ISSN: 2706-6495

تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 التابع لشركة الكهرباء السعودية

The impact of information security policies on the overall performance and operational efficiency of the Emergency Center 933 of the Saudi Electricity Company

إعداد:

الباحث/ ماهر محمد السلمي[1]، الباحث/ محمد فهيد السبيعي[2]، الدكتور/ ماهر حسن فقيها[3]، الباحثة/ خلود خالد السلمي[4]

ماجستير علم المعلومات (إدارة معلومات)، قسم علم المعلومات، كلية الآداب والعلوم الإنسانية، جامعة الملك عبدالعزيز، المملكة العربية السعودية [1،2،4]

أستاذ مشارك في قسم علم المعلومات، كلية الآداب والعلوم الإنسانية، جامعة الملك عبد العزيز، المملكة العربية السعودية [3]

[1*]Email: malsulami0654@stu.kau.edu.sa

المستخلص:

هدفت هذه الدراسة إلى التعرف على مستوى تطبيق سياسات أمن المعلومات في مركز الطوارئ 933، ومن ثم التحقق من مستوى الأداء العام والكفاءة التشغيلية في المركز. ونتبع في هذه الدراسة المنهج الوصفي التحليلي، يتكون مجتمع الدراسة من موظفي مركز الطوارئ 933، وتم اختيار عينة عشوائية بحجم 252 فردًا. تم استخدام استبانة كأداة لجمع البيانات، وتم تحليل النتائج باستخدام الإحصاءات الوصفية والتحليل الإحصائي. تبين الدراسة أن هناك إدراكًا إيجابيًا لأهمية سياسات أمن المعلومات في المركز، حيث تم تقدير أبعادها المختلفة بمتوسط حسابي مرتفع. كما أظهرت النتائج مستوى عالٍ من الأداء العام والكفاءة التشغيلية في المركز، مما يعكس جاهزيته لتقديم الخدمات بفعالية. ويشير التحليل إلى أن تطبيق سياسات أمن المعلومات يؤثر بشكل إيجابي على الأداء العام والكفاءة التشغيلية، ويسهم في تعزيز التنظيم واستخدام الموارد بشكل فعال. استنادًا إلى النتائج، نوصي بتعزيز برامج التدريب والتوعية بشأن سياسات أمن المعلومات بمركز الطوارئ 933، لضمان تطبيق السياسات بفعالية من قبل جميع الموظفين، والاستمرار في تطوير وتحسين التقنيات المستخدمة في مركز الطوارئ لضمان أنظمة الأمان والتشغيل تعمل بكفاءة عالية وفعالية، وكذلك مراجعة سياسات أمن المعلومات بشكل دوري ومستمر لضمان تحديثها ومواءمتها مع التطورات التكنولوجية والتهديدات الأمنية الجديدة، ويجب تعزيز التواصل الداخلي في المركز من خلال الاجتماعات الدورية والتوجيهات الواضحة لتحقيق فهم مشترك لأهداف المركز والتحديات التي قد تواجهه، وإجراء تقييمات دورية لأداء المركز العام والفردي لتحديد نقاط القوة والضعف.

الكلمات المفتاحية: سياسات أمن المعلومات، الأداء العام، الكفاءة التشغيلية، مركز الطوارئ 933

ISSN: 2706-6495

The impact of information security policies on the overall performance and operational efficiency of the Emergency Center 933 of the Saudi Electricity Company

Maher Mohammed Alsulami[1], Mohmmed Fehaid Alsubaie[2], Dr. Maher Mohsen Faqiha[3], Khouloud Khaled Alsulami[4]

Master of Information Science (Information Management), Department of Information Science, Faculty of Arts and Humanities, King Abdulaziz University, Saudi Arabia [1,2,4]

Associate Professor, Department of Information Science, Faculty of Arts and Humanities, King Abdulaziz University, Saudi Arabia[3]

Abstract:

