالكثير من التوصيات التي يجب أخذها في الاعتبار عند بناء نظام معلومات آمن (مادياً ومنطقياً) بحيث يجب تزويد كل موظف ببطاقة مغناطيسية مصحوبة بكلمة مرور لدخول المركز من خلال باب واحد فقط، وتحديد المسؤولية عن قضايا الأمن والحماية بوضوح مع نظام العقاب والمكافآت، وكذلك تدريب وتطوير الموظفين حول قضايا أمن المعلومات.

4. دراسة (NĂSTASE, et.al, 2009)، بعنوان: " Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises".

هدفت هذه الدراسة إلى التأكيد على أهمية تنفيذ أفضل ممارسات تكنولوجيا المعلومات في الشركات وتحديد التحديات الرئيسة التي يواجهها المدراء عند إنشاء إطار عمل معياري لمراقبة تكنولوجيا المعلومات من أجل تحقيق التوافق بين أفضل الممارسات والمتطلبات التجارية. أولاً ، وقد حاول الباحثون توضيح الضرورة المتزايدة لتطبيق معايير تكنولوجيا المعلومات في المنظمات العاملة في بيئات تقنية المعلومات مع التركيز على المعايير (COBIT وITIL وISO/IEC 27002).

كما هدفت هذه الدراسة إلى تحليل المعايير الثلاثة التي تُعدُّ بمثابة إرشاد للمنظمات الراغبة لتبني أفضل ممارسات تكنولوجيا المعلومات حول كيفية دمج الأطر العالمية الرائدة والممارسات والمعايير الأخرى في العلاقات بين المنظمات.

وقد ركز الجزء الأخير على أفضل الطرق للتنفيذ بطريقة فعالة لمعايير تكنولوجيا المعلومات، والتي تشمل تحديد استخدام المعايير وأفضل ممارسات تكنولوجيا المعلومات، وتحديد أولويات العمليات وفقاً لخطة عمل والتخطيط لخطوات نهج التنفيذ.

3.4.2 التعقيب على الدراسات السابقة:

تم إعداد الجدول رقم (1.1) والذي يوضح الفجوة البحثية وذلك من خلال التحدث عن أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة التي تناولت بعض الجوانب المتعلقة بالدراسة الحالية.

جدول (4.2): التعقيب على الدراسات السابقة.

م	أوجه المقارنة	الدراسة الحالية	أوجه التشابه والاختلاف مع الدراسات السابقة (الفجوة البحثية)
1	**متغيرات الدراسة**	تناولت هذه الدراسة متغيرين: **1- المتغير المستقل** واقع معايير أمن المعلومات (ISO-IEC 27002) **2- المتغير التابع** جودة الخدمات المقدمة في الجامعات الفلسطينية.	اتفقت هذه الدراسة في المتغير المستقل مع دراسة كل من: (المصري والأغا، 2018)، (العميري وآخرون، 2017)، (العربي، 2015)، (الدنف، 2013)، (عبد الجابر، 2013)، بينما اختلفت في المتغير التابع وهو أصل مشكلة الدراسة، وستركز الدراسة الحالية على معيار أمن الموارد البشرية كأحد معايير أمن المعلومات باعتباره الأصل في تحقيق الوظيفة الأمنية كأحد وظائف الإدارة بشكل عام.
2	**منهج الدراسة**	المنهج الوصفي التحليلي	اتفقت الدراسة مع جميع الدراسات السابقة في المنهجية.
3	**حدود الدراسة** **أ-الحد الموضوعي**	واقع معايير أمن المعلومات (ISO/IEC..27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة للطلبة.	اتفقت الدراسة في الحد الموضوعي نسبياً مع دراسة (الدنف، 2013)، (العميري وآخرون، 2017)، وانفردت الدراسة الحالية بدراسة العلاقة والأثر بين معايير أمن المعلومات ومتغير مهم لتحقيق الجودة في منظومة التعليم وهو جودة الخدمات المقدمة.

	ب- الحد المكاني	الجامعات الأهلية (جامعة الأزهر، الجامعة الإسلامية) والجامعات الخاصة (جامعة فلسطين)، والجامعات الحكومية(جامعة الأقصى) في قطاع غزة.	اتفقت الدراسة في الحد المكاني مع دراسة (الدنف، 2013) التي تم تطبيقها على الكليات التقنية في قطاع غزة بالنسبة للمتغير المستقل فقط. ودراسة (المصري والأغا، 2018) على الجامعات الفلسطينية بالنسبة لتطبيق المتغير المستقل فقط، والدراسة الحالية سيتم تطبيقها على الجامعات الفلسطينية في قطاع غزة، من وجهة نظر الإدارة.
	ج- الحد البشري	العاملون في الإدارة العليا والوسطى ودوائر شبكات المعلومات وتكنولوجيا المعلومات بالجامعات المذكورة.	اتفقت مع دراسة (الدنف، 2013) ودراسة (المصري والأغا، 2018)، ولكن الدراسة الحالية ستركز عل قياس جودة الخدمات من وجهة نظر الإدارة.
4	**أداة الدراسة**	الاستبانة	اتفقت مع جميع الدراسات السابقة باستخدام أداة الدراسة الاستبانة وأضافت بعض الدراسات الأخرى المقابلة.

4.4.2 ما تميزت به الدراسة:

1- تُعدَّ هذه الدراسة من أولى الدراسات بعد استقصاء الباحث وبعد استشارة الخبراء والمختصين التي تلقي الضوء على معايير أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية لاسيما في قطاع غزة، وعلاقة مدى الالتزام بهذه المعايير بجودة الخدمات المقدمة للطلاب.

2- قلة الدراسات التي تطرقت لمعايير أمن المعلومات في الجامعات الفلسطينية حيث وجد الباحث ندرة ملحوظة في تناول الدراسات لهذا الموضوع.

3- توضيح مدى العلاقة الموجودة بين الالتزام بتطبيق معايير أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية مع جودة الخدمات المقدمة للطلاب.

4- تقدم الدراسة صورة حقيقية عن واقع معايير أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية.

الفصل الثالث

منهجية الدراسة وإجراءاتها

1.3 مقدمة:

تعتبر منهجية الدراسة وإجراءاتها محوراً رئيساً يتم من خلاله إنجاز الجانب التطبيقي من الدراسة، وعن طريقها يتم الحصول على البيانات المطلوبة لإجراء التحليل الإحصائي للتوصل إلى النتائج التي يتم تفسيرها في ضوء أدبيات الدراسة المتعلقة بموضوع الدراسة.

وبناءً على ذلك تناول هذا الفصل وصفاً للمنهج المتبع ومجتمع وعينة الدراسة، وكذلك أداة الدراسة المستخدمة، وطريقة إعدادها وكيفية بنائها وتطويرها، ومدى صدقها وثباتها، وينتهي الفصل بالمعالجات الإحصائية التي استخدمت في تحليل البيانات واستخلاص النتائج، وفيما يلي وصف لهذه الإجراءات.

2.3 منهج الدراسة:

من أجل تحقيق أهداف الدراسة قام الباحث باستخدام المنهج الوصفي التحليلي الذي يحاول من خلاله وصف الظاهرة موضوع الدراسة، وتحليل بياناتها، والعلاقة بين مكوناتها، والآراء التي تطرح حولها والعمليات التي تتضمنها والآثار التي تحدثها.

ويعرف الحمداني (2006) المنهج الوصفي التحليلي بأنه: "المنهج الذي يسعى لوصف الظواهر أو الأحداث المعاصرة، أو الراهنة؛ فهو أحد أشكال التحليل والتفسير المنظم لوصف ظاهرة أو مشكلة، ويقدم بيانات عن خصائص معينة في الواقع، وتتطلب معرفة المشاركين في الدارسة والظواهر التي ندرسها والأوقات التي نستعملها لجمع البيانات".

ويرى الباحث أن تطبيق منهج الدراسة يصف واقع أمن المعلومات في الجامعات الفلسطينية وتفسير لطبيعة العلاقة بين أمن المعلومات وجودة الخدمات المقدمة من خلال المعايير الدولية، ويحلل واقع أمن المعلومات في الجامعات الفلسطينية بهدف الوصول الى مخرجات لتقديمها لصانع القرار لهذه الجامعات بهدف تطويرها وخاصة في اطار الأنظمة المتقدمة للوصول الى عدم اختراق المعلومات والحفاظ على خصوصيتها.

وقد استخدم الباحث مصدرين أساسيين للمعلومات:

1. **المصادر الثانوية:** اتجه الباحث في معالجة الإطار النظري للدراسة إلى مصادر البيانات الثانوية، والتي تتمثل في الكتب والمراجع العربية والأجنبية ذات العلاقة، والدوريات، والمقالات والتقارير، والأبحاث، والدراسات السابقة التي تناولت موضوع الدارسة، والبحث والمطالعة في مواقع الإنترنت المختلفة.
2. **المصادر الأولية:** لمعالجة الجوانب التحليلية لموضوع الدراسة لجأ الباحث إلى جمع البيانات الأولية من خلال الاستبانة كأداة للدراسة، صممت خصيصاً لهذا الغرض.

3.3 مجتمع الدراسة:

مجتمع الدراسة يعرف بأنه جميع مفردات الظاهرة التي يدرسها الباحث، وبناءً على مشكلة الدراسة وأهدافها؛ فإنَّ المجتمع المستهدف يتكون من المدراء والإداريين والعاملين في الإدارة العليا والوسطى، ودوائر شبكات المعلومات، وتكنولوجيا المعلومات بالجامعات الأهلية في قطاع غزة (جامعة الأزهر، الجامعة الإسلامية)، والجامعات الخاصة (جامعة فلسطين)، والجامعة الحكومية (جامعة الأقصى)،

بحيث كان حجم مجتمع الدراسة (601) كما هو موضح في جدول (1.3).

والجدول الآتي يوضح مجتمع الدراسة:

جدول(1.3) : يوضح مجتمع الدراسة

الرقم	المسمى	جامعة الأزهر		الجامعة الإسلامية		جامعة الأقصى		جامعة فلسطين
		أكاديمي	إداري	أكاديمي	إداري	أكاديمي	إداري	
1	عضو مجلس جامعة	18	0	23	0	20	0	13
2	نائب عميد أو مساعد	5	0	20	0	16	0	7
3	مدير دائرة	0	32	4	19	12	13	9
4	مساعد مدير، نائب مدير	0	9		17	3	2	2
5	رئيس قسم، مشرف	32	24	48	44	66	80	16
المجموع الفرعي		55	65	95	80	117	95	47
قسم التكنولوجيا		19		6		13		9
المجموع الكلي لكل جامعة		139		181		225		56
المجموع الكلي		601						

المصدر: بيانات شؤون الموظفين في الجامعات الفلسطينية في محافظات غزة 2019

4.3 عينة الدراسة:

1.4.3 العينة الاستطلاعية:

تكّونت عينة الدراسة الاستطلاعية من 40 موظف، بغرض تقنين أداة الدراسة، والتحقق من صلاحيتها للتطبيق على العينة الأصلية، وقد تم إدخالهم في التحليل النهائي للدراسة.

2.4.3 العينة الأصلية:

قام الباحث باستخدام طريقة العينة العشوائية الطبقية حسب الجامعة، حيث تم توزيع (370) استبانة على مجتمع الدراسة، وقد تم استرداد (333) استبانة بنسبة (90%)، وقد تم حساب حجم العينة من المعادلة التالية (Moore,2003):

$$n = \left(\frac{Z}{2m} \right)^2 \qquad (1)$$

حيث:

Z: القيمة المعيارية المقابلة لمستوى دلالة معلوم (مثلاً: Z=1.96 لمستوى دلالة $\alpha = 0.05$).

m: الخطأ الهامشي: ويُعبّر عنه بالعلامة العشرية (مثلاً: 0.05±)

يتم تصحيح حجم العينة في حالة المجتمعات النهائية من المعادلة:

$$n_{\text{المُعَدّل}} = \frac{nN}{N+n-1} \qquad (2)$$

حيث N تمثل حجم المجتمع

باستخدام المعادلة (1) نجد أن حجم العينة يساوي:

$$n = \left(\frac{1.96}{2\times 0.05}\right)^2 \cong 384$$

حيثُ إنَّ مجتمع الدراسة N =601، فإنَّ حجم العينة المُعَدّل باستخدام المعادلة (2) يساوي:

$$n_{\text{المُعَدّل}} = 234\frac{384*601}{601+384-1} \cong$$

وبذلك؛ فإنَّ حجم العينة المناسب في هذه الحالة يساوي 234 على الأقل.

5.3 أداة الدراسة:

تم إعداد استبانة حول "واقع تطبيق معايير أمن المعلومات (ISO- LEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة " حيث تتكون من ثلاثة أقسام رئيسة هي:

القسم الأول: وهو عبارة عن **المعلومات العامة** للمستجيبين (النوع، الجامعة، المؤهل العلمي، المسمى الوظيفي، وسنوات الخبرة).

القسم الثاني: وهو عبارة عن **معايير أمن المعلومات (ISO- LEC 27002)**، ويتكون من (61) فقرة، موزع على (12) مجالاً، وهي:

المجال الأول: تقييم المخاطر ومعالجتها، ويتكون من (5) فقرات.

المجال الثاني: السياسات الأمنية، ويتكون من (5) فقرات.

المجال الثالث: تنظيم أمن المعلومات، ويتكلون من (5) فقرات.

المجال الرابع: إدارة الأصول، ويتكون من (5) فقرات.

المجال الخامس: أمن الموارد البشرية، ويتكون من (5) فقرة.

المجال السادس: الأمن المادي والبيئي، ويتكون من (6) فقرات.

المجال السابع: إدارة العمليات/ الاتصالات وحمايتها، ويتكون من (5) فقرات.

المجال الثامن: التحكم في الوصول، ويتكون من (5) فقرات.

المجال التاسع: حيازة وتطوير وصيانة أنظمة المعلومات، ويتكون من (5) فقرات.

المجال العاشر: إدارة حوادث أمن المعلومات، ويتكون من (5) فقرة.

المجال الحادي عشر: إدارة استمرار العمل، ويتكون من (5) فقرة.

المجال الثاني عشر: الامتثال والتوافق، ويتكون من (5) فقرة.

وقد تم اعتمد الباحث على 12 مجال لشمول تلك المجالات وبناء على الدراسات الاستطلاعية الأولية والثانوية، حيث أن بعض المجالات متضمنة ضمن المجالات السابقة وتحديدا في الجامعات.

القسم الثالث: وهو عبارة عن **جودة الخدمات المقدمة،** ويتكون من (20) فقرة.

وقد تم استخدام مقياس ليكرت الخماسي لقياس استجابات المبحوثين لفقرات الاستبيان حسب جدول (2.3):

جدول (2.3): درجات مقياس ليكرت الخماسي

الاستجابة	قليلة جداً	قليلة	متوسطة	كبيرة	كبيرة جداً
الدرجة	1	2	3	4	5

6.3 خطوات بناء الاستبانة:

قام الباحث بإعداد أداة الدراسة للتعرف على " واقع تطبيق معايير أمن المعلومات (ISO-LEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة"، واتبع الباحث الخطوات الآتية لبناء الاستبانة:-

1- الإطلاع على الأدب الإداري، والدراسات السابقة ذات الصلة بموضوع الدراسة، والاستفادة منها في بناء الاستبانة، وصياغة فقراتها.
2- استشار الباحث عدداً من أساتذة الجامعات والمشرفين في تحديد مجالات الاستبانة، وفقراتها.
3- تحديد المجالات الرئيسة التي شملتها الاستبانة.
4- تحديد الفقرات التي تقع تحت كل مجال.

5- تم تصميم الاستبانة في صورتها الأولية.
6- تم مراجعة وتنقيح الاستبانة من قبل المشرف.
7- تم عرض الاستبانة على (10) من المحكمين من أعضاء هيئة التدريس في الجامعات الفلسطينية، كما هو في ملحق رقم (2).
8- في ضوء أراء المحكمين تم تعديل بعض فقرات الاستبانة من حيث الحذف أو الإضافة والتعديل، لتستقر الاستبانة في صورتها النهائية، ملحق (1).

7.3 صدق الاستبانة:

صدق الاستبانة يعني " أن يقيس الاستبيان ما وضع لقياسه" (الجرجاوي،2010)، كما يقصد بالصدق "شمول الاستقصاء لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها" (عبيدات وآخرون، 2001). وقد تم التأكد من صدق الاستبانة بطريقتين:

1- **صدق آراء المحكمين "الصدق الظاهري":**

يقصد بصدق المحكمين "هو أن يختار الباحث عددًا من المحكمين المتخصصين في مجال الظاهرة أو المشكلة موضوع الدراسة" (الجرجاوي،2010)، حيث تم عرض الاستبانة على مجموعة من المحكمين تألفت من (10) متخصصين في موضوع الدراسة، وأسماء المحكمين بالملحق رقم (2)، وقد استجاب الباحث لآراء المحكمين وقام بإجراء ما يلزم من حذف وتعديل في ضوء المقترحات المقدمة، وبذلك خرج الاستبيان في صورته النهائية (انظر الملحق رقم 2).

2- صدق المقياس:

أولا: الاتساق الداخلي Internal Validity

يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إلية هذه الفقرة، وقد قام الباحث بحساب الاتساق الداخلي للاستبانة، وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات الاستبانة، والدرجة الكلية للمجال نفسه.

- **الاتساق الداخلي لـ " معايير أمن المعلومات (ISO- LEC 27002) "**

جدول (3.3): نتائج الاتساق الداخلي – مجال " تقييم المخاطر ومعالجتها "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتوفر لدى الجامعة ضوابط لتقليص المخاطر التي تتعلق بالمعلومات	.890*	0.000
.2	يوجد توافق بين قوانين الجامعة مع اللوائح، والقوانين المحلية والدولية	.902*	0.000
.3	يوجد ضوابط لتشغيل ومتابعة الأنظمة	.875*	0.000
.4	تتوفر موازنة تطبيق الضوابط والضرر المتوقع حدوثه	.913*	0.000
.5	يتم تقييم المخاطر الأمنية بشكل دوري	.870*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (3.3) معامل الارتباط بين كل فقرة من فقرات مجال " تقييم المخاطر ومعالجتها "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (4.3): نتائج الاتساق الداخلي– مجال " السياسات الأمنية "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتوفر لدى الجامعة وثيقة عامة لسياسة أمن المعلومات	.831*	0.000
.2	تحرص الجامعة على المراجعة لسياسة أمن المعلومات	.927*	0.000
.3	تجاز وثيقة أمن المعلومات من الإدارة العليا للجامعة، ويتم تعميمها على كل العاملين، والجهات الخارجية ذات العلاقة	.872*	0.000
.4	تتوفر لدى الجامعة رؤية واضحة في إدارة أمن المعلومات	.840*	0.000
.5	تراعي الجامعة حساسية المعلومات الخارجية والخاصة بالسياسات الأمنية.	.812*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (4.3) معامل الارتباط بين كل فقرة من فقرات مجال " السياسات الأمنية "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $0.05 \geq \alpha$، وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (5.3): نتائج الاتساق الداخلي – مجال " تنظيم أمن المعلومات "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	تلتزم الإدارة العليا بدعم وتوفير مستلزمات أمن المعلومات	.837*	0.000
.2	يتم مراجعة أمن المعلومات بشكل دوري	.837*	0.000
.3	يوجد تحديد للمسئوليات التي تتعلق بأمن المعلومات	.781*	0.000
.4	يوجد تحديد لمتطلبات أمن المعلومات عند التعامل مع الأطراف الخارجية	.901*	0.000
.5	يوجد ضوابط لمعالجة المعلومات التي تستخدمها الأطراف الخارجية	.828*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($0.05 \geq \alpha$).