This study aimed to identify the level of implementation of information security policies at Emergency Center 933, and subsequently verify the level of overall performance and operational efficiency at the center. The researcher followed a descriptive analytical approach in this study. The study population consisted of employees at Emergency Center 933, and a random sample of 252 individuals was selected. A questionnaire was used as a data collection tool, and the results were analyzed using descriptive statistics and statistical analysis. The study revealed a positive perception of the importance of information security policies at the center, with their various dimensions being highly regarded. Furthermore, the results indicated a high level of overall performance and operational efficiency at the center, reflecting its readiness to provide services effectively. The analysis also indicated that the implementation of information security policies has a positive impact on overall performance and operational efficiency, contributing to enhanced organization and effective resource utilization. Based on the findings, It is recommended to enhance training and awareness on information security at the 933 Emergency Center, improve technologies for efficient operations, and regularly review policies to address emerging threats. Strengthening internal communication through meetings and clear directives is also advised to ensure alignment with the Center's goals and challenges.

Keywords: Information Security Policies, Overall Performance, Operational Efficiency, Emergency Center 933

1. المقدمة:

يعتبر أمن المعلومات فرع من فروع العلم الباحث في مجال توفير الحماية اللازمة للمعلومات ومنع الوصول لها وهدرها من غير حاجة أو صلاحية، وكذلك حمايتها من التهديدات الخارجية، ويعتبر هذا العلم نوعاً من تمكين سيطرة المستخدم على المعلومات بشكل كامل حيث تمتاز هذه العملية بأنها مستمرة ومواكبة لكل ما هو متطور من درجات الأمان وأساليب الحماية الحديثة للمعلومات، ففي ظل التطورات السريعة في مجال التكنولوجيا والاتصالات، أصبحت أمن المعلومات أحد الجوانب الحيوية والأساسية لأي مؤسسة أو منظمة. (عوض الله، 2017)

رغم الفائدة الكبيرة من توسع انتشار التكنولوجيا وتطورها التي ساعدت في تطور الخدمات وفاعليتها والتعامل مع المعلومات بكل يسر وسهولة. إلا أنها باتت تشكل خطر وتهديدات محتملة لاختراق هذه المعلومات. ولذلك جاءت سياسات أمن المعلومات لحماية سرية هذه المعلومات وكذلك نزاهتها وتوفيرها والوصول إليها. ويجدر الإشارة إلى أن الاستثمار في أمن المعلومات بات يُنظر إليه في السنوات الأخيرة على أنه أحد الاهتمامات الأساسية لإدارة البنية التحتية لتقنية المعلومات في المنظمات والمنشآت. بسبب ما تواجهه تلك المنظمات والمنشآت من زيادة في الاختراقات وكثرة الغارات اليومية، لاسيما في المعلومات التي يسهل على الجمهور الوصول إليها (AL-HAMAR , 2018).

ومن بين الهيئات التي تعتمد بشكل كبير على السلامة والأمان فيما يتعلق بالمعلومات هي مراكز الطوارئ933. تعتبر مراكز الطوارئ نقطة الاتصال والتنسيق الرئيسية في حالات الطوارئ، توفير الأمان والحماية للمعلومات في مراكز الطوارئ أصبح أمراً لا غنى عنه في ظل التهديدات المتزايدة لأمن المعلومات، بما في ذلك الهجمات السيبرانية والتسريبات السرية والاختراقات الإلكترونية. ولهذا السبب، أصبحت سياسات أمن المعلومات ضرورة ملحة لضمان استمرارية عمل مراكز الطوارئ وتحقيق أدائها العالي والكفاءة التشغيلية المطلوبة.

يحاول هذا البحث إلى استكشاف تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933. ستقوم الدراسة بتحليل مدى تبني مركز الطوارئ 933 لسياسات أمن المعلومات وتطبيقها.

من خلال التعرف على تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933، يمكن تطوير استراتيجيات فعالة لتعزيز الأمن السيبراني وتحسين الجاهزية لمواجهة التحديات المتزايدة في هذا العصر الرقمي.