يوضح جدول (5.3) معامل الارتباط بين كل فقرة من فقرات مجال " تنظيم أمن المعلومات "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($0.05 \geq \alpha$)، وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (6.3): نتائج الاتساق الداخلي – مجال " إدارة الأصول "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتم تحديد واضح لأنواع الأصول: (المعلومات، والأصول البرامجية، والأصول المادية، وخدمات المعلومات، والأفراد، وسمعة الجامعة وصورتها)	.865*	0.000
.2	يتم توثيق كافة الأصول وإنشاء سجل لحفظها	.916*	0.000
.3	يتم تحديد مستوى الحماية المناسبة لأهمية الأصل المعلوماتي	.927*	0.000
.4	يتم تحديد ملكية كل أصل من أصول الجامعة بوضوح	.876*	0.000
.5	يوجد اهتمام واضح من قبل الجامعة بالأصول المعنوية وخاصة المعلومات	.835*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($0.05 \geq \alpha$).

يوضح جدول (6.3) معامل الارتباط بين كل فقرة من فقرات مجال " إدارة الأصول "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha \leq 0.05$)، وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (7.3): نتائج الاتساق الداخلي – مجال " أمن الموارد البشرية "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتم التأكد من دقة السيرة الذاتية وتحديداً المؤهلات الأكاديمية، والمهنية	.803*	0.000
.2	تتأكد الجامعة أنَّ العاملين لديهم القدرة على التعامل مع أمن المعلومات	.925*	0.000
.3	يوجد وضوح وإعلان للعقوبات الخاصة بالخروقات الأمنية للمعلومات	.837*	0.000
.4	يوجد تدريب للعاملين على أمن المعلومات	.866*	0.000
.5	يتم إلغاء كلمات المرور وصلاحيات الوصول عند انتهاء خدمة الموظف	.807*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (7.3) معامل الارتباط بين كل فقرة من فقرات مجال " أمن الموارد البشرية "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (8.3): نتائج الاتساق الداخلي – مجال " الأمن المادي والبيئي "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يقتصر الوصول إلى مرافق معالجة المعلومات على الأفراد المخولين فقط	.834*	0.000
.2	تتجنب الإدارة وضع أي لوحات تدل على مرافق معالجة المعلومات	.798*	0.000
.3	يتم فحص الأجهزة والمعدات قبل دخولها غرف معالجة المعلومات	.901*	0.000
.4	يوجد منع للوصول غير المرخص للأجهزة والمعدات، وحاويات المعلومات	.909*	0.000
.5	توضع ضوابط لحماية معدات، وأجهزة المنظمة من أي أخطار طبيعية	.858*	0.000
.6	توضع ضوابط لحماية معدات، وأجهزة المنظمة من أي أخطار بشرية	.853*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (8.3) معامل الارتباط بين كل فقرة من فقرات مجال " الأمن المادي والبيئي "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $0.05 \geq \alpha$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (9.3): نتائج الاتساق الداخلي – مجال " إدارة العمليات/ الاتصالات وحمايتها "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	تمتلك الجامعة أنظمة للحماية من البرامج الخبيثة	.895*	0.000
.2	تهتم الجامعة بالنسخ الاحتياطي لمواجهة كل ما هو طارئ	.911*	0.000
.3	يوجد سياسات وإجراءات لحماية تبادل المعلومات	.870*	0.000
.4	تحمي الجامعة الرسائل الإلكترونية من الوصول غير المصرح	.898*	0.000
.5	يتم ضمان تشغيل نظام المعلومات على مدار الساعة بأمان	.894*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($0.05 \geq \alpha$).

يوضح جدول (9.3) معامل الارتباط بين كل فقرة من فقرات مجال " إدارة العمليات/ الاتصالات وحمايتها "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $0.05 \geq \alpha$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (10.3): نتائج الاتساق الداخلي – مجال " التحكم في الوصول "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	تمتلك الجامعة إجراءات إدارة دخول المستخدم	.875*	0.000
.2	تتوفر إدارة لمسؤوليات المستخدم (كلمات المرور، وتأمين الأجهزة في غياب المستخدمين، وخلو سطح المكتب والشاشة)	.904*	0.000
.3	تتوفر لدى إدارة الجامعة إجراءات للتحكم في الوصول للشبكة	.912*	0.000
.4	يوجد لدى إدارة الجامعة إجراءات التحكم في الدخول إلى برامج التطبيقات	.883*	0.000
.5	يمكن لمستخدمي النظم العمل والاتصال عن بعد ومراقبة العمل عن بعد، بعيداً عن شبكة الجامعة	.777*	0.000

يوضح جدول (10.3) معامل الارتباط بين كل فقرة من فقرات مجال " التحكم في الوصول "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (11.3): نتائج الاتساق الداخلي – مجال " حيازة وتطوير وصيانة أنظمة المعلومات "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتم تحديد المتطلبات الأمنية اللازمة لتأمين أنظمة المعلومات	.849*	0.000
.2	توجد آليات للتأكد من صحة البيانات في أنظمة المعلومات	.910*	0.000
.3	تهتم الإدارة بحماية سرية وسلامة المعلومات من خلال وسائل التشفير	.788*	0.000
.4	يوجد ضوابط للتحكم في الوصول إلى ملفات نظام المعلومات	.888*	0.000
.5	يوجد تحديد للمسئوليات، والأدوار المرتبطة بأنظمة المعلومات	.834*	0.000

يوضح جدول (11.3) معامل الارتباط بين كل فقرة من فقرات مجال " حيازة وتطوير وصيانة أنظمة المعلومات "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (12.3): نتائج الاتساق الداخلي – مجال " إدارة حوادث أمن المعلومات "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يوجد ضوابط للتبليغ عن مواطن الضعف في أنظمة المعلومات	.744*	0.000
.2	يتم التعلم والاستفادة من حوادث أمن المعلومات في المستقبل	.869*	0.000
.3	يتم التأكد من تدخل الجهات الأمنية للتحقيق قبل طمس الحقائق	.859*	0.000
.4	يوجد تحديد للمسئوليات عند وقوع حوادث أمن المعلومات	.749*	0.000
.5	يتم الاستعانة بلجان متخصصة للتحقيق في حوادث أمن المعلومات	.768*	0.000

يوضح جدول (12.3) معامل الارتباط بين كل فقرة من فقرات مجال " إدارة حوادث أمن المعلومات "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (13.3): نتائج الاتساق الداخلي – مجال " إدارة استمرار العمل "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	تتوفر إمكانيات وموارد مالية للإفادة منها لإعادة استمرارية العمل	.824*	0.000
.2	يتم الحفاظ على خصوصية وسرية حوادث أمن المعلومات لضمان استمرار العمل	.859*	0.000
.3	يوفر النظام جمع الأدلة في أقرب وقت ممكن بعد وقوع الحادث	.832*	0.000
.4	يتوفر تحديد لكل الأحداث التي يمكن أن تسبب الانقطاع في الأعمال	.842*	0.000
.5	يوجد توثيق لكل العمليات التي تم اتخاذها لإعادة استمرارية العمل	.762*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (13.3) معامل الارتباط بين كل فقرة من فقرات مجال " إدارة استمرار العمل "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية $\alpha \leq 0.05$ وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (14.3): نتائج الاتساق الداخلي – مجال " الامتثال والتوافق "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	يتم تحديد للتشريعات المعمول بها وحماية الملكية الفكرية	.718*	0.000
.2	تسعى الجامعة للحد من سوء استخدام المعلومات الشخصية	.886*	0.000
.3	يوجد ضوابط لبرامج التشفير والتأكد من أنها تتوافق مع التشريعات	.828*	0.000
.4	تحصل الجامعة على البرامج والتطبيقات الأصلية	.852*	0.000
.5	يتم المحافظة على تراخيص الاستخدام وأدلة التشغيل وأقراص التثبيت	.809*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (14.3) معامل الارتباط بين كل فقرة من فقرات مجال " الامتثال والتوافق "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha \leq 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

- **الاتساق الداخلي لـ" جودة الخدمات المقدمة "**

جدول (15.3): نتائج الاتساق الداخلي – مجال " جودة الخدمات المقدمة "

م	الفقرة	معامل بيرسون للارتباط	القيمة الاحتمالية (Sig.)
.1	تتوفر خدمة الموقع الإلكتروني للجامعة بشكل دائم دون أي انقطاع	.812*	0.000
.2	يتمتع الموقع الإلكتروني للجامعة بواجهة تفاعلية ذات جاذبية للمستخدمين	.829*	0.000
.3	يتوفر لدى الطالب نوع من خصوصية البيانات	.866*	0.000
.4	يستطيع الطالب التوصل للحل الأمثل لما يطلبه عبر الخدمات الإلكترونية المقدمة من قبل الجامعة	.834*	0.000
.5	يمكن للطالب التبليغ عن المشاكل وحلها دون الحاجة إلى الذهاب إلى الجامعة	.673*	0.000
.6	توفر الخدمات الإلكترونية المقدمة للطلبة الوقت والجهد في كثير من الأحيان	.908*	0.000
.7	يوجد سرعة في الاستجابة في تقديم الخدمة للطلاب	.852*	0.000
.8	يوجد سهولة في استرجاع كلمة السر في حالة فقدانها من قبل الطالب	.801*	0.000
.9	يوجد سهولة في عملية إجراء القبول والتسجيل عبر الموقع الإلكتروني	.835*	0.000
10	من الصعب أن يتمكن أحد غير الطالب من الدخول إلى حسابه	.813*	0.000
11	يستطيع الطالب التعامل بسهولة مع الخدمات التي يقدمها موقع الجامعة	.821*	0.000
12	يستطيع الطالب إنجاز كافة المعاملات الخاصة به من خلال موقع الجامعة الإلكتروني	.758*	0.000
13	تقوم الجامعة بتحديث الخدمات الإلكترونية بشكل مستمر	.760*	0.000
14	يتحمل موقع الجامعة الإلكتروني الضغط الشديد في أوقات تسجيل المواد وظهور العلامات الفصلية	.810*	0.000
15	الخدمات الإلكترونية التي تقدمها الجامعة تضاهي المؤسسات الأخرى.	.739*	0.000
16	يحصل الطالب على المعلومات بسرعة فائقة	.843*	0.000
17	تتوفر جميع المعلومات التي تخص الطالب على بوابته الالكترونية	.879*	0.000
18	يستطيع الطالب تغيير اسم المستخدم وكلمة المرور على بوابته بسهولة	.838*	0.000

19	يثق الطلاب بأمن وحماية المعلومات التي توفرها الجامعة	.904*	0.000
20	يحصل الطالب على المعلومات التي يحتاجها بدقة فائقة	.805*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يوضح جدول (15.3) معامل الارتباط بين كل فقرة من فقرات مجال " جودة الخدمات المقدمة "، والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha \leq 0.05$)، وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

ثانيا: الصدق البنائي (Structure Validity)

يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة الوصول إليها، ويبين مدى ارتباط كل مجال من مجالات الدراسة بالدرجة الكلية لفقرات الاستبانة.

جدول (16.3): نتائج الصدق البنائي للاستبانة

المجال	معامل بيرسون للارتباط	القيمة الاحتمالية(Sig.)
تقييم المخاطر ومعالجتها	.777*	0.000
السياسات الأمنية	.858*	0.000
تنظيم أمن المعلومات	.885*	0.000
إدارة الأصول	.943*	0.000
أمن الموارد البشرية	.849*	0.000
الأمن المادي والبيئي	.878*	0.000
إدارة العمليات/ الاتصالات وحمايتها	.846*	0.000
التحكم في الوصول	.902*	0.000
حيازة وتطوير وصيانة أنظمة المعلومات	.920*	0.000
إدارة حوادث أمن المعلومات	.770*	0.000
إدارة استمرار العمل	.859*	0.000
الامتثال والتوافق	.870*	0.000
معايير أمن المعلومات (ISO- LEC 27002).	.990*	0.000
جودة الخدمات المقدمة.	.940*	0.000

* الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

يبين جدول (16.3) أن جميع معاملات الارتباط في جميع مجالات الاستبانة دالة إحصائياً عند مستوى معنوية ($\alpha \leq 0.05$)، وبذلك تعتبر جميع مجالات الاستبانة صادقه لما وضعت لقياسه.

8.3 ثبات الاستبانة Reliability:

يقصد بثبات الاستبانة هو أن يعطي الاستبيان نفس النتائج إذا أعيد تطبيقه عدة مرات متتالية، ويقصد به أيضاً إلى أي درجة يعطي المقياس قراءات متقاربة عند كل مرة يستخدم فيها، أو ما هي درجة اتساقه وانسجامه واستمراريته عند تكرار استخدامه في أوقات مختلفة (الجرجاوي،2010: 97).

وقد تحقق الباحث من ثبات استبانة الدراسة من خلال معامل ألفا كرونباخ Cronbach's Alpha Coefficient، وكانت النتائج كما هي مبينة في جدول (3.17).

جدول (17.3): معامل ألفا كرونباخ لقياس ثبات الاستبانة

المجال	عدد الفقرات	معامل ألفا كرونباخ
تقييم المخاطر ومعالجتها	5	0.934
السياسات الأمنية	5	0.910
تنظيم أمن المعلومات	5	0.889
إدارة الأصول	5	0.930
أمن الموارد البشرية	5	0.901
الأمن المادي والبيئي	6	0.928
إدارة العمليات/ الاتصالات وحمايتها	5	0.935
التحكم في الوصول	5	0.918
حيازة وتطوير وصيانة أنظمة المعلومات	5	0.907
إدارة حوادث أمن المعلومات	5	0.854
إدارة استمرار العمل	5	0.894
الامتثال والتوافق	5	0.877
معايير أمن المعلومات (ISO- LEC 27002)	61	0.986
جودة الخدمات المقدمة	20	0.974
جميع فقرات الاستبانة معاً	**81**	**0.990**

واضح من النتائج الموضحة في جدول (17.3) أن قيمة معامل ألفا كرونباخ مرتفعة لكل مجال حيث تتراوح بين (0.854، 0.986)، بينما بلغت لجميع فقرات الاستبانة (0.990)، وهذا يعنى أن الثبات مرتفع ودال إحصائياً.

وبذلك تكون الاستبانة في صورتها النهائية كما هي في الملحق (1) قابلة للتوزيع. ويكون الباحث قد تأكد من صدق وثبات استبانة الدراسة مما يجعله على ثقة تامة بصحة الاستبانة، وصلاحيتها لتحليل النتائج واختبار فرضيات الدراسة.

اختبار التوزيع الطبيعي (Normality Distribution Test):

تم استخدام اختبار كولمجوروف – سمرنوف (K-S) (Kolmogorov-Smirnov Test) لاختبار ما إذا كانت البيانات تتبع التوزيع الطبيعي من عدمه، وكانت النتائج كما هي في جدول (3.18).

جدول (18.3): يوضح نتائج اختبار التوزيع الطبيعي

المجال	قيمة الاختبار	القيمة الاحتمالية (Sig.)
تقييم المخاطر ومعالجتها	1.036	0.233
السياسات الأمنية	0.571	0.901
تنظيم أمن المعلومات	0.747	0.631
إدارة الأصول	0.686	0.735
أمن الموارد البشرية	0.670	0.761
الأمن المادي والبيئي	0.919	0.366
إدارة العمليات/ الاتصالات وحمايتها	0.965	0.310
التحكم في الوصول	0.746	0.633
حيازة وتطوير وصيانة أنظمة المعلومات	0.574	0.897
إدارة حوادث أمن المعلومات	0.612	0.849
إدارة استمرار العمل	0.680	0.743
الامتثال والتوافق	0.776	0.583
معايير أمن المعلومات (ISO- LEC 27002)	0.644	0.801
جودة الخدمات المقدمة.	0.939	0.341
جميع مجالات الاستبانة.	0.668	0.764

واضح من النتائج الموضحة في جدول (18.3) أن القيمة الاحتمالية (.Sig) أكبر من مستوى الدلالة (0.05) وبذلك فإن توزيع البيانات لهذه المجالات يتبع التوزيع الطبيعي حيث تم استخدام الاختبارات المعلمية لتحليل البيانات واختبار فرضيات الدراسة.

9.3 الأساليب الإحصائية المستخدمة:

تم تفريغ وتحليل الاستبانة ببرنامج Statistical Package for the Social Sciences (SPSS)، حيث تم استخدام الأدوات الإحصائية الآتية:

1. النسب المئوية والتكرارات (Frequencies & Percentages): لوصف عينة الدراسة.
2. المتوسط الحسابي، والوزن النسبي، والإنحراف المعياري.
3. اختبار ألفا كرونباخ (Cronbach's Alpha) لمعرفة ثبات فقرات الاستبانة.
4. اختبار كولمجوروف – سمرنوف (K-S) Kolmogorov-Smirnov Test لاختبار ما إذا كانت البيانات تتبع التوزيع الطبيعي من عدمه.
5. معامل ارتباط بيرسون (Pearson Correlation Coefficient) لقياس درجة الارتباط: يقوم هذا الاختبار على دراسة العلاقة بين متغيرين. وقد استخدمه الباحث لحساب الاتساق الداخلي، والصدق البنائي للاستبانة وكذلك لدراسة العلاقة بين المجالات.
6. اختبار (T) في حالة عينة واحدة (T-Test) لمعرفة ما إذا كانت متوسط درجة الاستجابة قد وصلت إلى الدرجة المتوسطة وهي (3) أم زادت أو قلت عن ذلك. ولقد استخدمه الباحث للتأكد من دلالة المتوسط لكل فقرة من فقرات الاستبانة.
7. نموذج تحليل الانحدار الخطي المتعدد (Multiple Linear Regression- Model).
8. اختبار T في حالة عينتين (Independent Samples T-Test) لمعرفة ما إذا كان هناك فروقات ذات دلالة إحصائية بين مجموعتين من البيانات المستقلة.
9. اختبار تحليل التباين الأحادي (One Way Analysis of Variance - ANOVA) لمعرفة ما إذا كان هناك فروقات ذات دلالة إحصائية بين ثلاث مجموعات أو أكثر من البيانات.

الفصل الرابع

تحليل البيانات واختبار فرضيات الدراسة ومناقشتها

1.4 مقدمة:

يتضمن هذا الفصل عرضاً لتحليل البيانات، واختبار فرضيات الدراسة، وذلك من خلال الإجابة عن أسئلة الدراسة، واستعراض أبرز نتائج الاستبانة، والتي تم التوصل إليها من خلال تحليل فقراتها، والوقوف على المعلومات العامة للمستجيبين، لذا تم إجراء المعالجات الإحصائية للبيانات المتجمعة من استبانة الدراسة، إذ تم استخدام برنامج الرزم الإحصائية للدراسات الاجتماعية (SPSS) للحصول على نتائج الدراسة التي تم عرضها وتحليلها في هذا الفصل.

2.4 الوصف الإحصائي لعينة الدراسة وفق المعلومات العامة

وفيما يلي عرض لخصائص عينة الدراسة وفق المعلومات العامة

- **توزيع عينة الدراسة حسب النوع**

جدول (1.4): توزيع عينة الدراسة حسب النوع

النوع	العدد	النسبة المئوية %
ذكر	295	88.6
أنثى	38	11.4
المجموع	333	100.0

يتضح من جدول (1.4) أن ما نسبته (88.6%) من عينة الدراسة ذكوراً، بينما (11.4%) إناثاً.
ويعزو الباحث هذه النتيجة إلى أن طبيعة العمل في الجامعات تستلزم وجود كلا الجنسين، وتتناسب هذه النتيجة مع الإحصاءات الرسمية حيث إنَّ نسبة الذكور العاملين للعام (2016) كانت (81%)، ونسبة الإناث (19%).

- **توزيع عينة الدراسة حسب الجامعة**

جدول (2.4): توزيع عينة الدراسة حسب الجامعة

الجامعة	العدد	النسبة المئوية %
الأقصى	115	34.5
الأزهر	76	22.8
الإسلامية	101	30.3
فلسطين	41	12.4
المجموع	333	100.0

يتضح من جدول (2.4) أن ما نسبته (34.5%) من عينة الدراسة يتبعون جامعة الأقصى، (22.8%) يتبعون جامعة الأزهر، (30.3%) يتبعون الجامعة الإسلامية، بينما (12.3%) يتبعون جامعة فلسطين.
ويرى الباحث أن هذه النتيجة تتناسب مع حجم هذه الجامعات حيث إنَّ جامعتي: الأقصى والإسلامية تعتبران الأكبر في قطاع غزة من حيث حجم الموظفين، يليهما جامعة الأزهر، ثم جامعة فلسطين.

- **توزيع عينة الدراسة حسب المؤهل العلمي**

جدول (3.4): توزيع عينة الدراسة حسب المؤهل العلمي

المؤهل العلمي	العدد	النسبة المئوية %
دبلوم	6	1.8
بكالوريوس	117	35.1
دراسات عليا	210	63.1
المجموع	333	100.0

يتضح من جدول (3.4) أن ما نسبته (1.8%) من عينة الدراسة مؤهلهم العلمي دبلوم، (35.1%) مؤهلهم العلمي بكالوريوس، بينما (63.1%) مؤهلهم العلمي دراسات عليا.
ويعزو الباحث هذه النتيجة إلى أن طبيعة العمل في الجامعات تستلزم التأهيل العلمي، وغالباً ما يكون المؤهل من الدراسات العليا.

- **توزيع عينة الدراسة حسب المسمى الوظيفي**

جدول (4.4): توزيع عينة الدراسة حسب المسمى الوظيفي

المسمى الوظيفي	العدد	النسبة المئوية %
إدارة عليا	66	19.8
إدارة وسطى	221	66.4
دائرة التكنولوجيا وشبكة المعلومات	46	13.8
المجموع	333	100.0

يتضح من جدول (4.4) أن ما نسبته (19.8%) من عينة الدراسة مسماهم الوظيفي إدارة عليا، (66.4%) مسماهم الوظيفي إدارة وسطى، بينما (13.8%) مسماهم الوظيفي دائرة التكنولوجيا وشبكة المعلومات. وتتناسب هذه النتيجة مع الهرم الإداري حيث إنَّ حجم الإدارة الوسطى أكبر من حجم الإدارة العليا.

- **توزيع عينة الدراسة حسب سنوات الخبرة**

جدول (5.4): توزيع عينة الدراسة حسب سنوات الخبرة

سنوات الخبرة	العدد	النسبة المئوية %
أقل من خمس سنوات	13	3.9
5- 10 سنوات	95	28.5
10-15 سنة	124	37.3
أكثر من 15 سنة	101	30.3
المجموع	333	100.0

يتضح من جدول (5.4) أن ما نسبته (3.9%) من عينة الدراسة سنوات خبرتهم أقل من خمس سنوات، (28.5%) تتراوح سنوات خبرتهم من (5- 10) سنوات، (37.3%) تتراوح سنوات خبرتهم من (10-15) سنة، بينما (30.3%) سنوات خبرتهم أكثر من (15) سنة.

ويرى الباحث بأن تنوع سنوات الخبرة لعينة الدراسة هو أمر طبيعي، غير أن فئة الخبرة أقل من خمس سنوات هي الأقل، ويعزو الباحث هذا الأمر إلى أن عملية توظيف موظفين جدد قد وصلت إلى أقل المعدلات وذلك في ظل الأزمات المالية الخانقة التي تمر بها الجامعات الفلسطينية.

3.4 المحك المعتمد في الدراسة (Ozen *et al.*, 2012):

لتحديد المحك المعتمد في الدراسة فقد تم تحديد طول الخلايا في مقياس ليكرت الخماسي من خلال حساب المدى بين درجات المقياس (5−1=4)، ومن ثم تقسيمه على أكبر قيمة في المقياس للحصول على طول الخلية أي (5/4=0.80) وبعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس (بداية المقياس وهي واحد صحيح) وذلك لتحديد الحد الأعلى لهذه الخلية، وهكذا أصبح طول الخلايا كما هو موضح في الجدول الآتي:

جدول (6.4): يوضح المحك المعتمد في الدراسة

المتوسط الحسابي	الوزن النسبي	درجة الموافقة
من 1 – 1.80	من 20% –36%	قليلة جدا
أكبر من 1.80 – 2.60	أكبر من 36% – 52%	قليلة
أكبر من 2.60 – 3.40	أكبر من 52%– 68%	متوسطة
أكبر من 3.40 – 4.20	أكبر من 68%– 84%	كبيرة
أكبر من 4.20 – 5	أكبر من 84 %–100%	كبيرة جداً

المصدر (المصري والأغا، 2018)

ولتفسير نتائج الدراسة والحكم على مستوى الاستجابة، اعتمد الباحث على ترتيب المتوسطات الحسابية على مستوى المجالات للاستبيان، ومستوى الفقرات في كل مجال، وقد حدد الباحث درجة الموافقة حسب المحك المعتمد للدراسة.

4.4 تحليل فقرات الاستبانة:

أولاً: تحليل فقرات " معايير أمن المعلومات(ISO- LEC 27002)"

- **تحليل فقرات مجال " تقييم المخاطر ومعالجتها "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي والترتيب وقيمة اختبار t لمعرفة درجة الموافقة، النتائج موضحة في جدول (7.4).

جدول (7.4): المتوسط الحسابي، والإنحراف المعياري والوزن النسبي والترتيب وقيمة اختبارt لكل فقرة من فقرات مجال " تقييم المخاطر ومعالجتها "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يتوفر لدى الجامعة ضوابط لتقليص المخاطر التي تتعلق بالمعلومات	4.00	0.96	79.94	1	كبيرة	18.86	0.000
2.	يوجد توافق بين قوانين الجامعة مع اللوائح والقوانين المحلية والدولية	3.64	1.01	72.85	2	كبيرة	11.65	0.000
3.	يوجد ضوابط لتشغيل ومتابعة أنظمة العمل	3.62	1.02	72.43	3	كبيرة	11.07	0.000
4.	تتوفر موازنة تطبيق الضوابط والضرر المتوقع حدوثه	3.44	1.01	68.73	5	كبيرة	7.88	0.000
5.	يتم تقييم المخاطر الأمنية بشكل دوري	3.56	0.96	71.17	4	كبيرة	10.58	0.000
	جميع فقرات المجال معاً	3.65	0.84	73.02		كبيرة	14.07	0.000

من جدول (7.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.65) أي أن الوزن النسبي (73.02%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.
وقد حصلت الفقرة " يتوفر لدى الجامعة ضوابط لتقليص المخاطر التي تتعلق بالمعلومات" على أعلى درجة موافقة بنسبة (79.94%)، بينما حصلت الفقرة " تتوفر موازنة تطبيق الضوابط والضرر المتوقع حدوثه" على أقل درجة موافقة بنسبة (68.73%).
ويرى الباحث بأن المخاطر التي تتعلق بالمعلومات هي من الأمور التي تمثل تهديداً واضحاً للجامعات الفلسطينية ولخصوصياتها، ولذلك تسعى الجامعات لوضع ضوابط ومحددات لتقليص هذه المخاطر.

ويعزو الباحث ذلك أنَّ مخاطر سرقة المعلومات وانتهاك الخصوصية أصبحت من الأمور الشائعة في ظل التطور التكنولوجي الرهيب، ولذلك كان لزاماً على الجامعات الفلسطينية العمل على التخلص من هذه المخاطر من خلال وضع مجموعة من الضوابط التي تقلصها وتحد من هذه المخاطر.
واتفقت هذه النتائج مع بعض الدراسات كدراسة (العميري وآخرون، 2017)، ودراسة (العربي، 2015)، ودراسة (الدنف، 2013).
واختلفت هذه النتائج مع دراسة (الحافظ والنعيمي، 2010)، ودراسة (Yilmaz & Yalman, 2016) التي كشفت أن الجامعات لا تأخذ بعناية كافية تصنيف البيانات وتشفير البيانات المعرضة للهجوم.

- **تحليل فقرات مجال " السياسات الأمنية "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (8.4).

جدول (8.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " السياسات الأمنية "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يتوفر لدى الجامعة وثيقة عامة لسياسة أمن المعلومات	3.56	0.93	71.11	1	كبيرة	10.84	0.000
2.	تحرص الجامعة على المراجعة لسياسة أمن المعلومات	3.29	0.97	65.71	5	متوسطة	5.39	0.000

3.	تجـــاز وثيقـــة أمـــن المعلومـات مـن الإدارة العليـا للجامعـة ويـتم تعميمهـا علـى كـل العـــاملين والجهـــات الخارجية ذات العلاقة	3.38	0.97	67.53	3	متوسطة	7.04	0.000
4.	تتـوفر لـدى الجامعـة رؤية واضحة في إدارة أمن المعلومات	3.32	1.00	66.43	4	متوسطة	5.84	0.000
5.	تراعـــي الجامعـــة حساســية المعلومــات الخارجيـــة والخاصـــة بالسياسات الأمنية	3.49	0.99	69.79	2	كبيرة	9.00	0.000
	جميـع فقـرات المجـال معاً	3.41	0.80	68.11		كبيرة	9.31	0.000

من جدول (8.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.41) أي أن الوزن النسبي (68.11%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يتوفر لدى الجامعة وثيقة عامة لسياسة أمن المعلومات " أعلى درجة موافقة بنسبة (71.11%)، بينما حصلت الفقرة " تحرص الجامعة على المراجعة لسياسة أمن المعلومات " على أقل درجة موافقة بنسبة (65.71%).

ويرى الباحث أنَّ هذه النتيجة توضح مدى أهمية أمن المعلومات بالنسبة للجامعات حيث تضع الجامعات وثيقة عامة لسياسة أمن المعلومات.

ويعزو الباحث هذه النتيجة إلى أهمية أمن المعلومات للمؤسسات كافة ومن ضمنها الجامعات، حيث أن أي انتهاك للمعلومات الخاصة بالجامعة يمثل تهديداً خطيراً قد يترتب عليه مشاكل كبيرة للجامعة، وبالتالي فإن الحفاظ على أمن المعلومات هو أولوية كبيرة ويحتاج بذل الكثير من الجهد في سبيله.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (المصري والأغا، 2018)، ودراسة (العميري وآخرون، 2017)، ودراسة (عبد الجابر، 2013) بأن الوزن النسبي لجميع فقرات السياسات الأمنية كانت مرتفعة.

واختلفت هذه النتيجة مع دراسة (Alnawaiseh, 2014) التي توصلت إلى أنه لا يوجد وعي لدى الموظفين في جامعة مؤتة حول قضايا أمن المعلومات، واختلفت مع دراسة (العربي، 2015) حيث حصل محور السياسات الأمنية على أقل قيمة بنسبة (19.05%).

- **تحليل فقرات مجال " تنظيم أمن المعلومات "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (9.4).

جدول (9.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " تنظيم أمن المعلومات "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	تلتزم الإدارة العليا بدعم وتوفير مستلزمات أمن المعلومات	3.56	0.94	71.29	2	كبيرة	10.99	0.000
2.	يتم مراجعة أمن المعلومات بشكل دوري	3.29	0.99	65.89	5	متوسطة	5.43	0.000
3.	يوجد تحديد للمسئوليات التي تتعلق بأمن المعلومات	3.84	0.99	76.82	1	كبيرة	15.57	0.000
4.	يوجد تحديد لمتطلبات أمن المعلومات عند التعامل مع الأطراف الخارجية	3.48	0.95	69.70	4	كبيرة	9.27	0.000
5.	يوجد ضوابط لمعالجة المعلومات التي تستخدمها الأطراف الخارجية	3.52	1.02	70.45	3	كبيرة	9.33	0.000

	جميع فقرات المجال معاً	3.54	0.79	70.82		كبيرة	12.46	0.000

من جدول (9.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.54) أي أن الوزن النسبي (70.82%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يوجد تحديد للمسئوليات التي تتعلق بأمن المعلومات " أعلى درجة موافقة بنسبة (76.82%)، بينما حصلت الفقرة " يتم مراجعة أمن المعلومات بشكل دوري " على أقل درجة موافقة بنسبة (65.89%).

وهذا يوضح أنَّ أهم السياسات التي تحافظ على مستوى أمن المعلومات هو عملية تحديد المسؤوليات، حيث إنَّ تحديد المسؤوليات يعتبر عاملاً مهماً في منع أي شخص غير مخول له من الوصول إلى المعلومات.

ويعزو الباحث ذلك إلى أهمية الحفاظ على أمن المعلومات واتباع كافة الوسائل التي تساعد على ترسيخ أمن المعلومات والحفاظ عليه، حيثُ أنَّ هذا الأمر يمثل ضرورة لا غنى للجامعات والقائمين عليها.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013)، ودراسة (الدنف، 2013)، ودراسة (المصري والأغا، 2018) في أن جميع فقرات تنظيم المعلومات كانت مرتفعة.

واختلفت مع دراسة (عمار والكبيسي، 2012) التي توصلت إلى عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية.

- **تحليل فقرات مجال " إدارة الأصول "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (10.4).

جدول (10.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " إدارة الأصول "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يتم تحديد واضح لأنواع الأصول (المعلومات، والأصول البرامجية، والأصول المادية، وخدمات	3.56	0.95	71.17	1	كبيرة	10.69	0.000

	المعلومات، والأفراد، وسمعة وصورة الجامعة)							
2.	يتم توثيق كافة الأصول وإنشاء سجل لحفظها.	3.46	1.02	69.25	4	كبيرة	8.23	0.000
3.	يتم تحديد مستوى الحماية المناسبة لأهمية الأصل المعلوماتي.	3.50	1.01	70.03	3	كبيرة	9.08	0.000
4.	يتم تحديد ملكية كل أصل من أصول الجامعة بوضوح.	3.55	0.98	71.05	2	كبيرة	10.30	0.000
5.	يوجد اهتمام واضح من قبل الجامعة بالأصول المعنوية وخاصة المعلومات.	3.43	0.98	68.65	5	كبيرة	8.07	0.000
	جميع فقرات المجال معاً	3.50	0.83	70.03		كبيرة	11.02	0.000

من جدول (10.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.50) أي أن الوزن النسبي (70.03%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.
وقد حصلت الفقرة " يتم تحديد واضح لأنواع الأصول (المعلومات، والأصول البرامجية، والأصول المادية، وخدمات المعلومات، والأفراد، وسمعة وصورة الجامعة)" على أعلى درجة موافقة بنسبة (71.17%)، بينما حصلت الفقرة " يوجد اهتمام واضح من قبل الجامعة بالأصول المعنوية وخاصة المعلومات " على أقل درجة موافقة بنسبة (68.65%).
وهذا يوضح بأن إدارة الأصول من العناصر الأساسية في أمن المعلومات، وأنَّ إنزال الأسماء مسمياتها وتوضيح كل ما يتعلق بها يسهل عملية متابعتها والتأكد من أن كل ما يتعلق بالأصول يمضي بشكل سليم وصحيح.

ويعزو الباحث ذلك أنَّ أصول الجامعة من العناصر شديدة الأهمية، وأنَّها تمثل العنصر الأكثر قيمة في الجامعة، وبالتالي تسعى الجامعة للحفاظ على هذا العنصر من أي تلاعب أو انتهاك.
واتفقت هذه النتائج مع بعض الدراسات كدراسة (المصري والأغا، 2018)، ودراسة (العميري وآخرون، 2017).

واختلفت هذه النتيجة مع دراسة (العربي، 2015) حيث توصلت الدراسة أن الجامعات تطبق معايير أمن المعلومات بنسبة (28.2%).

- **تحليل فقرات مجال " أمن الموارد البشرية "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (11.4).

جدول (11.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " أمن الموارد البشرية "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يتم التأكد من دقة السيرة الذاتية وتحديدا المؤهلات الأكاديمية والمهنية للعاملين	3.68	0.97	73.69	1	كبيرة	12.85	0.000
2.	تتأكد الجامعة أنَّ العاملين لديهم القدرة على التعامل مع قضايا أمن المعلومات	3.34	0.99	66.85	4	متوسطة	6.30	0.000
3.	يوجد وضوح وإعلان للعقوبات الخاصة بالخروقات الأمنية للمعلومات	3.40	1.01	67.99	3	متوسطة	7.18	0.000
4.	يوجد تدريب للعاملين على أمن المعلومات	3.34	0.97	66.73	5	متوسطة	6.35	0.000
5.	يتم إلغاء كلمات المرور وصلاحيات الوصول عند انتهاء خدمة الموظف	3.66	0.97	73.15	2	كبيرة	12.36	0.000
	جميع فقرات المجال	3.48	0.80	69.68		كبيرة	11.07	0.000

	معاً							

من جدول (11.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.48) أي أن الوزن النسبي (69.68%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يتم التأكد من دقة السيرة الذاتية وتحديدا المؤهلات الأكاديمية والمهنية للعاملين " على أعلى درجة موافقة بنسبة (73.69%)، بينما حصلت الفقرة " يوجد تدريب للعاملين على أمن المعلومات " على أقل درجة موافقة بنسبة (66.73%).

وهذا يوضح مدى أهمية الموارد البشرية بالنسبة للجامعة وكذلك أمن الموارد البشرية، حيث أن الحفاظ على أمن الموارد البشرية وكل ما يرتبط بها يمثل أحد الأولويات الأمنية التي تسعى الجامعة للتأكد منها.

ويعزو الباحث ذلك أنَّ الموارد البشرية مثلها مثل الأصول المادية، تعتبر ركناً أساسياً في نجاح الجامعة، بل إنها الأهم حسب بعض الباحثين، وبالتالي فإن التأكد من أمن المعلومات المرتبطة بالموارد البشرية يمثل أحد الحاجات الأساسية التي يجب على الجامعة التأكد من سلامتها.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) ودراسة (NĂSTASE, et.al, 2009)، ودراسة (Yilmaz & Yalman, 2016) التي توصلت إلى أن العامل البشري يؤثر مباشرة في كل مرحلة من مراحل أمن المعلومات.