1.1. مشكلة الدراسة:

لقد أشارت الدراسات السابقة بوجود قصور لدى الكثير من المنظمات السعودية، كدراسة الذنيبات (2018) التي توصلت إلى أن أداء الممارسات التنظيمية والإدارية لأمن المعلومات كان منخفض، وقد اشارت دراسة الشمالي (2017) إلى أن ممارسات أمن المعلومات له تأثير إيجابي على الأداء، لذا تأتي هذه الدراسة لبيان تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933، رغم أن مركز الطوارئ 933 ، يعمل على حماية بياناته ومعلوماته من السرقة والاختراق وذلك من خلال الإدارة السليمة لأمن معلوماته وشبكات اتصاله، وبسبب التطور التكنولوجي ووسائل تخزين المعلومات وتبادلها بطرق مختلفة. سعى مركز الطوارئ 933، إلى مواكبة التطور التكنولوجي ووسائل حماية أمن المعلومات والبيانات ذات الصلة بعمله وذلك للحد من السرقة والاختراق من خلال الإدارة السليمة لأمن معلوماتهما. وعليه تحددت مشكلة الدراسة في الإجابة على التساؤل الرئيسي التالي:

ما تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933؟

2.1. أهمية الدراسة:

1.2.1. الأهمية العلمية:

دراسة تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 تمثل إسهاماً علمياً مهماً في مجال علم المعلومات. من خلال هذه الدراسة، سيتم معرفة التأثير الذي تمارسه سياسات أمن المعلومات على أداء مركز الطوارئ 933. وسيساهم ذلك في إثراء المعرفة العلمية المتعلقة بتفاعل السياسات الأمنية مع كفاءة أداء مراكز الطوارئ، مما يسهم في تطوير المفاهيم في هذا المجال.

كما تكتسب هذه الدراسة أهميتها العلمية من إمكانية استخدام الباحثين لها في تطوير قسم أمن المعلومات بمركز الطوارئ 933 بعد التعرف على أثر سياسات أمن المعلومات ومساهمتها في تسهيل العمليات والإجراءات باستخدام المعلومات والبيانات وتداولها على تحسين الأداء العام والكفاءة التشغيلية في مركز الطوارئ 933 وكذلك فتح مجالات للباحثين والمهتمين بهذا الموضوع من خلال المعلومات التي ستوفرها الدراسة .

2.2.1. الأهمية العملية:

تكتسب هذه الدراسة أهميتها العملية من توفير أسس علمية سليمة ومادة علمية تساعد في تحسين قسم أمن المعلومات في مركز الطوارئ 933 للتعامل مع الكم الهائل من المعاملات الإلكترونية وبما تحتوي عليه من معلومات كما تفيد في تسهيل تداول المعلومات واستخدامها، وتوفير الوقت والجهد على صانعي القرار والموظفين.

يمكن أن تسهم النتائج العملية لهذه الدراسة في تحسين أداء وفاعلية مراكز الطوارئ في التعامل مع التحديات الأمنية الحديثة والتهديدات السيبرانية.

3.1. أهداف الدراسة:

1. التعرف على مستوى تطبيق سياسات أمن المعلومات في مركز الطوارئ 933.
2. التعرف على مستوى الأداء العام في مركز الطوارئ 933.
3. التعرف على مستوى الكفاءة التشغيلية في مركز الطوارئ 933.
4. الكشف عن تأثير سياسات أمن المعلومات على الأداء العام وكفاءة التشغيل والاستجابة في مركز الطوارئ 933.
5. تقديم توصيات عملية لتحسين سياسات أمن المعلومات في مركز الطوارئ 933 بناءً على النتائج والتحليلات الحاصلة من الدراسة.
6. إثراء المعرفة والفهم في مجال أمن المعلومات وتطبيقاتها في بيئة المراكز الطارئة والمؤسسات الحكومية.