واختلفت هذه النتيجة مع دراسة (عمار والكبيسي، 2012) التي توصلت إلى عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية.

- **تحليل فقرات مجال " الأمن المادي والبيئي "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (12.4).

جدول (12.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " الأمن المادي والبيئي "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يقتصر الوصول إلى مرافق معالجة المعلومات على الأفراد	3.79	0.93	75.86	1	كبيرة	15.62	0.000

	المخولين فقط							
2.	تتجنب الإدارة وضع أي لوحات تدل على مرافق معالجة المعلومات	3.36	0.95	67.27	6	متوسطة	7.01	0.000
3.	يتم فحص الأجهزة والمعدات قبل دخولها غرف معالجة المعلومات	3.42	1.02	68.37	5	كبيرة	7.50	0.000
4.	يوجد منع للوصول غير المرخص للأجهزة والمعدات وحاويات المعلومات	3.48	0.95	69.61	3	كبيرة	9.21	0.000
5.	توضع ضوابط لحماية معدات وأجهزة المنظمة من أي أخطار طبيعية	3.53	0.95	70.51	2	كبيرة	10.07	0.000
6.	توضع ضوابط لحماية معدات وأجهزة المنظمة من أي أخطار بشرية	3.43	0.95	68.55	4	كبيرة	8.20	0.000
	جميع فقرات المجال معاً	3.50	0.78	70.03		كبيرة	11.71	0.000

من جدول (12.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.50) أي أن الوزن النسبي (70.03%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يقتصر الوصول إلى مرافق معالجة المعلومات على الأفراد المخولين فقط" على أعلى درجة موافقة بنسبة (75.86%)، بينما حصلت الفقرة " تتجنب الإدارة وضع أي لوحات تدل على مرافق معالجة المعلومات " على أقل درجة موافقة بنسبة (67.27%).

وهذه النتيجة توضح أنَّ كلً من الأمن المادي والبيئي عنصران مهمان في أمن المعلومات، حيث أن منع الوصول للمعلومات إلا على الأشخاص المخولين بذلك، والتأكد من فحص الأجهزة والمعدات قبل استخدامها، وكذلك وضع ضوابط لحماية معدات وأجهزة المنظمات، كلها أمور توضح مدى أهمية الأمن المادي والبيئي للحفاظ على أمن المعلومات الخاص بالجامعة.

ويعزو الباحث ذلك أنَّ اقتصار عملية الوصول إلى المعلومات على أشخاص محددين يقلل من خطر انتهاك أمن المعلومات بدرجة كبيرة، وكذلك يساعد على اكتشاف أي انتهاك للمعلومات وحصره في خيارات قليلة، كما أن الحفاظ على الأجهزة وفحصها بشكل دوري يساهم في ذلك بشكل كبير.
واتفقت هذه النتائج مع بعض الدراسات كدراسة (العميري وآخرون، 2013)، ودراسة (عبد الجابر، 2013).
واختلفت هذه النتيجة مع دراسة (الحافظ والنعيمي، 2010) التي توصلت إلى وجود ندرة وانحسار في التأكيد على عمل إدارة دورة حياة المعلومات في ظل المواصفة (ISO 27001).

- **تحليل فقرات مجال " إدارة العمليات/ الاتصالات وحمايتها "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (13.4).

جدول (13.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " إدارة العمليات/ الاتصالات وحمايتها "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	تمتلك الجامعة أنظمة للحماية من البرامج الخبيثة	3.69	0.95	73.75	1	كبيرة	13.21	0.000
2.	تهتم الجامعة بالنسخ الاحتياطي لمواجهة كل ما هو طارئ	3.47	1.06	69.37	5	كبيرة	8.09	0.000
3.	يوجد سياسات وإجراءات لحماية تبادل المعلومات	3.57	1.05	71.41	2	كبيرة	9.90	0.000

4.	تحمي الجامعة الرسائل الإلكترونيـــــة مـــــن الوصول غير المصرح	3.51	0.97	70.15	4	كبيرة	9.57	0.000
5.	يتم ضمان تشغيل نظام المعلومـات علـى مـدار الساعة بأمان	3.56	1.00	71.17	3	كبيرة	10.22	0.000
	جميـع فقـرات المجـال معاً	3.56	0.84	71.17		كبيرة	12.16	0.000

من جدول (13.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.56) أي أن الوزن النسبي (71.17%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " تمتلك الجامعة أنظمة للحماية من البرامج الخبيثة " على أعلى درجة موافقة بنسبة (73.75%)، بينما حصلت الفقرة " تهتم الجامعة بالنسخ الاحتياطي لمواجهة كل ما هو طارئ " على أقل درجة موافقة بنسبة (69.37%).

وهذا يوضح أن إدارة العمليات بما فيها الاتصالات وحمايتها من أشد الأمور خطورة على أمن المعلومات، حيث أن الاتصالات تعتبر الجسر الأساسي والرئيسي لعملية انتهاك المعلومات، حيث أن عمليات سرقة المعلومات التقليدية بالوصول إلى الأجهزة بشكل شخصي قد اندثرت مع التقدم الرهيب في التكنولوجيا وأصبح الوصول إلى المعلومات من خلال برامج الاتصالات والشبكات.

ويعزو الباحث ذلك أنَّ شبكات الاتصالات تمثل تهديداً خطيراً لكل من يسعى للحفاظ على معلوماته، حيث أن هناك الكثير من أنواع التهديدات التي تطال المعلومات وأمنها سواء كانت برمجيات خبيثة أو القدرة على السيطرة على أسماء المستخدمين وكلمات المرور، ولهذا نجد أن هناك اهتماماً كبيراً من قبل الجامعات لتحييد هذه التهديدات وتقليل مستواها إلى أقل درجة ممكنة من خلال توفير أنظمة حماية ضد البرامج الخبيثة، وكذلك وضع جدار ناري، ومضادات فيروسات، والاحتفاظ بنسخ احتياطية لمواجهة أي أمر طارئ.. الخ.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (العميري وآخرون، 2017)، ودراسة (المصري والأغا، 2018).

واختلفت هذه النتيجة مع دراسة (العربي، 2015) التي توصلت إلى أن الجامعات العربية تطبق معايير أمن المعلومات بنسبة (28.2%).

- **تحليل فقرات مجال " التحكم في الوصول "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (14.4).

جدول (14.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " التحكم في الوصول "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	تمتلك الجامعة إجراءات إدارة دخول المستخدم	4.05	0.92	80.96	1	كبيرة	20.78	0.000
2.	تتوفر إدارة لمسؤوليات المستخدم (كلمات المرور، تأمين الأجهزة في غياب المستخدمين، خلو سطح المكتب والشاشة)	3.61	1.02	72.17	4	كبيرة	10.86	0.000
3.	تتوفر لدى إدارة الجامعة إجراءات للتحكم في الوصول للشبكة	3.63	1.06	72.59	3	كبيرة	10.83	0.000
4.	يوجد لدى إدارة الجامعة إجراءات التحكم في الدخول إلى برامج التطبيقات	3.55	1.01	71.05	5	كبيرة	9.99	0.000
5.	يمكن لمستخدمي النظم العمل والاتصال عن بعد ومراقبة العمل عن بعد، بعيداً عن شبكة الجامعة	3.71	0.97	74.29	2	كبيرة	13.46	0.000

	جميع فقرات المجال معاً	3.71	0.85	74.22		كبيرة	15.34	0.000

من جدول (14.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.71) أي أن الوزن النسبي (74.22%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.
وقد حصلت الفقرة " تمتلك الجامعة إجراءات إدارة دخول المستخدم " على أعلى درجة موافقة بنسبة (80.96%)، بينما حصلت الفقرة " يوجد لدى إدارة الجامعة إجراءات التحكم في الدخول إلى برامج التطبيقات " على أقل درجة موافقة بنسبة (71.05%).
وتتناسب هذه النتيجة مع نتيجة محور تنظيم أمن المعلومات، حيث أن كلاهما كان بنسبة كبيرة وهذا يوضح مدى أهمية التحكم في الوصول وتحديد من هم الأشخاص المخول لهم بالوصول إلى المعلومات، وذلك لمنع أي تهديد أو عملية اختراق أو انتهاك لأمن المعلومات الخاصة بالجامعة وموظفيها.

ويعزو الباحث ذلك إلى عملية التحكم في الوصول التي تعتبر أحد السياسات الفاعلة والناجحة في تقليل التهديدات المرتبطة بأمن المعلومات، وكذلك سهولة تحديد من المسؤول عن أي انتهاك محتمل لأمن المعلومات.
واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013)، ودراسة (الدنف، 2013)، ودراسة (المصري والأغا، 2018).
واختلفت مع دراسة (عمار والكبيسي، 2012) التي توصلت إلى عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية.

- **تحليل فقرات مجال " حيازة وتطوير وصيانة أنظمة المعلومات "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (15.4).

جدول (15.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " حيازة وتطوير وصيانة أنظمة المعلومات "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يـتم تحديـد المتطلبـات	3.74	0.90	74.71	1	كبيرة	14.92	0.000

	الأمنية اللازمة لتأمين أنظمة المعلومات.							
2.	توجد آليات للتأكد من صحة البيانات في أنظمة المعلومات.	3.42	0.98	68.35	5	كبيرة	7.75	0.000
3.	تهتم الإدارة بحماية سرية وسلامة المعلومات من خلال وسائل التشفير.	3.49	0.94	69.79	4	كبيرة	9.54	0.000
4.	يوجد ضوابط للتحكم في الوصول إلى ملفات نظام المعلومات.	3.50	0.98	69.94	3	كبيرة	9.22	0.000
5.	يوجد تحديد للمسئوليات والأدوار المرتبطة بأنظمة المعلومات.	3.64	0.91	72.77	2	كبيرة	12.82	0.000
	جميع فقرات المجال معاً	3.56	0.78	71.12		كبيرة	12.95	0.000

من جدول (15.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.56) أي أن الوزن النسبي (71.12%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يتم تحديد المتطلبات الأمنية اللازمة لتأمين أنظمة المعلومات " على أعلى درجة موافقة بنسبة (74.71%)، بينما حصلت الفقرة " توجد آليات للتأكد من صحة البيانات في أنظمة المعلومات" على أقل درجة موافقة بنسبة (68.35%).

وتوضح هذه النتيجة مدى أهمية تطوير وصيانة أنظمة المعلومات بشكل مستمر، حيثُ أنَّ متابعة التحديثات الأمنية التي تقوم بنشرها شركات أمن المعلومات وشركات برامج مضادات البرامج الخبيثة تساهم بشكل كبير في تحييد التهديدات والتقليل منها، وكذلك فإن تطوير نظام المعلومات بشكل مستمر يضمن إغلاق العديد من الثغرات الأمنية التي يستغلها المتسللون ولصوص المعلومات.

ويعزو الباحث ذلك أنَّ هناك قناعة راسخة لدى إدارة الجامعات حول أهمية تطوير وتحديث أنظمة المعلومات بشكل مستمر، حيث أنَّ تطوير وتحديث نظام المعلومات يعتبر من البديهيات والمسلمات في مجال أمن المعلومات، ولا يغيب ذلك عن إدارة الجامعة من حيث أهميته وفائدته الكبيرة في تقليل التهديدات المرتبطة بانتهاك أمن المعلومات.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (الدنف، 2013) التي توصلت إلى أن الإدارات العليا للكليات التقنية تدرك أهمية سياسات أمن المعلومات.
واختلفت هذه النتيجة مع دراسة (Alnawaiseh, 2014) التي توصلت إلى أنه لا يوجد وعي لدى الموظفين في جامعة مؤتة حول قضايا أمن المعلومات.

- **تحليل فقرات مجال " إدارة حوادث أمن المعلومات "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (16.4).

جدول (16.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " إدارة حوادث أمن المعلومات "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يوجد ضوابط للتبليغ عن مواطن الضعف في أنظمة المعلومات	3.71	0.89	74.17	1	كبيرة	14.54	0.000
2.	يتم التعلم والاستفادة من حوادث أمن المعلومات في المستقبل	3.39	0.96	67.75	5	متوسطة	7.40	0.000
3.	يتم التأكد من تدخل الجهات الأمنية للتحقيق قبل طمس	3.44	0.96	68.89	4	كبيرة	8.42	0.000

	الحقائق							
4.	يوجد تحديد للمسئوليات عند وقوع حوادث أمن المعلومات	3.51	1.00	70.15	3	كبيرة	9.30	0.000
5.	يـتم الاسـتعانة بلجـان متخصصة للتحقيق في حوادث أمن المعلومات	3.52	0.97	70.39	2	كبيرة	9.73	0.000
	جميـع فقـرات المجـال معاً	3.51	0.77	70.27		كبيرة	12.13	0.000

من جدول (16.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.51) أي أن الوزن النسبي (70.27%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.
وقد حصلت الفقرة " يوجد ضوابط للتبليغ عن مواطن الضعف في أنظمة المعلومات " على أعلى درجة موافقة بنسبة (74.17%)، بينما حصلت الفقرة " يتم التعلم والاستفادة من حوادث أمن المعلومات في المستقبل " على أقل درجة موافقة بنسبة (67.75%).
وتمثل هذه النتيجة تفسيراً لقناعات الجامعة حول ضرورة متابعة نظم المعلومات الخاصة بها والاستفادة من أي حوادث سابقة مثلت تهديداً لنظام المعلومات وأمن المعلومات، وبالتالي كان لزاماً على الجامعة وإدارتها التعلم والاستفادة من حوادث أمن المعلومات في المستقبل لمنع أي تكرار لهذه الحوادث.

ويعزو الباحث ذلك أنَّ الاستفادة والتعلم من الحوادث التي حدثت في السابق تمثل مصدراً ممتازاً لزيادة الخبرة في مجال أمن المعلومات، وكذلك منع أي احتمال لتكرار مثل هذه الحوادث.
واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) التي أظهرت فاعلية اجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع والاكتشاف والتصحيح).
واختلفت هذه النتيجة مع دراسة (Alnawaiseh, 2014) التي توصلت إلى عدم وجود التزام من قبل الموظفين في جامعة مؤتة حول حماية النظام من المخاطر المادية.

- **تحليل فقرات مجال " إدارة استمرار العمل "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (17.4).

جدول (17.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " إدارة استمرار العمل "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	تتوفر إمكانيات وموارد مالية للإفادة منها لإعادة استمرارية العمل	3.72	0.94	74.34	1	كبيرة	13.97	0.000
2.	يتم الحفاظ على خصوصية وسرية حوادث أمن المعلومات لضمان استمرار العمل	3.44	0.98	68.73	5	كبيرة	8.10	0.000
3.	يوفر النظام جمع الأدلة في أقرب وقت ممكن بعد وقوع الحادث	3.52	0.95	70.42	3	كبيرة	9.96	0.000
4.	يتوفر تحديد لكل الأحداث التي يمكن أن تسبب الانقطاع في الأعمال	3.46	0.99	69.13	4	كبيرة	8.45	0.000
5.	يوجد توثيق لكل العمليات التي تم اتخاذها لإعادة استمرارية العمل	3.62	0.94	72.31	2	كبيرة	11.96	0.000
	جميع فقرات المجال معاً	3.55	0.78	70.98		كبيرة	12.90	0.000

من جدول (17.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.55) أي أن الوزن النسبي (70.98%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " تتوفر إمكانيات وموارد مالية للإفادة منها لإعادة استمرارية العمل " أعلى درجة موافقة بنسبة (74.34%)، بينما حصلت الفقرة " يتم الحفاظ على خصوصية وسرية حوادث أمن المعلومات لضمان استمرار العمل " أقل درجة موافقة بنسبة (68.73%).

وتمثل هذه النتيجة أهمية توفير المكونات والموارد المادية لغرض استمرار العمل، حيث أن غياب أن عنصر تحتاجه المنظمة لاستمرار العمل قد يمثل عائقاً وتهديداً للاستمرارية.

ويعزو الباحث ذلك أنَّ استمرارية العمل بشكل طبيعي يُعدُّ أمراً مهماً من وجهة نظر الإدارة في الجامعات، حيث أن أي تأخير أو تعطيل للعمل قد يؤدي إلى نتائج كارثية على مستوى الأنشطة الأساسية التي تقوم بها الجامعة لصالح المستفيدين منها.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (المصري والأغا، 2018) التي توصلت إلى أن المتوسط الحسابي النسبي لجميع فقرات ممارسة معيار أمن المعلومات (ISO/IEC 27002) يساوي (84.37%).

واختلفت هذه النتيجة مع دراسة (العربي، 2015) التي توصلت إلى أن الجامعات حرصت على تطبيق معايير فرعية في (11) معياراً أساسياً بنسبة 28.2% من إجمالي معايير آيزو 27002.

- **تحليل فقرات مجال " الامتثال والتوافق "**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (18.4).

جدول (18.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " الامتثال والتوافق "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	يتم تحديد للتشريعات المعمول بها وحماية الملكية الفكرية	3.61	0.94	72.27	1	كبيرة	11.85	0.000
2.	تسعى الجامعة للحد من سوء استخدام المعلومات الشخصية	3.31	0.96	66.27	5	متوسطة	5.92	0.000

3.	يوجد ضوابط لبرامج التشفير والتأكد من أنها تتوافق مع التشريعات القانونية	3.45	1.01	68.92	4	كبيرة	8.06	0.000
4.	تحصل الجامعة على البرامج والتطبيقات الأصلية	3.51	1.04	70.27	3	كبيرة	8.99	0.000
5.	يتم المحافظة على تراخيص الاستخدام وأدلة التشغيل وأقراص التثبيت	3.52	1.01	70.42	2	كبيرة	9.36	0.000
	جميع فقرات المجال معاً	3.48	0.82	69.61		كبيرة	10.72	0.000

من جدول (18.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.48) أي أن الوزن النسبي (69.61%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " يتم تحديد للتشريعات المعمول بها وحماية الملكية الفكرية " على أعلى درجة موافقة بنسبة (72.27%)، بينما حصلت الفقرة " تسعى الجامعة للحد من سوء استخدام المعلومات الشخصية " على أقل درجة موافقة بنسبة (66.27%).

وتتناسب هذه النتيجة مع ما هو متعارف عليه في مجال أمن المعلومات، حيث أن وضع تشريعات وقوانين مرتبطة بأمن المعلومات وملاحظة مدى التزام العاملين بها هو أحد أهم معايير التقييم لمدى نجاعة نجاح المؤسسة في الحفاظ على أمن المعلومات الخاص بها.

ويعزو الباحث ذلك أنَّ الجامعة ولغرض الوصول إلى تقييم لمدى حفاظها على أمن معلوماتها تسعى إلى التأكد من مدى التزام العاملين فيها بالقوانين والإجراءات التي وضعتها للحفاظ على أمن المعلومات، حيث كلما كان التزام وامتثال العاملين لهذه القوانين والإجراءات أكبر، كلما كانت عملية المحافظة على أمن المعلومات أكبر وأفضل.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (العميري وآخرون، 2017) التي توصلت إلى توافق أغلب ممارسات أمن المعلومات في المكتبة الرئيسة مع ممارسات المعيار الدولي لأمن المعلومات(ISO/IEC 27002).

- **تحليل جميع فقرات معايير أمن المعلومات(ISO- LEC 27002)**

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (19.4).

جدول (19.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لجميع فقرات " معايير أمن المعلومات(ISO– LEC 27002) "

المجال	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
تقييم المخاطر ومعالجتها	3.65	0.84	73.02	2	كبيرة	14.07	0.000
السياسات الأمنية	3.41	0.80	68.11	12	كبيرة	9.31	0.000
تنظيم أمن المعلومات	3.54	0.79	70.82	6	كبيرة	12.46	0.000
إدارة الأصول	3.50	0.83	70.03	8	كبيرة	11.02	0.000
أمن الموارد البشرية	3.48	0.80	69.68	10	كبيرة	11.07	0.000
الأمن المادي والبيئي	3.50	0.78	70.03	8	كبيرة	11.71	0.000
إدارة العمليات/ الاتصالات وحمايتها	3.56	0.84	71.17	3	كبيرة	12.16	0.000
التحكم في الوصول	3.71	0.85	74.22	1	كبيرة	15.34	0.000
حيازة وتطوير وصيانة أنظمة المعلومات	3.56	0.78	71.12	4	كبيرة	12.95	0.000
إدارة حوادث أمن المعلومات	3.51	0.77	70.27	7	كبيرة	12.13	0.000
إدارة استمرار العمل	3.55	0.78	70.98	5	كبيرة	12.90	0.000
الامتثال والتوافق.	3.48	0.82	69.61	11	كبيرة	10.72	0.000
جميع فقرات " معايير أمن المعلومات(ISO-LEC 27002) "	**3.54**	**0.71**	**70.75**		**كبيرة**	**13.89**	**0.000**

من جدول (19.4) تبين أن المتوسط الحسابي لجميع فقرات معايير أمن المعلومات (ISO- LEC 27002) يساوي (3.54) (الدرجة الكلية من 5) أي أن الوزن النسبي (70.75%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات معايير أمن المعلومات(ISO- LEC 27002) بشكل عام. وهذه النتيجة توضح مدى حاجة الجامعات إلى الحفاظ على أمن معلوماتها وذلك من خلال ممارسة معايير أمن المعلومات بصورة كبيرة، حيث توصلت النتائج في الجدول أعلاه إلى أن الجامعات الفلسطينية تمارس معايير أمن المعلومات (ISO- LEC 27002) جميعها بصورة كبيرة.

ويعزو الباحث ذلك إلى أهمية وخطورة المعلومات بالنسبة للجامعات الفلسطينية، حيث تمثل المعلومات العصب الرئيسي للعمل وأي تأثير أو تهديد قد يطال المعلومات وأمنها، يمثل تهديداً خطيراً لعمل الجامعات واستمراريته، ولهذا نجد أن الجامعات قد اهتمت بتطبيق معايير أمن المعلومات والالتزام بها بصورة كبيرة.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (العميري وآخرون، 2017) التي توصلت إلى توافق أغلب ممارسات أمن المعلومات في المكتبة الرئيسة مع ممارسات المعيار الدولي لأمن المعلومات(ISO/IEC 27002)، وكذلك دراسة (المصري والأغا، 2018) التي توصلت إلى أن المتوسط الحسابي النسبي لجميع فقرات ممارسة معيار أمن المعلومات (ISO/IEC 27002) يساوي (84.37%).

بينما اختلفت هذه النتيجة مع دراسة (العربي، 2015) التي توصلت إلى أن جامعات الدراسة حرصت على تطبيق معايير فرعية في (11) معياراً أساسياً بنسبة 28.2% من إجمالي معايير آيزو 27002.

كما اختلفت هذه النتيجة مع دراسة (الدنف، 2013) التي توصلت إلى أن الإدارات العليا للكليات التقنية تدرك أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة.

ثانيا: تحليل فقرات مجال " جودة الخدمات المقدمة "

تم استخدام المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لمعرفة درجة الموافقة، النتائج موضحة في جدول (20.4).

جدول (20.4): المتوسط الحسابي، والإنحراف المعياري، والوزن النسبي، والترتيب، وقيمة اختبار(t) لكل فقرة من فقرات مجال " جودة الخدمات المقدمة "

م	الفقرة	المتوسط الحسابي	الإنحراف المعياري	الوزن النسبي	الترتيب	درجة الموافقة	قيمة الاختبار	القيمة الاحتمالية
1.	تتوفر خدمة الموقع الإلكتروني للجامعة بشكل دائم دون أي انقطاع	3.95	0.92	78.92	1	كبيرة	18.70	0.000
2.	يتمتع الموقع الإلكتروني للجامعة بواجهة تفاعلية ذات جاذبية للمستخدمين	3.52	1.01	70.36	10	كبيرة	9.31	0.000
3.	يتوفر لدى الطالب نوع من خصوصية البيانات	3.54	1.03	70.84	8	كبيرة	9.60	0.000
4.	يستطيع الطالب التوصل للحل الأمثل لما يطلبه عبر الخدمات الإلكترونية المقدمة من قبل الجامعة	3.46	0.98	69.13	15	كبيرة	8.48	0.000
5.	يمكن للطالب التبليغ عن المشاكل وحلها دون الحاجة إلى الذهاب إلى الجامعة	3.42	1.02	68.43	19	كبيرة	7.55	0.000
6.	توفر الخدمات الإلكترونية المقدمة للطلبة الوقت والجهد في كثير من الأحيان	3.47	1.05	69.49	11	كبيرة	8.23	0.000
7.	يوجد سرعة في الاستجابة في تقديم الخدمة للطلاب	3.44	1.00	68.89	16	كبيرة	8.08	0.000

.8	يوجد سهولة في استرجاع كلمة السر في حالة فقدانها من قبل الطالب	3.46	0.98	69.19	14	كبيرة	8.58	0.000
.9	يوجد سهولة في عملية إجراء القبول والتسجيل عبر الموقع الإلكتروني	3.64	1.00	72.73	2	كبيرة	11.61	0.000
10	من الصعب أن يتمكن أحد غير الطالب من الدخول إلى حسابه	3.56	1.01	71.29	4	كبيرة	10.15	0.000
11	يستطيع الطالب التعامل بسهولة مع الخدمات التي يقدمها موقع الجامعة	3.56	1.00	71.27	5	كبيرة	10.25	0.000
12	يستطيع الطالب إنجاز كافة المعاملات الخاصة به من خلال موقع الجامعة الإلكتروني	3.42	0.98	68.35	20	كبيرة	7.75	0.000
13	تقوم الجامعة بتحديث الخدمات الإلكترونية بشكل مستمر	3.44	1.03	68.89	16	كبيرة	7.90	0.000
14	يتحمل موقع الجامعة الإلكتروني الضغط الشديد في أوقات تسجيل المواد وظهور العلامات الفصلية	3.44	0.97	68.76	18	كبيرة	8.18	0.000
15	الخدمات الإلكترونية التي تقدمها الجامعة تضاهي المؤسسات الأخرى	3.55	0.97	70.99	7	كبيرة	10.34	0.000
16	يحصل الطالب على المعلومات بسرعة فائقة	3.47	0.99	69.37	13	كبيرة	8.64	0.000

17	تتـوفر جميـع المعلومـات التـي تخـص الطالـب علـى بوابته الالكترونية	3.54	1.02	70.72	9	كبيرة	9.57	0.000
18	يستطيع الطالب تغير اسم المسـتخدم وكلمـة المـرور علـى بوابتـه الالكترونيـة بسهولة	3.57	0.99	71.47	3	كبيرة	10.54	0.000
19	يثق الطـلاب بـأمن وحمايـة المعلومـات التـي توفرهـا الجامعة	3.56	1.03	71.23	6	كبيرة	9.95	0.000
20	يحصـل الطالـب علـى المعلومـات التـي يحتاجهـا بدقة فائقة	3.47	1.05	69.43	12	كبيرة	8.16	0.000
	جميع فقرات المجال معاً	3.52	0.75	70.49		كبيرة	12.83	0.000

من جدول (20.4) تبين أن المتوسط الحسابي للمجال بشكل عام يساوي (3.52) أي أن الوزن النسبي (70.49%)، وهذا يعني أن هناك موافقة بدرجة كبيرة من قبل أفراد العينة على فقرات هذا المجال.

وقد حصلت الفقرة " تتوفر خدمة الموقع الإلكتروني للجامعة بشكل دائم دون أي انقطاع " على أعلى درجة موافقة بنسبة (78.92%)، بينما حصلت الفقرة " يستطيع الطالب إنجاز كافة المعاملات الخاصة به من خلال موقع الجامعة الإلكتروني " على أقل درجة موافقة بنسبة (68.35%).

وتمثل هذه النتيجة دليلاً واضحاً على أن جودة الخدمات المقدمة من قبل الجامعة أصبحت تمثل هدفاً شديد الأهمية للجامعات والمستفيدين منها على حد سواء، حيث أن قطاع الجامعات أصبح اليوم يشهد منافسة كبيرة في ظل وجود عدد كبير من الجامعات وفي ظل محدودية عدد الطلاب ومحدودية الموارد المالية المتوفرة لدى الطلاب.

ويعزو الباحث ذلك أنَّ المنافسة الشديدة التي تشهدها الجامعات الفلسطينية أجبرتها على أن تهتم بجودة الخدمات التي تقدمها، حيث أصبحت الخيارات كثيرة بالنسبة للطلاب وأصبح الطالب يفاضل بين الجامعات على عدة أسس ومعايير يأتي على رأس هذه الأسس والمعايير مدى جودة الخدمات التي تقدمها الجامعة، ثم تأتي بعض المعايير الأخرى مثل التكلفة والوقت والجهد.

كذلك يعزو الباحث ذلك لوجود هيئة الجودة والمواصفات الفلسطينية والتي لها دور مهم في مدى تطبيق الجامعات الفلسطينية لمعايير الجودة بما ينعكس على جودة الخدمات المقدمة للطلبة.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (زقاي، 2017) التي توصلت إلى أن درجة تقدير الطلبة لأبعاد جودة الخدمات التعليمية المقدمة في الجامعة جاء بدرجة متوسطة، حيث حصل على درجة كلية بلغت (57.4%). وكذلك دراسة (السعافين، 2015) التي توصلت إلى أن مستوى جودة الخدمات الطلابية في الجامعات الفلسطينية متوسطاً، حيث كان الوزن النسبي للأبعاد الخمسة هو (53.84%).

بينما اختلفت هذه النتيجة مع دراسة (سلمان، 2012) التي توصلت إلى أن جودة الخدمات الجامعية كما يدركها طلبة جامعة الأقصى بين الضعيف والمتوسط في معظم أبعاد المقياس، وكذلك دراسة (Napitupulu, 2018) التي توصلت إلى وجود فجوة بين الإدراك وتوقعات المستجيبين الذين لديهم قيمة سلبية لكل عنصر. وهذا يعني أن مرافق الخدمات في الجامعة لا تلبي في الوقت الحالي توقعات الطلاب.

5.4 اختبار فرضيات الدراسة

الفرضية الرئيسة الأولى: توجد علاقة ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين أبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.

لاختبار هذه الفرضية تم استخدام اختبار "معامل بيرسون للارتباط"، والجدول الآتي يوضح ذلك.

جدول (21.4): معامل الارتباط بين أبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة

الفرضية	معامل بيرسون للارتباط	القيمة الاحتمالية(Sig.)
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تقييم المخاطر ومعالجتها في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.691*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين السياسات الأمنية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.643*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تنظيم أمن المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.695*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين إدارة الأصول في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.769*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين أمن الموارد البشرية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.733*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين الأمن المادي والبيئي في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.792*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين إدارة العمليات/ الاتصالات وحمايتها في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.775*	0.000

توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين التحكم في الوصول في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.755*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين حيازة وتطوير وصيانة أنظمة المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.816*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين إدارة حوادث أمن المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.744*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين إدارة استمرار العمل في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.795*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين الامتثال والتوافق في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	.774*	0.000
توجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين أبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.	**.855***	**0.000**

*الارتباط دال إحصائياً عند مستوى دلالة$\alpha \geq 0.05$).

يبين جدول (21.4) أن معامل الارتباط يساوي (0.855)، وأن القيمة الاحتمالية (Sig.) تساوي (0.000) وهي أقل من مستوى الدلالة (0.05) وهذا يدل على وجود علاقة ذات دلالة إحصائية بين أبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.

ويعزو الباحث ذلك إلى الممارسة العملية لأنظمة إدارة أمن المعلومات يضمن وجود أساس قوي للحفاظ على هذه المعلومات من الانتهاك والاختراق والتلاعب بها، وبالتالي؛ فإنَّ معلومات الجامعة وطلابها وموظفيها أصبحت في أمان وهذا الأمر يساعد على ضمان استمرارية العمل بشكل سليم وبدون أي خلل، ومن ثم فإن هذا الأمر ينعكس على جودة الخدمات التي تقدمها الجامعة ككل.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) التي توصلت إلى فاعلية اجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع، والاكتشاف، والتصحيح) من خلال اختبار ثلاثة أنواع من المخاطر التي

تهدد أمن المعلومات الالكترونية وهي مخاطر اختراق الشبكات والهندسة الاجتماعية والبرمجيات الضارة.

الفرضية الرئيسة الثانية: يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) لأبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية على جودة الخدمات المقدمة للطلبة.

لاختبار هذه الفرضية تم استخدام الانحدار الخطي المتعدد والجدول الآتي يوضح ذلك:

جدول (22.4): تحليل الانحدار المتعدد

المتغيرات المستقلة	معاملات الانحدار	قيمة اختبار T	القيمة الاحتمالية .Sig
المقدار الثابت	0.351	3.353	0.000
تقييم المخاطر ومعالجتها.	0.036	0.761	0.224
السياسات الأمنية.	-0.096	-1.872	0.031
تنظيم أمن المعلومات.	-0.056	-0.988	0.162
إدارة الأصول.	0.135	2.376	0.009
أمن الموارد البشرية.	0.051	1.019	0.155
الأمن المادي والبيئي.	0.102	1.793	0.037
إدارة العمليات/ الاتصالات وحمايتها.	0.107	2.206	0.014
التحكم في الوصول.	0.096	2.052	0.020
حيازة وتطوير وصيانة أنظمة المعلومات.	0.172	2.898	0.002
إدارة حوادث أمن المعلومات.	0.075	1.517	0.065
إدارة استمرار العمل.	0.162	2.953	0.002
الامتثال والتوافق.	0.108	2.224	0.013
معامل الارتباط = 0.876		معامل التحديد المُعدَّل= 0.758	
قيمة الاختبار F = 87.343		القيمة الاحتمالية = 0.000	

من النتائج الموضحة في جدول (22.4) يمكن استنتاج ما يلي:

- معامل الارتباط = (0.876)، ومعامل التحديد المُعدَّل= (0.758) وهذا يعني أن (75.8%) من التغير في جودة الخدمات المقدمة للطلبة تم تفسيره من خلال العلاقة الخطية، والنسبة المتبقية قد ترجع إلى عوامل أخرى تؤثر في جودة الخدمات المقدمة للطلبة.
- قيمة الاختبار (F) المحسوبة بلغت (87.343)، كما أن القيمة الاحتمالية تساوي (0.000) مما يعني رفض الفرضية الصفرية والقبول بوجود علاقة ذات دلالة إحصائية بين أبعاد قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة.

تبين أن المتغيرات المستقلة المؤثرة في " جودة الخدمات المقدمة للطلبة " هي: السياسات الأمنية، إدارة الأصول، الأمن المادي والبيئي، إدارة العمليات/ الاتصالات وحمايتها، التحكم في الوصول، حيازة وتطوير وصيانة أنظمة المعلومات، إدارة استمرار العمل، الامتثال والتوافق، بينما تبين ضعف تأثير باقي المتغيرات " تقييم المخاطر ومعالجتها، تنظيم أمن المعلومات، أمن الموارد البشرية، إدارة حوادث أمن المعلومات".

وتتفق هذه النتيجة مع النتيجة السابقة حيث أن وجود ما يضمن أمن المعلومات واستقرارها ومنع أي انتهاك أو تلاعب فيها، سوف يؤدي بشكل حتمي إلى زيادة جودة الأعمال واستمراريتها، وبالتالي فإن جودة الخدمات التي تقدمها الجامعات الفلسطينية مرتبطة بشكل وثيق بالمعلومات وأمنها وكل ما يؤثر على أمن المعلومات سوف يؤثر على جودة الخدمات التي تقدمها الجامعات الفلسطينية.

ويعزو الباحث ذلك أنَّ جودة الخدمات التي تقدمها الجامعات هي عبارة عن المنتج النهائي الذي يمر عبر سلسلة من المراحل والعمليات التي تعتمد كل واحدة منها على الأخرى ويعتبر أمن المعلومات أحد أهم هذه المراحل، ومن ثم فإن أي عامل يمكن أن يؤثر على أمن المعلومات بشكل إيجابي فإنه بشكل تلقائي يؤثر على جودة الخدمات المقدمة.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) التي توصلت إلى فاعلية اجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية من خلال أوجهها الثلاثة (المنع والاكتشاف والتصحيح) من خلال اختبار ثلاثة أنواع من المخاطر التي تهدد أمن المعلومات الالكترونية وهي مخاطر اختراق الشبكات والهندسة الاجتماعية والبرمجيات الضارة.

الفرضية الرئيسة الثالثة: توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى للمعلومات العامة "النوع، الجامعة، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة".

ويشتق من هذه الفرضية الرئيسة الفرضيات الفرعية الآتية:

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى النوع.**

لاختبار هذه الفرضية تم استخدام اختبار " T – لعينتين مستقلتين "، والجدول الآتي يوضح ذلك.

جدول (23.4): نتائج اختبار" T – لعينتين مستقلتين " – النوع

المجال	المتوسطات		قيمة الاختبار	القيمة الاحتمالية (Sig.)
	ذكر	أنثى		
تقييم المخاطر ومعالجتها	3.68	3.45	1.543	0.124
السياسات الأمنية	3.43	3.25	1.306	0.193
تنظيم أمن المعلومات	3.55	3.47	0.598	0.550
إدارة الأصول	3.52	3.35	1.216	0.225
أمن الموارد البشرية	3.51	3.27	1.776	0.077
الأمن المادي والبيئي	3.52	3.39	0.970	0.333
إدارة العمليات/ الاتصالات وحمايتها	3.56	3.56	0.005	0.996
التحكم في الوصول	3.71	3.69	0.167	0.867
حيازة وتطوير وصيانة أنظمة المعلومات	3.57	3.48	0.642	0.522
إدارة حوادث أمن المعلومات	3.53	3.37	1.187	0.236
إدارة استمرار العمل	3.56	3.46	0.724	0.469
الامتثال والتوافق	3.49	3.42	0.478	0.633
معايير أمن المعلومات (ISO- LEC 27002)	3.55	3.43	1.007	0.315

من النتائج الموضحة في جدول (23.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" T – لعينتين مستقلتين " أكبر من مستوى الدلالة (0.05) وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى النوع.