4.1. تساؤلات الدراسة

بناءً على أهداف الدراسة المحددة، يمكن تحديد التساؤلات التالية:

1. ما مستوى تطبيق سياسات أمن المعلومات وأبعادها في مركز الطوارئ 933 من وجهة نظر الموظفين فيه؟
2. ما مستوى الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين فيه؟

5.1. منهج الدراسة:

سوف يستخدم في هذه الدراسة المنهج الوصفي التحليلي، لأن هذا المنهج يصف الظاهرة بشكل واضح من خلال المعلومات التي ستجمع وسيتم تحليلها بالطرق الإحصائية المناسبة. بهدف التعرف على تأثير سياسات أمن المعلومات على الأداء العام

والكفاءة التشغيلية لمركز الطوارئ 933، سيتم في هذه الدراسة استعراض الأدبيات المتعلقة بسياسات أمن المعلومات وتأثيرها على الأداء العام والكفاءة التشغيلية في مركز الطوارئ 933. سيتم تحديد المتغيرات المرتبطة بسياسات أمن المعلومات والأداء العام والكفاءة التشغيلية، مثل تنفيذ السياسات والامتثال لها وتأثيرها على عمليات المركز. كما سيتم تصميم الأدوات المناسبة (الاستبيان) لجمع البيانات من المشاركين في المركز. سيتم جمع البيانات من خلال الأدوات المصممة في الخطوة السابقة، مع الأخذ في الاعتبار ضمان الدقة والموثوقية. سيتم تحليل البيانات باستخدام أساليب تحليلية مثل التحليل الإحصائي لتقديم العلاقات بين المتغيرات. وسيتم في النهاية استنتاج النتائج المستخلصة من التحليل والبيانات المقدمة، وستُقدم توصيات عملية لتحسين سياسات أمن المعلومات وبناء على الاستنتاجات الناتجة من الدراسة.

6.1. مصطلحات الدراسة:

أمن المعلومات :

أمن المعلومات مفهوم يشير إلى نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية تقنية، يشير الى الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. (أحمد، 2016) وعرف أبو ذويب (2019) أمن المعلومات بأنه حماية المعلومات من الوصول غير المسموح به. (أبو ذويب، 2019).

التعريف الإجرائي: أمن المعلومات في مركز الطوارئ 933 هي الجهود والسياسات والتدابير المتخذة لحماية المعلومات المتواجدة في المركز من التهديدات والمخاطر التي تهددها، سواء كانت تلك التهديدات من الداخل أو الخارج. يتضمن أمن المعلومات مجموعة من الاستراتيجيات التي تهدف إلى توفير الحماية للمعلومات، بالإضافة إلى تطبيق وسائل وإجراءات تقنية متطورة لضمان سلامة وسرية المعلومات ومنع الوصول غير المسموح بها، سواء كان هذا الوصول من داخل المؤسسة أو من خارجها.

سياسات أمن المعلومات:

سياسات أمن المعلومات هي قواعد عملية وفنية موثقة لحماية جهة ما من مخاطر أمن المعلومات التي تحدق بأعمالها وبنيتها التحتية التقنية، وتقدم وثائق السياسات المكتوبة هذه وصفاً عاماً للضوابط المختلفة التي ستستخدمها المؤسسة لإدارة مخاطر أمن المعلومات لديها، وتعتبر وثائق سياسات أمن المعلومات إعلانا رسميا عن نية الإدارة لحماية أصول المعلومات لديها من المخاطر ذات العلاقة. قد تكون سياسات أمن المعلومات مدعومة بإجراءات الأمن المعلومات في بعض الحالات، وتبين هذه الإجراءات الأنشطة الرئيسية اللازمة لتطبيق تلك السياسات (المركز الوطني الإرشادي لأمن المعلومات،1432هـ).

التعريف الإجرائي: مجموعة من القواعد والإجراءات والأدوات الأمنية التي تحمي على نطاق واسع معلومات المؤسسة الحساسة من سوء الاستخدام أو الوصول غير المصرح به أو التعطيل أو الإتلاف.