وهذا يوضح بأن القناعات الموجودة لدى الذكور والإناث حول معايير أمن المعلومات هي قناعات وأفكار مشتركة لا خلاف عليها.

ويعزو الباحث ذلك أنَّ المعايير المرتبطة بأمن المعلومات هي من البديهيات والمسلمات التي لا نقاش ولا جدال فيها، وبالتالي هناك اتفاق في وجهات النظر حولها سواء من الذكور أو الإناث.

واختلفت هذه النتائج مع بعض الدراسات كدراسة (الدنف، 2013) التي توصلت إلى وجود فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات بقطاع غزة

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى الجامعة.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (24.4): نتائج اختبار" التباين الأحادي " – الجامعة

المجال	المتوسطات				قيمة الاختبار	القيمة الاحتمالية (.Sig)
	الأقصى	الأزهر	الاسلامية	فلسطين		
تقييم المخاطر ومعالجتها.	3.50	3.55	3.97	3.48	*7.550	0.000
السياسات الأمنية.	3.34	3.36	3.58	3.23	2.612	0.051
تنظيم أمن المعلومات.	3.49	3.43	3.78	3.32	*4.875	0.002
إدارة الأصول.	3.45	3.39	3.72	3.30	*3.845	0.010
أمن الموارد البشرية.	3.40	3.37	3.74	3.29	*5.417	0.001
الأمن المادي والبيئي.	3.48	3.39	3.67	3.35	*2.759	0.042
إدارة العمليات/ الاتصالات وحمايتها.	3.54	3.45	3.71	3.44	1.765	0.154
التحكم في الوصول.	3.69	3.51	3.99	3.47	*6.397	0.000
حيـــازة وتطـــوير وصـــيانة أنظمـــة	3.50	3.48	3.76	3.37	*3.506	0.016

إدارة حوادث أمن المعلومات.	3.46	3.43	3.70	3.37	*2.879	0.036
إدارة استمرار العمل.	3.53	3.39	3.73	3.44	*3.296	0.021
الامتثال والتوافق.	3.46	3.36	3.67	3.29	*3.158	0.025
معايير أمن المعلومات(ISO- LEC 27002).	3.49	3.43	3.75	3.36	*4.879	0.002

من النتائج الموضحة في جدول (24.4) يمكن استنتاج ما يلي:

تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أكبر من مستوى الدلالة (0.05) للمجالين " السياسات الأمنية، إدارة العمليات/ الاتصالات وحمايتها "، وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة حول هذين المجالين تُعزى إلى الجامعة. وهذا يوضح بأن هناك اتفاق من قبل عينة الدراسة حول السياسات الأمنية وإدارة العمليات والاتصالات وحمايتها كأهم المعايير الأمنية التي يجب الالتزام بها.

أما بالنسبة لباقي المجالات والمجالات مجتمعة معا فقد تبين أن القيمة الاحتمالية (.Sig) أقل من مستوى الدلالة (0.05) وبذلك يمكن استنتاج أنه توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة حول هذه المجالات والمجالات مجتمعة معا تُعزى إلى الجامعة، وذلك لصالح الذين يعملون في الجامعة الإسلامية.

وعلى الرغم من وجود اتفاق من قبل أفراد عينة الدراسة حول أهمية المعايير الأمنية الخاصة بأمن المعلومات، إلا أن هناك اهتماماً أكبر من قبل أفراد عينة الدراسة في الجامعة الإسلامية في بعض المجالات مثل التحكم في الوصول، وكذلك إدارة حوادث أمن المعلومات ... الخ.

ويعزو الباحث ذلك أنَّ الجامعة الإسلامية بغزة هي أقدم جامعة موجودة في قطاع غزة مقارنة بالجامعات الأخرى، وهذا بدوره قد أثر بشكل كبير على حجم الخبرات التي تحتفظ بها الجامعة الإسلامية في أمن المعلومات والأمور المتعلقة بها، حيث أن عامل الزمن يعتبر من العوامل المهمة في زيادة حجم الخبرات لدى الجامعة حول المعلومات وأمنها.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) حيث أظهرت النتائج فروق ذات دلالة إحصائية بين إجابات أفراد العينة تعود للخلفية الشخصية لكل منهم خاصة في مجالات طبيعة الدور الوظيفي وسنوات الخبرة وحيازة شهادات مهنية وحجم الشركة وكونها أجنبية أو محلية.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى المؤهل العلمي.**

لاختبار هذه الفرضية تم استخدام اختبار " T – لعينتين مستقلتين "، والجدول الآتي يوضح ذلك.

جدول (25.4): نتائج اختبار" T – لعينتين مستقلتين " – المؤهل العلمي

المجال	المتوسطات		قيمة الاختبار	القيمة الاحتمالية (Sig.)
	بكالوريوس فأقل	دراسات عليا		
تقييم المخاطر ومعالجتها	3.69	3.63	0.659	0.511
السياسات الأمنية	3.42	3.40	0.171	0.864
تنظيم أمن المعلومات	3.53	3.55	-0.275	0.783
إدارة الأصول	3.56	3.47	0.973	0.331
أمن الموارد البشرية	3.57	3.43	1.491	0.137
الأمن المادي والبيئي	3.58	3.45	1.473	0.142
إدارة العمليات/ الاتصالات وحمايتها	3.65	3.51	1.452	0.148
التحكم في الوصول	3.71	3.71	-0.076	0.940
حيازة وتطوير وصيانة أنظمة المعلومات	3.62	3.52	1.166	0.244
إدارة حوادث أمن المعلومات	3.56	3.49	0.770	0.442
إدارة استمرار العمل	3.60	3.52	0.923	0.357
الامتثال والتوافق	3.50	3.47	0.371	0.711
معايير أمن المعلومات (ISO- LEC 27002)	3.58	3.51	0.876	0.382

من النتائج الموضحة في جدول (25.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" T – لعينتين مستقلتين " أكبر من مستوى الدلالة (0.05) وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى المؤهل العلمي.

وهذا يوضح بأن هناك اتفاقاً من قبل أفراد عينة الدراسة حول معايير أمن المعلومات وأهميتها وأهمية الالتزام بها في الجامعات الفلسطينية.

ويعزو الباحث ذلك إلى التأهيل العلمي لأفراد عينة الدراسة يضمن أنهم قد مروا في أثناء دراستهم على موضوع المعلومات وأمنها وما يرتبط بها من تهديدات ومخاطر، ولهذا نجد أن التأهيل العلمي يساعد على جمع وجهات النظر حول أهمية معايير أمن المعلومات وأهمية الالتزام بها.

واختلفت هذه النتائج مع بعض الدراسات كدراسة (الدنف، 2013) التي توصلت إلى وجود فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات بقطاع غزة.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى المسمى الوظيفي.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (26.4): نتائج اختبار" التباين الأحادي " – المسمى الوظيفي

المجال	المتوسطات			قيمة الاختبار	القيمة الاحتمالية (Sig.)
	إدارة عليا	إدارة وسطى	دائرة التكنولوجيا وشبكة المعلومات		
تقييم المخاطر ومعالجتها	3.42	3.75	3.52	*4.535	0.011
السياسات الأمنية	3.31	3.44	3.37	0.808	0.447
تنظيم أمن المعلومات	3.46	3.61	3.33	2.874	0.058
إدارة الأصول	3.42	3.53	3.49	0.451	0.637
أمن الموارد البشرية	3.39	3.51	3.47	0.648	0.524
الأمن المادي والبيئي	3.40	3.53	3.54	0.752	0.472
إدارة العمليات/ الاتصالات وحمايتها	3.47	3.57	3.63	0.543	0.581
التحكم في الوصول	3.69	3.78	3.42	*3.462	0.033
حيازة وتطوير وصيانة أنظمة المعلومات	3.49	3.58	3.55	0.335	0.715

إدارة حوادث أمن المعلومات	3.40	3.53	3.57	0.938	0.393
إدارة استمرار العمل	3.46	3.57	3.59	0.588	0.556
الامتثال والتوافق	3.46	3.51	3.35	0.755	0.471
معايير أمن المعلومات (ISO- LEC 27002)	3.45	3.58	3.49	1.002	0.368

من النتائج الموضحة في جدول (26.4) يمكن استنتاج ما يلي:

تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أقل من مستوى الدلالة (0.05) للمجالين " تقييم المخاطر ومعالجتها، والتحكم في الوصول "، وبذلك يمكن استنتاج أنه توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة حول هذه المجالات تُعزى إلى المسمى الوظيفي، وذلك لصالح الذين مسماهم الوظيفي إدارة وسطى.

وتوضح هذه النتيجة إلى أن الإدارة الوسطى لديها اهتمام بشكل أكبر من باقي الإدارة في عملية تقييم المخاطر ومعالجتها حيث أن عملية تقييم المخاطر ومعالجتها تقع على عاتق الإدارة الوسطى بشكل أساسي، فهي الإدارة التي تصل بين من قاموا بارتكاب الأخطاء المرتبطة بمخاطر أمن المعلومات (الإدارة الدنيا) وبين من يقوموا باتخاذ القرارات في سبيل معالجة هذه المخاطر والتخلص منها (الإدارة العليا).

أما بالنسبة لباقي المجالات والمجالات مجتمعة معا؛ فقد تبين أن القيمة الاحتمالية (.Sig) أكبر من مستوى الدلالة (0.05) وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة حول هذه المجالات والمجالات مجتمعة معا تُعزى إلى المسمى الوظيفي.

وتوضح هذه النتيجة إلى هناك اتفاقاً من قبل المسميات الوظيفية المختلفة حول أهمية تقييم المخاطر ومعالجتها، والتحكم في الوصول إلى المعلومات، وهذا يوضح مدى أهمية هذه المعايير المرتبطة بأمن المعلومات وخصوصا عملية التحكم في الوصول.

ويعزو الباحث ذلك إلى جميع الإدارات تبدي اهتماماً كبيراً في الحفاظ على أمن المعلومات، وأنَّ انتهاك للمعلومات وأمنها سوف يضر بالمؤسسة ككل وليست إدارة أو جزء من المؤسسة.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (عبد الجابر، 2013) التي أظهرت النتائج فروق ذات دلالة إحصائية بين إجابات أفراد العينة تعود للخلفية الشخصية لكل منهم لاسيما في مجالات طبيعة الدور الوظيفي وسنوات الخبرة وحيازة شهادات مهنية وحجم الشركة وكونها أجنبية أو محلية.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى سنوات الخبرة.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (27.4): نتائج اختبار" التباين الأحادي " – سنوات الخبرة

المجال	المتوسطات			قيمة الاختبار	القيمة الاحتمالية (Sig.)
	أقل من 10 سنوات	10- 15	أكثر من 15 سنة		
تقييم المخاطر ومعالجتها.	3.62	3.76	3.56	1.622	0.199
السياسات الأمنية.	3.32	3.47	3.42	0.987	0.374
تنظيم أمن المعلومات.	3.47	3.56	3.60	0.788	0.456
إدارة الأصول.	3.41	3.55	3.54	0.912	0.403
أمن الموارد البشرية.	3.45	3.49	3.51	0.188	0.829
الأمن المادي والبيئي.	3.51	3.48	3.52	0.093	0.911
إدارة العمليات/ الاتصالات وحمايتها.	3.57	3.54	3.57	0.066	0.936
التحكم في الوصول.	3.64	3.71	3.79	0.813	0.444
حيازة وتطوير وصيانة أنظمة المعلومات.	3.50	3.58	3.58	0.395	0.674
إدارة حوادث أمن المعلومات.	3.49	3.55	3.50	0.187	0.830
إدارة استمرار العمل.	3.58	3.53	3.53	0.143	0.867
الامتثال والتوافق.	3.40	3.53	3.50	0.784	0.457
معايير أمن المعلومات(ISO- LEC 27002).	3.50	3.56	3.55	0.260	0.771

من النتائج الموضحة في جدول (27.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أكبر من مستوى الدلالة 0.05، وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى سنوات الخبرة.

وهذا يوضح بأن أمن المعلومات يعد هدفاً أساسياً للأفراد والمؤسسات بشكل عام، حيث أن الموظف سواء كانت خبرته كبيرة أو خبرته قليلة فإن أمن المعلومات يمثل له أمراً بالغ الأهمية والخطورة.
ويعزو الباحث ذلك إلى أمن المعلومات يُعدُّ عصباً أساسياً للقيام بالأعمال على أكمل وجه، وأن أي انتهاك لأمن المعلومات قد يمثل خطراً كبيراً حول استمرارية الأعمال والنتائج النهائية لها.
واختلفت هذه النتائج مع بعض الدراسات كدراسة (الدنف، 2013) التي توصلت إلى وجود فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة.

الفرضية الرئيسة الرابعة: توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى للمعلومات العامة "النوع، الجامعة، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة".

ويشتق من هذه الفرضية الرئيسة الفرضيات الفرعية الآتية:

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى إلى الجنس.**

لاختبار هذه الفرضية تم استخدام اختبار " T – لعينتين مستقلتين "، والجدول الآتي يوضح ذلك.

جدول (28.4): نتائج اختبار" T – لعينتين مستقلتين " – الجنس

	المتوسطات		قيمة الاختبار	القيمة الاحتمالية (Sig.)
	ذكر	أنثى		
مستوى جودة الخدمات المقدمة للطلبة	3.54	3.38	1.278	0.202

من النتائج الموضحة في جدول (28.4) تبين أن القيمة الاحتمالية (Sig.) المقابلة لاختبار" T – لعينتين مستقلتين " أكبر من مستوى الدلالة 0.05، وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى الجنس.
وهذا يوضح أن هناك انطباع مشترك من قبل الطلبة حول جودة الخدمات التي تقدمها الجامعات حيث أن الطلاب على اختلاف جنسهم يتم معاملتهم نفس المعاملة في الجامعة ولا يوجد محاباة لجنس على آخر.

ويعزو الباحث ذلك أنَّ الجامعات تهتم بجودة الخدمات التي تقدمها للطلاب على اختلاف جنسهم، وذلك للحصول على أكبر قدر ممكن من الطلاب في ظل المنافسة الشديدة التي تواجهها الجامعات الفلسطينية في عملية الحصول على الطلاب للدراسة فيها.

واتفقت هذه النتائج مع بعض الدراسات كدراسة (السعافين، 2015) التي توصلت إلى عدم وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات أفراد عينة الطلبة لمستوى جودة الخدمات الطلابية في الجامعات الفلسطينية في محافظات غزة تُعزى لمتغير الجنس.

واختلفت هذه النتيجة مع دراسة (سلمان، 2012) التي توصلت إلى وجود فروق ذات دلالة إحصائية تُعزى لمتغير الجنس بين الذكور والإناث ولصالح الإناث في مستوى جودة الخدمات الجامعية المدركة في جميع الأبعاد ما عدا بعد (الأمان).

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى إلى الجامعة.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (29.4): نتائج اختبار" التباين الأحادي " – الجامعة

	المتوسطات				قيمة الاختبار	القيمة الاحتمالية (Sig.)
	الأقصى	الأزهر	الاسلامية	فلسطين		
مستوى جودة الخدمات المقدمة للطلبة	3.45	3.38	3.73	3.49	*3.843	0.010

* الفرق بين المتوسطات دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$).

من النتائج الموضحة في جدول (29.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أقل من مستوى الدلالة 0.05، وبذلك يمكن استنتاج أنه توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة حول هذه المجالات تُعزى إلى الجامعة.

وهذا يوضح بأن الخدمات التي تقدمها الجامعات الفلسطينية متقاربة ومتساوية في غالب الأحيان.

ويعزو الباحث ذلك إلى المنافسة الشديدة التي تواجهها الجامعات الفلسطينية في عملية الحصول على الطلاب للتسجيل فيها قد أجبرتها على تقديم أفضل ما لديها لتحصل على حصتها من عدد الطلاب الخريجين من الثانوية العامة.

وقد اختلفت هذه النتيجة مع دراسة (السعافين، 2015) التي توصلت إلى وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات أفراد العينة لمستوى جودة الخدمات الطلابية في الجامعات الفلسطينية تُعزى لمتغير الجامعة، وذلك لصالح الجامعة الإسلامية، ثم جامعة الأزهر، ثم جامعة الأقصى.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى إلى المؤهل العلمي.**

لاختبار هذه الفرضية تم استخدام اختبار " T – لعينتين مستقلتين "، والجدول الآتي يوضح ذلك.

جدول (30.4): نتائج اختبار" T – لعينتين مستقلتين " – المؤهل العلمي

	المتوسطات		قيمة الاختبار	القيمة الاحتمالية (Sig.)
	بكالوريوس فأقل	دراسات عليا		
مستوى جودة الخدمات المقدمة للطلبة	3.59	3.48	1.305	0.193

من النتائج الموضحة في جدول (30.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" T – لعينتين مستقلتين " أكبر من مستوى الدلالة (0.05) وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى المؤهل العلمي.

وهذا يوضح أن هناك اتفاقاً من قبل الطلاب على جودة الخدمات التي تقدمها الجامعات الفلسطينية على اختلاف تخصصاتهم.

ويعزو الباحث ذلك أنَّ الجامعات الفلسطينية هي جامعات صغيرة الحجم نسبياً وبالتالي فإن جميع التخصصات غالباً ما تكون في نفس المكان ويحصلون على نفس الخدمات المقدمة، وبالتالي نجد أن هناك اتفاقاً منهم حول جودة هذه الخدمات.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى إلى المسمى الوظيفي.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (31.4): نتائج اختبار" التباين الأحادي " – المسمى الوظيفي

	المتوسطات			قيمة الاختبار	القيمة الاحتمالية (.Sig)
	إدارة عليا	إدارة وسطى	دائرة التكنولوجيا وشبكة المعلومات		
مستوى جودة الخدمات المقدمة للطلبة.	3.45	3.52	3.66	1.139	0.321

من النتائج الموضحة في جدول (31.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أكبر من مستوى الدلالة 0.05، وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى المسمى الوظيفي.

وهذا يوضح أن هناك اتفاقاً من قبل عينة الدراسة على اختلاف مسمياتها الوظيفية حول جودة الخدمات المقدمة.

ويعزو الباحث ذلك إلى المسميات الوظيفية جميعها تحاول تقديم أفضل ما لديها للطلاب وبالتالي هناك قناعة لديهم بأن الخدمات المقدمة هي أفضل ما يمكن الوصول له في ظل الظروف التي تمر بها الجامعات الفلسطينية.

- **توجد فروق ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين متوسطات استجابات أفراد العينة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى إلى سنوات الخبرة.**

لاختبار هذه الفرضية تم استخدام اختبار " التباين الأحادي "، والجدول الآتي يوضح ذلك

جدول (32.4): نتائج اختبار" التباين الأحادي " – سنوات الخبرة

	المتوسطات			قيمة الاختبار	القيمة الاحتمالية (.Sig)
	أقل من 10 سنوات	10- 15	أكثر من 15 سنة		
مستوى جودة الخدمات المقدمة للطلبة.	3.46	3.58	3.53	0.657	0.519

من النتائج الموضحة في جدول (32.4) تبين أن القيمة الاحتمالية (.Sig) المقابلة لاختبار" التباين الأحادي " أكبر من مستوى الدلالة 0.05، وبذلك يمكن استنتاج أنه لا توجد فروق ذات دلالة إحصائية بين متوسطات تقديرات عينة الدراسة تُعزى إلى سنوات الخبرة.

وهذا يوضح بأن هناك اتفاقاً من قبل أفراد عينة الدراسة على اختلاف سنوات الخبرة لديهم حول جودة الخدمات التي تقدمها الجامعات الفلسطينية.

ويعزو الباحث ذلك أنَّ الموظفين الجدد والقدامى على اختلاف سنوات خبراتهم لديهم نفس القناعة تجاه الخدمات التي تقدمها الجامعات الفلسطينية للطلاب، وأنَّ الجامعات تحاول تقديم أفضل ما لديها في ضوء المنافسة الشديدة في قطاع التعليم العالي.

الفصل الخامس

ملخص النتائج والتوصيات

مقدمة:

يهدف هذا الفصل إلى استعراض أهم نتائج الدراسة واستنتاجاتها، وما خلص إليه الباحث بعد عملية تحليل البيانات، واختبار فرضيات الدراسة، والوقوف على علاقة تطبيق معايير أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية بجودة الخدمات المقدمة. بعد ذلك يقدم الباحث التوصيات المقترحة في ضوء نتائج الدراسة والاستنتاجات التي توصل إليها من خلال تلك النتائج لتحقيق غاية البحث، وينقسم هذا الفصل إلى ما يلي:

1.5 النتائج

وسيتم تقسيم النتائج إلى ما يلي:

1- النتائج المرتبطة بواقع تطبيق معايير أمن المعلومات وجودة الخدمات المقدمة:

- يتم تطبيق معايير أمن المعلومات (ISO-LEC..27002) في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.75%).
- يتم تطبيق معايير تقييم المخاطر في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (73.02%).

- يتم تطبيق معايير السياسات الأمنية في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (68.11%).
- يتم تطبيق معايير تنظيم أمن المعلومات في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.82%).
- يتم تطبيق معايير تنظيم إدارة الأصول في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.03%).
- يتم تطبيق معايير أمن الموارد البشرية في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (69.68%).
- يتم تطبيق معايير الأمن المادي والبيئي في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.03%).
- يتم تطبيق معايير إدارة العمليات/ الاتصالات وحمايتها في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (71.17%).
- يتم تطبيق معايير التحكم في الأصول في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (74.22%).
- يتم تطبيق معايير حيازة وتطوير وصيانة أنظمة المعلومات في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (71.12%).
- يتم تطبيق معايير إدارة حوادث أمن المعلومات في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.27%).
- يتم تطبيق معايير إدارة استمرار العمل في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (70.98%).
- يتم تطبيق معايير الامتثال والتوافق في الجامعات الفلسطينية بصورة كبيرة، وذلك بنسبة بلغت (69.61%).
- هناك موافقة كبيرة على جودة الخدمات المقدمة في الجامعات الفلسطينية وذلك بنسبة تأكيد بلغت (70.49) حسب استجابات عينة الدراسة.

2- النتائج المرتبطة بعلاقة تطبيق معايير أمن المعلومات بجودة الخدمات المقدمة:

- توجد علاقة طردية قوية ذات دلالة إحصائية بين تطبيق معايير أمن المعلومات (ISO-IEC..27002) في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.855).
- توجد علاقة ذات دلالة إحصائية بين تقييم المخاطر ومعالجتها في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.691).
- توجد علاقة ذات دلالة إحصائية بين السياسات الأمنية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.643).
- توجد علاقة ذات دلالة إحصائية بين تنظيم أمن المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.695).
- توجد علاقة ذات دلالة إحصائية بين إدارة الأصول في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.769).
- توجد علاقة ذات دلالة إحصائية بين أمن الموارد البشرية في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.733).
- توجد علاقة ذات دلالة إحصائية بين الأمن المادي والبيئي في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.792).
- توجد علاقة ذات دلالة إحصائية بين إدارة العمليات/ الاتصالات وحمايتها في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.775).

- توجد علاقة ذات دلالة إحصائية بين التحكم في الوصول في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.755).
- توجد علاقة ذات دلالة إحصائية بين حيازة وتطوير وصيانة أنظمة المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.816).
- توجد علاقة ذات دلالة إحصائية بين إدارة حوادث أمن المعلومات في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.744).
- توجد علاقة ذات دلالة إحصائية بين إدارة استمرار العمل في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.795).
- توجد علاقة ذات دلالة إحصائية بين الامتثال والتوافق في الجامعات الفلسطينية، وجودة الخدمات المقدمة للطلبة، وذلك بمعامل ارتباط يساوي (0.774).

3- النتائج المرتبطة بأثر تطبيق معايير أمن المعلومات على جودة الخدمات المقدمة:

- يوجد أثر ذو دلالة إحصائية لتطبيق معايير أمن المعلومات ممثلة بالمعايير (السياسات الأمنية، وإدارة الأصول، والأمن المادي والبيئي، وإدارة العمليات/ الاتصالات وحمايتها، والتحكم في الوصول، وحيازة وتطوير وصيانة أنظمة المعلومات، وإدارة استمرار العمل، والامتثال والتوافق) على جودة الخدمات المقدمة؛ حيث تفسر هذه المتغيرات (75.8%) من جودة الخدمات المقدمة.

4- النتائج المرتبطة بقياس الفروق بين استجابات عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات:

- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى لمتغير الجنس (ذكر، أنثى).
- توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC..27002) تُعزى لمتغير الجامعة لصالح الجامعة الإسلامية.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى لمتغير المؤهل العلمي.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى لمتغير المسمى الوظيفي.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات(ISO-IEC 27002) تُعزى لمتغير سنوات الخبرة.

5- النتائج المرتبطة بقياس الفروق بين استجابات عينة الدراسة حول مستوى قواعد الممارسة العملية لأنظمة إدارة أمن المعلومات:

- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى لمتغير الجنس (ذكر، أنثى).

- توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى لمتغير الجامعة لصالح الجامعة الإسلامية بغزة.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى لمتغير المؤهل العلمي.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى لمتغير المسمى الوظيفي.
- لا توجد فروق ذات دلالة إحصائية عند مستوى ($\alpha \leq 0.05$) بين متوسطات درجات تقدير أفراد عينة الدراسة حول مستوى جودة الخدمات المقدمة للطلبة تُعزى لمتغير سنوات الخبرة.

2.5 التوصيات

بناء على النتائج التي توصل لها الباحث، يمكن الخروج بالتوصيات الآتية:

1- ضرورة الاهتمام بمستوى تطبيق معايير أمن المعلومات في الجامعات الفلسطينية وذلك لعلاقتها وأثرها الواضح على جودة الخدمات التي تقدمها للطلبة.

2- العمل على تعزيز مستوى تطبيق معايير أمن المعلومات حيث تراوحت نسبة تطبيق معايير أمن المعلومات من (68.11% إلى 74.22%).

3- ضرورة الاهتمام بمستوى تطبيق المعايير التي كانت نسبتها متدنية مقارنة بباقي المعايير، مثل (معيار السياسات الأمنية، ومعيار الامتثال والتوافق، ومعيار أمن الموارد البشرية) حيث كانت نسبة تطبيقها أقل من (70%).

4- العمل على زيادة جودة الخدمات التي تقدمها الجامعات الفلسطينية إلى الطلاب وذلك حتى تكون عنصر جذب للطلاب إلى الجامعات الفلسطينية في ظل المنافسة الشديدة التي يشهدها قطاع التعليم العالي في ظل الظروف الاقتصادية الصعبة التي يمر بها طلاب القطاع.

5- العمل على زيادة الالتزام بحوكمة التعليم من خلال معايير التعليم الدولية.

6- العمل على توعية وتثقيف العاملين في الجامعات الفلسطينية حول أهمية أمن المعلومات والمعايير المرتبطة بأمن المعلومات، وذلك لتسهيل عملية تطبيق هذه المعايير في الجامعات الفلسطينية.

7- العمل على تطوير مجموعة من معايير أمن المعلومات الخاصة بالجامعات الفلسطينية والعربية، وتكون مرجعيتها في عملية التطوير معايير الآيزو (27001، 27002) وذلك حتى تتناسب هذه المعايير مع البيئة العربية والفلسطينية.

8- العمل على غرس ثقافة أمن المعلومات في جميع موظفي الجامعات الفلسطينية من أدناها لأعلاها؛ وذلك لتسهيل تطبيق معايير أمن المعلومات في الجامعات الفلسطينية.

9- ضرورة الاهتمام بالبنية التحتية لنظم المعلومات من أجهزة، وشبكات، وموارد بشرية، وتطوير هذه البنية بشكل مستمر يواكب التطورات الحادثة في المجال.

3.5 الدراسات المستقبلية

نظراً لأن هذه الدراسة قد ركزت على تطبيق معايير أمن المعلومات في الجامعات الفلسطينية، وربطتها بجودة الخدمات التي تقدمها هذه الجامعات؛ فكان لابُدَّ من إجراء دراسات أخرى في نفس المجال مثل:

- اجراء دراسة حول المعيقات والمشاكل التي تحول دون تطبيق معايير أمن المعلومات في الجامعات الفلسطينية.
- إجراء دراسة حول حوكمة الجامعات الفلسطينية لمعايير أمن المعلومات.
- وضع تصور مقترح لتحسين جودة أمن المعلومات في الجامعات الفلسطينية.
- اجراء دراسة حول كيفية استخدام التكنولوجيا في تطبيق معايير أمن المعلومات.
- اجراء دراسة حول مستوى تطبيق معايير أمن المعلومات في الجامعات الفلسطينية.

المصادر والمراجع

القرآن الكريم.

أولاً: المراجع باللغة العربية:

أ. الكتب

- الجرجاوي، ز (2010). القواعد المنهجية لبناء الاستبيان، الطبعة الثانية، مطبعة أبناء الجراح، فلسطين.
- الحمداني، م (2006): مناهج البحث العلمي، الأردن، عمان، مؤسسة الوراق للنشر.
- داوود، ح. (2004). أمن شبكة المعلومات. ط1، الرياض: معهد الإدارة العامة، مكتبة الملك فهد الوطنية.
- السالمي، ع. (2001). تقنيات المعلومات الإدارية. الطبعة الأولى، دار وائل للنشر، عمان، الأردن.
- السويل، م. (2007). المدخل إلى علم التشفير.
- شبلي، هـ.، مروان، م. (2009). إدارة المنشآت المعاصرة. دار الصفاء للنشر والتوزيع.
- الطائي، م. (2004). نظم المعلومات الإدارية المتقدمة. ط1، دار وائل للنشر والتوزيع، عمان، الأردن.
- عبيدات، ذ، عدس، ع، وعبد الحق، ك. (2001). البحث العلمي- مفهومه وأدواته وأساليبه، دار الفكر للنشر والتوزيع، عمان.
- القحطاني، ذ. (2015). أمن المعلومات. مدونة الملك عبد العزيز للعلوم والتقنية، فهرسة مكتبة الملك فهد الوطنية أثناء النشر.

ب. المجلات المنشورة والمؤتمرات العلمية:

- الأبروي، م. (2010). ما المقصود بأمن المعلومات أمن الانترنت. مجلة رسالة التربية، (27)، 126-130.
- البكري، ي. (2017). أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلى مكتبتي جامعة النيلين وجامعة وادي النيل. ورقة مقدمة للمؤتمر (23) لجمعية المكتبات المتخصصة بعنوان:

جودة برامج التدريب والتأهيل في المكتبات والمعلومات: خريطة الطريقة نحو الاعتماد المهني والأكاديمية، الفترة من 7–9 مارس، 2017م.

- بن جمعة، ن. (2015): مستوى جودة الخدمات الطلابية ورضا الطلاب عنها في جامعة الملك سعود. مجلة رسالة التربية وعلم النفس، العدد(51)، ص ص1–28.
- الحافظ، ع ، النعيمي، أ. (2010): دور (ISO 27001:2005) في تعزيز مفهوم إدارة دورة حياة المعلومات (أنموذج مقترح). مجلة جامعة تكريت للعلوم الإدارية والاقتصادية، المجلد (6)، العدد (17).
- الحانوتي، ت. (2014). أمن المعلومات: هاجس العالم الرقمي. المؤتمر الدولي الأول بعنوان المكتبات ومراكز المعلومات في بيئة رقمية متغيرة، جمعية المكتبات والمعلومات الأردنية، عمان، 189–207.
- الحدابي، د ، قشوة، هـ. (2009): "جودة الخدمة التعليمية بكلية التربية بحجة من وجهة نظر طلبة الاقسام العلمية". المجلة لضمان جودة التعليم الجامعي، المجلد (2) العدد (4)، ص ص 92–108.
- حمودة، ب. (2014). سياسة أمن المعلومات في شبكة المكتبات بجامعة النيلين. اتحاد الجامعات العربية– جمعية كليات الحاسبات والمعلومات. 3(5)، 55–62.
- زقاي، ح. زاني، م. (2017): مستوى جودة الخدمات التعليمية وأثرها في رضا الطلبة: دراسة تطبيقية على طلبة جامعة سعيدة– الجزائر. المجلة العربية لضمان الجودة في التعليم الجامعي– اليمن، المجلد (10)، العدد (30).
- سلمان، م. (2012): مستوى جودة الخدمات الجامعية كما يدركها طلبة جامعة الأقصى بغزة طبقاً لمقياس جودة الخدمة (SERVPERF). مجلة جامعة الأقصى (سلسلة العلوم الإنسانية) المجلد السابع عشر، ص ص 1–50.
- عبد الكريم، ن.، والربيعي، خ. (2013). أمن وسرية المعلومات وأثرها على الأداء التنافسي. مجلة دراسات محاسبية ومالية، 8(23)، 289–317.

- العربي، أ. (2013): المعايير الدولية لسياسات أمن المعلومات: دراسة تحليلية لمعايير المنظمة الدولية للتوحيد القياسي ومدى تطبيقها في الجامعات العربية. مجلة مكتبة الملك فهد الوطنية، المجلد(19)، العدد(2)، ص ص157-210.
- العربي، أ. (2015). معيار المنظمة الدولية للتوحيد القياسي ايزو 27002 لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية. مجلة جامعة طيبة، المجلد(4)، العدد(7)، ص ص 661-738.
- عز الدين، م.، ومصطفى، أ. (2016). درجة رضا الطلبة نحو الخدمات التعليمية: دراسة حالة على جامعة أبو ظبي. مجلة دراسات، المجلد(3)، العدد(43)، ص ص 1197-1212.
- علي، إ. (2017). أمن المعلومات الصحية. مجلة التقدم العلمي- مؤسسة الكويت للتقدم العلمي (KFAS)، العدد (99).
- عمار، ز. الكبيسي، ي. (2012): التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية : دراسة مسحية تحليلية. المجلة العربية الدولية للمعلوماتية، السعودية، المجلد (1)، العدد (1)، ص ص 35-41.
- العميري، م ، السالمي، ج ، الحجي، خ ، أبو الكشك، ع. (2017): واقع ممارسات أمن المعلومات في المكتبة الرئيسة بجامعة السلطان قابوس، ومدى توافقها مع المعيار الدولي لأمن المعلومات، دراسة حالة (ISO/IEC 27002). المؤتمر الدولي الثالث والعشرين (SLA-AGC) البحرين.
- الكسر، ش. (2018): "دور تطبيق معايير الجودة الشاملة في تحقيق الحوكمة الإدارية في الجامعات". مجلة كلية التربية الأساسية للعلوم التربوية والانسانية، العدد(39)، ص ص 417-430.
- المصري، ن ، الأغا، م. (2018): "واقع العدالة التنظيمية كمصدر للتنافسية من خلال ممارسة الجامعات الفلسطينية لمعيار أمن المعلومات (ISO/IEC 27002) في ضوء التماثل التنظيمي: مقترح تطبيقي تنموي استراتيجي". المجلة العربية لضمان جودة التعليم العالي، المجلد (11)، العدد (35)، ص ص 3-36.

- يـونس، ر. (2017). دارسـة واقـع إدارة أمـن نظـم المعلومـات فـي المؤسسـات السـورية. مجلة جامعة البعث، المجلد (39)، العدد (31).

ج. الرسائل العلمية

- جـودة، س (2014). دور تقيـيم أداء المـوارد البشـرية فـي تحسـين جـودة خـدمات بلـديات قطاع غزة. أكاديمية الإدارة والسياسة، غزة، فلسطين. (رسالة ماجستير غير منشورة).
- الـدنف، أ. (2013): واقـع إدارة أمـن نظـم المعلومـات فـي الكليـات التقنيـة بقطـاع غـزة وسـبل تطويرها. الجامعة الإسلامية، غزة، فلسطين. (رسالة ماجستير غير منشورة).
- دهليـز، م. (2018). جـودة الخـدمات المقدمـة مـن دوائـر الضـريبة وأثرهـا فـي تحسـين الأداء التنظيمـي لمكاتـب المحاسـبة والتـدقيق بقطـاع غـزة. أكاديميـة الإدارة والسياسـة، غـزة، فلسطين. (رسالة ماجستير غير منشورة).
- الـدهيمات، ع (2011). جـودة الخـدمات الإلكترونيـة التـي تقـدمها مكتبـات الجامعـات الأردنيـة الرسـمية والخاصـة مـن وجهـة نظـر المسـتفيدين. جامعـة الشـرق الأوسـط، عمـان، الأردن. (رسالة ماجستير غير منشورة).
- السـر، أ. (2014). جـودة المواقـع الإلكترونيـة وتأثيرهـا علـى الميـزة التنافسـية للجامعـات الفلسـطينية فـي قطـاع غـزة مـن وجهـة نظـر الطلبـة. الجامعـة الإسـلامية، غـزة، فلسـطين. (رسالة ماجستير غير منشورة).
- السـعافين، ف. (2017): اسـتراتيجية مقترحـة لتحسـين مسـتوى جـودة الخـدمات الطلابيـة فـي الجامعـات الفلسـطينية، الجامعـة الإسـلامية، غـزة، فلسـطين. (رسـالة ماجسـتير غيـر منشورة).
- عبـد الجـابر، ي. (2013): مـدى فاعليـة إجـراءات الرقابـة الداخليـة فـي تـوفير أمـن المعلومـات الإلكترونيـة فـي الشـركات الصـناعية الأردنيـة. جامعـة الشـرق الأوسـط، عمـان، الأردن. (رسالة ماجستير غير منشورة).
- عبـد الواحـد، آ. (2015). سياسـات أمـن المعلومـات وعلاقتهـا بفاعليـة نظـم المعلومـات الإداريـة فـي الجامعـات الفلسـطينية. رسـالة ماجسـتير غيـر منشـورة، جامعـة الأزهـر، غـزة– فلسطين.