الأداء العام

يعتبر الأداء العام للمؤسسة المنظومة المحصلة المتكاملة لنتاج أعمال المنظمة في ضوء تفاعلاتها الداخلية والخارجية وهو بهذا المفهوم يشتمل على أبعاد ثلاثة هي. أداء الأفراد في وحدتهم التنظيمية؛ أداء الوحدات التنظيمية في الإطار العام للمنظمة؛ 13: أداء المؤسسة في إطار البيئة الخارجية الاقتصادية والاجتماعية والثقافية. (صيام، 2026)

التعريف الإجرائي: الأداء العام لمركز الطوارئ 933 يتعلق بالنتائج والإنجازات التي يحققها في مختلف المجالات والأبعاد. يشمل ذلك قدرة المركز على استخدام البنية التحتية المتاحة بفعالية وفاعلية في تنفيذ وإدارة العمليات الطارئة، بما في ذلك الأنظمة والتجهيزات التقنية والتدريب اللازم للموظفين. كما يتضمن الأداء العام تقييم مدى قدرة المركز على التعامل مع الحالات الطارئة بشكل سليم.

الكفاءة التشغيلية

تعرف الكفاءة التشغيلية بأنها العلاقة بين كمية الموارد المستخدمة والنتائج المحققة، من خلال تعظيم المخرجات أو تخفيض الكمية المستخدمة من المدخلات للوصول إلى حجم معين من المخرجات (إبريهي، 2019)

التعريف الإجرائي: الكفاءة التشغيلية تعبر عن الناتج الذي يمكن تحقيقه في المنظمات ما هو أكبر من مجموع المدخلات في عمليات الإنتاج وممكن استخدامها لغرض المقارنة مع الوحدات التنظيمية الأخرى في المنظمة من خلال قياس الانحرافات في الأداء لتلك الوحدات المتشابهة في العمل من خلال قياس كفاءة الوحدة الأفضل من غيرها.

مركز الطوارئ 933

مركز الطوارئ 933 هو مركز مختص بتقديم الخدمات الطارئة التابع لشركة الكهرباء السعودية. وهو المركز المخصص للتعامل مع الحالات الطارئة والمشاكل التقنية المتعلقة بتوزيع الكهرباء في المناطق المختلفة. يعمل هذا المركز على استقبال البلاغات والمكالمات ذات الصلة بانقطاع التيار الكهربائي، الحوادث الناتجة عن الشبكة الكهربائية، الأعطال التقنية، وأي مشاكل أخرى تتعلق بالكهرباء. ويقوم فريق العمل في مركز الطوارئ 933 بالتحرك الفوري لحل هذه المشاكل واستعادة الخدمة بأسرع وقت ممكن لضمان استمرارية توفير الكهرباء للمناطق المتأثرة.

2. الدراسات السابقة:

سيتم هنا عرض الدراسات السابقة ذات العلاقة بموضوع الدراسة.

أولاً: الدراسات العربية

1- دراسة البركى (2020) التي تدور حول واقع تطبيق متطلبات نظم إدارة أمن المعلومات المتوافقة مع المواصفة ISO 27001: 2005 بالمصارف العاملة بمدينتي بنغازي والبيضاء، وتعتبر هذه الدراسة تجسيدا وتأكيدا على مفاهيم جديدة في بيئة جديدة وهي متطلبات تطبيق نظم إدارة أمن المعلومات المتوافقة مع المواصفة ISO 2005 : 27001 والمعروفة اختصارا ب (ISMS)، في قطاع المصارف في ليبيا، حيث هدفت هذه الدراسة إلى التعرف على واقع تطبيق متطلبات نظم إدارة أمن المعلومات، في خمسة (5) من المصارف العاملة بمدينتي بنغازي والبيضاء، و أوضحت نتائجها أن واقع تطبيق متطلبات نظم إدارة أمن المعلومات جاء بدرجة متوسطة التطبيق بالمصارف المبحوثه، وأوصت الدراسة بإنشاء إدارة تتم بمجال أمن المعلومات داخل المصارف المبحوثه، بالإضافة إلى نشر الوعي بأمن المعلومات وأهميته لجميع الموظفين.

2- دراسة (Bogale, et al ,2019) هدفت هذه الدراسة إلى التعرف على واقع الممارسة الفعلية المتعلقة بخلق الوعي بأمن المعلومات في بنك ENAT في أثيوبيا، وأوضحت نتائجها أن مستوى الوعي بأمن المعلومات غير مرضي لدى الموظفين، كما أن البنك لا يوجد لديه إجراءات منظمة بشكل جيد في حالة الهجمات الإلكترونية، وتنظيم الشبكات اللاسلكية وغيرها من تنفيذ وإدارة أمن المعلومات ليست بصورة جيدة، واقترح الباحثون برنامجا من شأنه مساعدة البنك فيما يتعلق بخلق الوعي بأمن المعلومات والممارسات الجيدة لموظفيه التعزيز موقفه الأمني.

3- دراسة (فيلالي ويحياوي، 2019: 361 -362) تناولت هذه الدراسة أمن المعلومات من زاوية إدارة المخاطر نجد أن (شركة ألجيريا ديجيتال تراندس للتوجهات الرقمية،2018) قامت بالاشتراك مع مؤسسة " رابيد 7" الرائد العالمي في قطاع إدارة المخاطر، بدراسة احصائية شملت أكثر من 1000 مؤسسة جزائرية، وأوضحت نتائجها أن المؤسسات الجزائرية لا تزال بعيدة عن المقاييس المفترضة في مجال استخدام التدابير الأمنية، وتبين أن 47% من المؤسسات الجزائرية موضوع الدراسة اعترفت بانعدام أي حماية لنظامها من الهجمات الالكترونية، كما أن 52% من المؤسسات صرحت بأنها لا تمتلك سياسة لحماية المنظومات المعلوماتية، ولا موظفين متخصصين ومؤهلين في مجال تقنيات الاتصالات، كما تبين أن 57% من المؤسسات لا تستضيف بياناتها لدى (Servers) خوادم حواسيب جزائرية.

4- تم دراسة القحطاني (2018) كان الهدف الأبرز للدراسة هو تحديد السياسات التي ستوفر الحماية لنظم المعلومات في جامعة الأميرة نورة, والتي تتناسب مع الثقافة الفريدة للمملكة العربية السعودية, ولتحقيق هذا الهدف وُضعت أهداف ثانوية منها تنفيذ المقابلات والمسوحات بهدف تحديد ماهية الحالة الراهنة لأمن تكنولوجيا المعلومات في الجامعة, بالإضافة إلى التعرف على الحواجز الثقافية والقانونية المحددة أمام أمن المعلومات، وقد استخدمت الباحثة المنهج الوصفي ,في حين اعتمدت المقابلة الشخصية والاستبيان كأدوات في تجميع بيانات الدراسة, في حين كانت أبرز النتائج التي توصلت لها أن معظم العاملين في المؤسسات والجامعات في المملكة العربية السعودية لا يشاركون في تطوير أي سياسة لأمن المعلومات, وبالتالي فهم لا يدركون تماماً أهمية أمن المعلومات. في حين خرجت الدراسة بعدد من التوصيات منها أهمية وضع المنظمات سياسات واضحة فيما يتعلق بتعامل العاملين مع البيانات الحساسة وفقاً لتصنيف البيانات، كما يفضل أن يُدرَب العاملين على كيفية الحذر في التعامل مع الرسائل الإلكترونية المريبة التي يتلقونها عبر التطبيقات كالبريد الإلكتروني أو التطبيقات الاجتماعية كتطبيق الواتساب وغيرها، مع تشجيع العاملين على الإبلاغ السريع عن أية حوادث إلكترونية متعلقة بأمن المعلومات.

5- وفي دراسة الحمر (2018) حول تحسين عمليات أمن المعلومات لدى المؤسسات القطرية من خلال تطوير إطار شامل لإدارة أمن المعلومات قابل للتطبيق، مع مراعاة ثقافة قطر وبيئتها، بالإضافة إلى تعزيز الوعي والثقافة المعلوماتية. واستخدمت الدراسة المنهج الوصفي كما قامت بتجميع بيانات الدراسة عن طريق المقابلات والاستبيان , وتوصلت الدراسة إلى نتائج من أهمها عدم كفاية الوعي الأمني بالمعلومات في المنظمات في قطر، بالإضافة إلى عدم توفر موظفين متخصصين في أمن المعلومات , وانعدام الثقافة الأمنية، في حين كانت أبرز التوصيات المطالبة بتجنب تطبيق الضوابط الإلزامية لأمن المعلومات بمستوى واحد على كافة المنظمات دون مراعاة لحجمها وقيمة أصولها المعلوماتية ,كما أنه من الإيجابي السماح بمزيد من المرونة في اختيار عناصر التحكم في تدابير أمن المعلومات .