- عـودة، إ. (2012). العلاقــة التأثيريــة بــين جــودة الخــدمات الإلكترونيــة وســمعة الجامعــات. رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان، الأردن.
- مقرانــي، ق. (2016). تقيـيم مـدى مسـاهمة أمـن نظـم المعلومـات الإلكترونيــة فــي الحـد مـن مخـاطر نظـم المعلومـات. رسـالة ماجسـتير غيـر منشـورة، جامعـة قاصـدي مربـاح، ورقلـة، الجزائر.

ثانياً: المراجع باللغة الإنجليزية

- Alnawaiseh, A. J. (2014). SECURITY INFORMATION SYSTEM OF THE COMPUTER CENTER IN MU'TAH UNIVERSITY. ***European Scientific Journal, ESJ***, *10*(27).
- Calder, A., & Watkins, S. (2012). ***IT Governance: an international guide to data security and ISO27001/ISO27002***. Kogan Page Publishers.
- Harris، S.، & Foreword By-Kowtko، J. (2001). **CISSP certification all-in-one exam guide**. McGraw-Hill Professional.
- ISO/IEC 27002، (2013). **Information technology — Security techniques — Code of practice for information security controls**. Second edition 2013-10-01، Copyrighted material licensed to University of Toronto by Thomson Scientific، Inc. (www.techstreet.com). This copy downloaded on 2015-07-07 13:54:34 -0500 by authorized user University of Toronto User
- Kotler, P., & Armstrong, G. (2013). **Principles of Marketing** (16th Global Edition).
- Kumar,S.,(2006),**Total Quality Management**, Laxmi Publications(p)LTD 22,Golden
- Napitupulu, D., Rahim, R., Abdullah, D., Setiawan, M. I., Abdillah, L. A., Ahmar, A. S., ... & Pranolo, A. (2018, January). Analysis of Student Satisfaction Toward Quality of Service Facility. In ***Journal of Physics: Conference Series*** (Vol. 954, No. 1, p. 012019). IOP Publishing.
- Năstase, P., Năstase, F., & Ionescu, C. (2009). Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. ***Economic computation & economic cybernetics studies & research***, *43*(1), 16.
- Ozen, G., Yaman, M. and Acar, G. (2012). Determination of the employment status of graduates of recreation department. ***The Online Journal of Recreation and Sport*** , Vol. 1, Issue 2.
- Parasuraman, A., Zeithaml, V., & Berry, L. (2002). SERVQUAL: a multiple-item scale for measuring consumer perceptions of service quality. Retailing: critical concepts, 64(1), 140.

- Sharma، N. C. (2015). **Understanding Preparedness for Information System Disasters in Australian Higher Education Organizations**: A Comparative Case Study Approach (Doctoral dissertation، Griffith University).
- tandard, A. (2015). ISO/IEC 27002. ***Information technology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015), Standards Australia.***
- tandard, A. (2015). ISO/IEC 27002. ***Information technology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015), Standards Australia.***
- **The Practice of Business Statistics**, 2003, Moore, D., McCabe, G., Duckworth, W, Sclove, S.
- Tipton، H. F.، & Nozaki، M. K. (2007). **Information security management handbook**. CRC press.
- Whitman Michael، Mattod Herberet (2011). **Principles of Information Security**، 4th edition، Boston : Cengage Learning /Course Technology
- Yilmaz, R., & Yalman, Y. (2016). A Comparative Analysis of University Information Systems within the Scope of the Information Security Risks. *TEM Journal*, *5*(2), 180.

ثالثاً: المواقع الإلكترونية

- **http://alazhar.edu.ps.**
- **http://alaqsa.edu.ps**
- **http://up.edu.ps**
- **http://www.gu.edu.ps**
- **http://www.iugaza.edu.ps**
- **http://www.qou.edu**

ملحق رقم (1): الاستبانة في صورتها النهائية

جامعة القدس

برنامج الدراسات العليا

معهد التنمية المستدامة

بناء المؤسسات وتنمية الموارد البشرية

أخي الموظف، أختي الموظفة...

تحية طيبة وبعد:

يقوم الباحث بإجراء دراسة بعنوان: "**واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة**"، وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في برنامج بناء المؤسسات وتنمية الموارد البشرية.

ولتحقيق أهداف الدراسة أعد الباحث استبانة مكونة من ثلاثة أجزاء؛ الأول: يتمثل بال**بيانات العامة**، والثاني: **معايير أمن المعلومات (ISO-IEC 27002)**، والثالث: **جودة الخدمات المقدمة**.

الأخ الكريم، الأخت الكريمة، إن تعبئة الاستبانة يعد إسهاماً مقدراً منكم في دعم خدمة البحث العلمي، ونؤكد لكم بأنَّ المعلومات المحصلة من خلال هذه الأداة لن تستخدم إلا لأغراض البحث العلمي، ولن تؤثر استجابتك بأي شكل من الأشكال على وضعك الشخصي أو المهني.

لذا يرجى قراءة كل بند من بنود الاستبانة بعناية ودقة، ووضع إشارة (✓) واحدة فقط امام كل عبارة من عبارات الأداة، مع مراعاة أن تكون الإجابة من خلال الواقع الفعلي، وليس كما تفضل أو كما ترجو أن يكون عليه الحال.

شكرا لكم على حسن التعاون

الدكتور المشرف: د. محمد أبو سعدة

الباحث: همام سالم المصري

ملاحظة: نود اعلامكم بأن هذه الاستبانة ستأخذ من وقتكم 10 دقائق تقريبا.

أولاً: معلومات عامة:

يرجى وضع إشارة (X) أمام الحالة التي تنطبق عليك:

1- **الجنس:**

☐ ذكر ☐ أنثى

2- **الجامعة:**

☐ الأقصى ☐ الأزهر ☐ الإسلامية ☐ فلسطين

3- **المؤهل العلمي:**

☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا

4- المسمى الوظيفي:

☐ إدارة عليا ☐ إدارة وسطى ☐ دائرة شبكات المعلومات

5-سنوات الخبرة:

☐ 1-5 سنوات ☐ 5-10 سنوات ☐ 10-15 سنة ☐ أكثر من 15 سنة

ثانيا: معايير أمن المعلومات (ISO-IEC 27002)

م	العبارة	درجة التوافر				
		كبيرة جداً	كبيرة	متوسطة	قليلة	قليلة جداً
المحور الأول: تقييم المخاطر ومعالجتها						
1.	يتوفر لدى الجامعة ضوابط لتقليص المخاطر التي تتعلق بالمعلومات.					
2.	يوجد توافق بين قوانين الجامعة مع اللوائح والقوانين المحلية والدولية.					
3.	يوجد ضوابط لتشغيل الأنظمة ومتابعتها.					
4.	تتوفر موازنة تطبيق الضوابط والضرر المتوقع حدوثه.					
5.	يتم تقييم المخاطر الأمنية بشكل دوري.					
المحور الثاني: السياسات الأمنية						
1.	يتوفر لدى الجامعة وثيقة عامة لسياسة أمن المعلومات.					
2.	تحرص الجامعة على المراجعة لسياسة أمن المعلومات.					
3.	تجاز وثيقة أمن المعلومات من الإدارة العليا للجامعة ويتم تعميمها على كل العاملين والجهات الخارجية ذات العلاقة.					
4.	تتوفر لدى الجامعة رؤية واضحة في إدارة أمن المعلومات.					
5.	تراعي الجامعة حساسية المعلومات الخارجية والخاصة بالسياسات الأمنية.					
المحور الثالث: تنظيم أمن المعلومات						
1.	تلتزم الإدارة العليا بدعم مستلزمات أمن المعلومات وتوفيرها.					
2.	يتم مراجعة أمن المعلومات بشكل دوري.					
3.	يوجد تحديد للمسئوليات التي تتعلق بأمن المعلومات.					
4.	يوجد تحديد لمتطلبات أمن المعلومات عند التعامل مع الأطراف الخارجية.					
5.	يوجد ضوابط لمعالجة المعلومات التي تستخدمها الأطراف الخارجية.					
المحور الرابع: إدارة الأصول						
1.	يتم تحديد واضح لأنواع الأصول (المعلومات– الأصول البرامجية– الأصول المادية– خدمات المعلومات– الأفراد– سمعة الجامعة وصورتها).					
2.	يتم توثيق كافة الأصول وإنشاء سجل لحفظها.					
3.	يتم تحديد مستوى الحماية المناسبة لأهمية الأصل المعلوماتي.					
4.	يتم تحديد ملكية كل أصل من أصول الجامعة بوضوح.					
5.	يوجد اهتمام واضح من قبل الجامعة بالأصول المعنوية وخاصة المعلومات.					

م	العبارة	درجة التوافر				
		كبيرة جداً	كبيرة	متوسطة	قليلة	قليلة جداً
المحور الخامس: أمن الموارد البشرية						
1.	يتم التأكد من دقة السيرة الذاتية وتحديدا المؤهلات الأكاديمية والمهنية للعاملين.					
2.	تتأكد الجامعة أنَّ العاملين لديهم القدرة على التعامل مع قضايا أمن المعلومات.					
3.	يوجد وضوح وإعلان للعقوبات الخاصة بالخروقات الأمنية للمعلومات.					
4.	يوجد تدريب للعاملين على أمن المعلومات.					
5.	يتم إلغاء كلمات المرور وصلاحيات الوصول عند انتهاء خدمة الموظف.					
المحور السادس: الأمن المادي والبيئي						
1.	يقتصر الوصول إلى مرافق معالجة المعلومات على الأفراد المخولين فقط.					
2.	تتجنب الإدارة وضع أي لوحات تدل على مرافق معالجة المعلومات.					
3.	يتم فحص الأجهزة والمعدات قبل دخولها غرف معالجة المعلومات.					
4.	يوجد منع للوصول غير المرخص للأجهزة والمعدات وحاويات المعلومات.					
5.	توضع ضوابط لحماية معدات المنظمة وأجهزتها من أي أخطار طبيعية.					
6.	توضع ضوابط لحماية معدات المنظمة وأجهزتها من أي أخطار بشرية.					
المحور السابع: إدارة العمليات/ الاتصالات وحمايتها						
1.	تمتلك الجامعة أنظمة للحماية من البرامج الخبيثة.					
2.	تهتم الجامعة بالنسخ الاحتياطي لمواجهة كل ما هو طارئ.					
3.	يوجد سياسات وإجراءات لحماية تبادل المعلومات.					
4.	تحمي الجامعة الرسائل الإلكترونية من الوصول غير المصرح.					
5.	يتم ضمان تشغيل نظام المعلومات على مدار الساعة بأمان.					
المحور الثامن: التحكم في الوصول						
1.	تمتلك الجامعة إجراءات إدارة دخول المستخدم.					
2.	تتوفر إدارة لمسؤوليات المستخدم (كلمات المرور، تأمين الأجهزة في غياب المستخدمين، خلو سطح المكتب والشاشة).					
3.	تتوفر لدى إدارة الجامعة إجراءات للتحكم في الوصول الى الشبكة.					
4.	يوجد لدى إدارة الجامعة إجراءات التحكم في الدخول إلى برامج التطبيقات.					
5.	يمكن لمستخدمي النظم العمل والاتصال عن بعد ومراقبة العمل عن بعد، بعيداً عن شبكة الجامعة.					

م	العبارة	درجة التوافر				
		كبيرة جداً	كبيرة	متوسطة	قليلة	قليلة جداً
المحور التاسع: حيازة أنظمة المعلومات وتطويرها وصيانتها						
1.	يتم تحديد المتطلبات الأمنية اللازمة لتأمين أنظمة المعلومات.					
2.	توجد آليات للتأكد من صحة البيانات في أنظمة المعلومات.					
3.	تهتم الإدارة بحماية سرية وسلامة المعلومات من خلال وسائل التشفير.					
4.	توجد ضوابط للتحكم في الوصول إلى ملفات نظام المعلومات.					
5.	يوجد تحديد للمسئوليات والأدوار المرتبطة بأنظمة المعلومات.					
المحور العاشر: إدارة حوادث أمن المعلومات						
1.	توجد ضوابط للتبليغ عن مواطن الضعف في أنظمة المعلومات.					
2.	يتم التعلم والاستفادة من حوادث أمن المعلومات في المستقبل.					
3.	يتم التأكد من تدخل الجهات الأمنية للتحقيق قبل طمس الحقائق.					
4.	يوجد تحديد للمسئوليات عند وقوع حوادث أمن المعلومات.					
5.	تتم الاستعانة بلجان متخصصة للتحقيق في حوادث أمن المعلومات.					
المحور الحادي عشر: إدارة استمرار العمل						
1.	تتوفر إمكانيات وموارد مالية للإفادة منها لإعادة استمرارية العمل.					
2.	يتم الحفاظ على خصوصية حوادث أمن المعلومات وسريتها لضمان استمرار العمل.					
3.	يوفر النظام جمع الأدلة في أقرب وقت ممكن بعد وقوع الحادث.					
4.	يتوفر تحديد لكل الأحداث التي يمكن أن تسبب الانقطاع في الأعمال.					
5.	يوجد توثيق لكل العمليات التي تم اتخاذها لإعادة استمرارية العمل.					
المحور الثاني عشر: الامتثال والتوافق						
1.	يتم تحديد للتشريعات المعمول بها وحماية الملكية الفكرية.					
2.	تسعى الجامعة للحد من سوء استخدام المعلومات الشخصية.					
3.	توجد ضوابط لبرامج التشفير والتأكد من أنها تتوافق مع التشريعات القانونية.					
4.	تحصل الجامعة على البرامج والتطبيقات الأصلية.					
5.	تتم المحافظة على تراخيص الاستخدام وأدلة التشغيل وأقراص التثبيت.					

ثالثا: جودة الخدمات المقدمة

م	العبارة	درجة التوافر				
		كبيرة جداً	كبيرة	متوسطة	قليلة	قليلة جداً
1.	تتوفر خدمة الموقع الإلكتروني للجامعة بشكل دائم دون أي انقطاع.					
2.	يتمتع الموقع الإلكتروني للجامعة بواجهة تفاعلية ذات جاذبية للمستخدمين.					
3.	يتوفر لدى الطالب نوع من خصوصية البيانات.					
4.	يستطيع الطالب التوصل الى الحل الأمثل لما يطلبه عبر الخدمات الإلكترونية المقدمة من قبل الجامعة.					
5.	يمكن للطالب التبليغ عن المشكلات وحلها دون الحاجة إلى الذهاب إلى الجامعة.					
6.	توفر الخدمات الإلكترونية المقدمة للطلبة الوقت والجهد في كثير من الأحيان.					
7.	يوجد سرعة في الاستجابة حين تقديم الخدمة للطلاب.					
8.	توجد سهولة في استرجاع كلمة السر في حالة فقدانها من قبل الطالب.					
9.	توجد سهولة في عملية إجراء القبول والتسجيل عبر الموقع الإلكتروني.					
10.	من الصعب أن يتمكن أحد غير الطالب من الدخول إلى حسابه.					
11.	يستطيع الطالب التعامل بسهولة مع الخدمات التي يقدمها موقع الجامعة.					
12.	يستطيع الطالب إنجاز كافة المعاملات الخاصة به من خلال موقع الجامعة الإلكتروني.					
13.	تقوم الجامعة بتحديث الخدمات الإلكترونية بشكل مستمر.					
14.	يتحمل موقع الجامعة الإلكتروني الضغط الشديد في أوقات تسجيل المواد وظهور العلامات الفصلية.					
15.	الخدمات الإلكترونية التي تقدمها الجامعة تضاهي المؤسسات الأخرى.					
16.	يحصل الطالب على المعلومات بسرعة فائقة.					
17.	تتوفر جميع المعلومات التي تخص الطالب على بوابته الالكترونية.					
18.	يستطيع الطالب تغيير اسم المستخدم وكلمة المرور على بوابته الالكترونية بسهولة.					
19.	يثق الطلاب بأمن المعلومات وحمايتها التي توفرها الجامعة.					
20.	يحصل الطالب على المعلومات التي يحتاج اليها بدقة فائقة.					

شاكرين لكم حسن تعاونكم معنا،،،

ملحق رقم (2) قائمة بأسماء السادة المحكمين

م	الاسم	المؤسسة	التخصص
1.	د. جهاد المصري	القدس المفتوحة	مساعد رئيس فرع رفح
2.	د. حسن سعدوني	القدس / أبوديس	الإدارة الدولية
3.	د. أشرف محمد مشمش	الأقصى	رئيس قسم إدارة الأعمال
4.	د. سليمان الطلاع	الأزهر	إدارة الأعمال
5.	د. نضال حمدان المصري	القدس المفتوحة	إدارة الأعمال
6.	د. حازم الشيخ عيد	القدس المفتوحة	أستاذ مشارك في الاحصاء
7.	د. فؤاد محمد عودة	جامعة غزة	إدارة الاعمال
8.	د. عماد العبادلة	القدس المفتوحة	احصاء رياضي
9.	د. ابراهيم عابدين	القدس المفتوحة	إدارة الأعمال
10.	د. رشاد حماد	الكلية العربية للعلوم التطبيقية	إدارة الأعمال

ملحق رقم (3) كتاب تسهيل مهمة

التاريخ: 2019/3/12

تسهيل مهمة

يفيد برنامج التنمية المستدامة – بناء مؤسسات وتنمية موارد بشرية –جامعة القدس بأن الطالب/ة جهاد سالم كامل نصري ورقمه/ها الأكاديمي: 21620443

هو /هي أحد طلبة معهد التنمية المستدامة في جامعة القدس يقوم بعمل بحث ودراسة عن:

ISO-IEC27002 تطبيق معايير أمن المعلومات في واقع الجامعات الفلسطينية في محافظة القدس

وعليه نرجو التكرم منكم بمساعدته/ها للحصول على المعلومات اللازمة لهذه الدراسة ،علما بأن المعلومات والبيانات التي يحصل عليها الطالب تعامل بسرية تامة ولأغراض البحث العلمي فقط .

وتفضلوا بقبول وافر الاحترام والتقدير ،،،

د. تهاني جفال

منسقة برنامج التنمية المستدامة

نسخة : الملف

Gaza Taf AL Hawa
Tel:08-2644260
email: tjaffal@staff.alquds.edu

غزة- تل الهوى
هاتف: 08-2644260
البريد الالكتروني: tjaffal@staff.alquds.edu

ملحق رقم (4): طلب تحكيم استبانة

جامعـة القدس

برنامــج الدراســات العليا

معهد التنمية المستدامة

بناء المؤسسات وتنمية الموارد البشرية

حضرة الدكتور: ..... المحترم

تحية طيبة وبعد،،،

يقوم الباحث بإجراء دراسة بعنوان: "**واقع تطبيق معايير أمن المعلومات (ISO-IEC 27002) في الجامعات الفلسطينية، وعلاقتها بجودة الخدمات المقدمة**"، وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في برنامج بناء المؤسسات وتنمية الموارد البشرية.

أرجـو التكـرم بتحكـيم اسـتبانة الدراسـة لمـا عهـدناه فـيكم مـن خبـرة ومعرفـة علميـة فـي البحـوث العلمية.

وتفضلوا بقبول فائق الاحترام والتقدير والشكر على المساعدة

اشراف الدكتور: محمد أبو سعدة

إعداد الطالب: همام سالم المصري

فهرس الملاحق

فهرس الجداول

فهرس المحتويات