6- دراسة الذنيبات (2018) بعنوان " الممارسة الفاعلة لإدارة أمن المعلومات في المنظمات الحكومية السعودية وفقاً للمواصفة ISO / IEC 27002 : 2013". هدفت الدراسة إلى الكشف عن واقع نظام إدارة أمن المعلومات المطبق في المنظمات الحكومية السعودية بالتركيز على دراسة حالة جامعة الطائف، وتحديد مدى امتثالها للمواصفة الدولية (ISO/ IEC27002:2013) ثم تحديد ما هي الخطوات الواجب اتخاذها من قبل الجامعة لتحسين ممارسة إدارة أمن المعلومات، اعتمدت الدراسة على تصميم البحث المختلط، حيث تم استخدام طرق البحث النوعي المتمثلة بالمقابلات والملاحظة المباشرة وفحص الوثائق، توصلت الدراسة إلى عدد من النتائج كان من أهمها:1-\tتطبق الجامعة نظاما محددا لإدارة أمن المعلومات وهو نظام ISO/ IEC.2-\t 27001 تمتثل الجامعة بمستوى متوسط للممارسات التنظيمية والإدارية لأمن المعلومات وفقا للمواصفة العالمية 27002:2013

ISO/IEC.3-\tحددت الدراسة الضوابط الأمنية والممارسات الأمنية التي تحتاج لتحسين في سبيل تحسين جاهزية الجامعة لتطبيق سياسات أمن المعلومات.

7- كما هدفت دراسة تادرس (2017) إلى الكشف عن مخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها على مختلف مستوياتهم الإدارية، واقتراح أهم السبل لمواجهتها. استخدام المنهج الوصفي التحليلي في هذه الدراسة لاستنباط النتائج باستخدام عينة عشوائية بسيطة مكونة من [225] موظفا، وبعد أن عولجت البيانات التي وردت في الاستبانة باستخدام الأساليب الإحصائية المناسبة، توصلت الدراسة إلى أن الدرجة الكلية لمخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البقاء كما يراها موظفوها (متوسطة) بمتوسط حسابي [3.40]. حيث جاء (مخاطر الأفراد) في المرتبة الأولي تلاه في المرتبة الثانية (مخاطر العمليات) بينما جاء (مخاطر البيانات) في المرتبة الأخيرة. وأشارت النتائج أن أهم سبل التغلب على هذه المخاطر هو (تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمان نظام المعلومات). وأوصت الدراسة اتباع بعض الإجراءات الأمنية اللازمة لإحكام أمن المعلومات خصوصا في ظل ارتباط الشبكة المحلية بشبكة الإنترنت؛ ومن تلك الإجراءات تقنية الحوائط النارية والتشفير ودعم أجهزة عدم انقطاع التيار الكهربائي، توفر عدد كاف من موظفي الحماية ممن يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية، وتوفر وصف وظيفي للوظائف المتعلقة بالحماية والأمان مع تشكيل اللجان والمجالس المطلوبة لتيسير إجراءات العمل في مجال أمن المعلومات.

8- دراسة الشمالي (2017) هدفت هذه الدراسة إلى تعرف أمن المعلومات وسريتها وأثرها في الأداء المصرفي في البنوك العاملة في الأردن، وقد تكون مجتمع الدراسة من البنوك العاملة في الأردن، وأخذت عينة عشوائية طبقية متناسبة بنسبة 50% من مجتمع الدراسة. أظهرت نتائج الدراسة أن مستوى ممارسة أمن المعلومات وسريتها في البنوك العاملة في الأردن من حيث الأهمية النسبية كانت مرتفعة، إذ بلغ المتوسط الحسابي (4.11)، كما تبين أن الأهمية النسبية للأداء المصرفي في البنوك العاملة في الأردن كانت مرتفعة، إذ بلغ المتوسط الحسابي (4.07). وبينت نتائج الدراسة وجود أثر ذي دلالة إحصائية لأمن المعلومات وسريتها (الحماية المادية، حماية الأفراد، الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن. وأخيرا توصلت الدراسة إلى عدد من التوصيات منها ضرورة أن تقوم إدارة البنوك بالممارسات العملية اللازمة لنشر أمن المعلومات وسريتها وتعميق ثقافتها في مختلف المستويات الإدارية عن طريق إعداد البرامج التدريبية لجميع المستويات الإدارية، وضرورة زيادة الإنفاق على برامج أمن وسرية المعلومات والسعي للحصول على الشهادات العالمية المطابقة لأنظمة المعلومات الدولية

9- وأشارت دراسة العتيبي (2013) إلى مدى العلاقة بين أمن نظم المعلومات وإبداع موظفي شركة الاتصالات السعودية، على وجه الخصوص، يعتقد البعض أن أدوات وأساليب ممارسة أمن نظم المعلومات تشكل قيودًا على العاملين وتقتل إبداعهم، وتكون مجتمع الدراسة من العاملين في مبيعات كبار العملاء ومبيعات قطاع الأعمال في وحدة قطاع الأعمال بالشركة والبالغ عددهم 599 موظف بالسعودية، وكان منهج الدراسة المتبع هو المنهج الوصفي. وقد استخدم الباحث الاستبيان كأداة دراسة، وكانت وأهم النتائج أن أفراد العينة يتفقون مع واقع أمن نظم المعلومات، كما أنهم مبدعون ومرنون، وهناك علاقة مباشرة بين أمن المعلومات. مستوى إبداع النظام والعاملين. كما خلصت الدراسة إلى عدم وجود فروق ذات دلالة إحصائية حول محور الإبداع باختلاف الوظيفة، بالمقابل هناك فروق ذات دلالة إحصائية حول محور أمن نظم المعلومات باختلاف الوظيفة وهي أكبر لدى الموظف أهم التوصيات تعزيز ودعم وجود الكوادر الوطنية الموثوقة للعمل في مجالات أمن نظم المعلومات بشركة الاتصالات السعودية، العمل على نشر الوعي لجميع الأطراف ذات العلاقة داخل الشركة وخارجها من عاملين ومستفيدين.

ثانياً: الدراسات الأجنبية

1- دراسة (Mui, 2023) هدفت هذه الدراسة إلى فهم تجارب العاملين، الذي قاموا بتغيير حالة عملهم من العمل الشخصي إلى العمل عن بعد، مع سياسات أمان المعلومات والعلاقات داخل المؤسسات، ومدى امتثالهم لسياسات أمان المعلومات. تم استخدام إطار نظري مبني على نظرية السلوك المخطط (TPB) لاستكشاف تأثيرات السلوك على الموظفين، ونظرية الروابط الاجتماعية (SBT) لمعالجة قوة العلاقات وتأثير الامتثال. استخدمت هذه الدراسة المنهج البحثي الكيفي لإجراء مقابلات مع المشاركين، سواء كانوا يعملون في الوجه الشخصي أو عن بعد، لجمع البيانات. وقد شملت التجارب الحياتية للمشاركين تجاربهم مع تنفيذ وتطبيق سياسات أمان المعلومات في المؤسسة، وثقافتها المؤسسية، وتأثيرات قادة الرأي على تشكيل الامتثال لهذه السياسات، بالإضافة إلى وضوح وتدريب سياسات أمان المعلومات للموظفين. من بين العوامل الرئيسية التي أثرت على امتثال المشاركين لسياسات أمان المعلومات، سواء كانوا يعملون في الوجه الشخصي أو عن بعد، كانت الأتمتة والأوقات المزدحمة والكفاءة والتوفر والتدريب وتطبيق سياسات أمان المعلومات. بشكل عام، أفاد المشاركون في الدراسة بوجود علاقات إيجابية داخل مؤسستهم، بغض النظر عن طبيعة عملهم، ولكن لاحظ معظمهم أن بناء العلاقات كان أسهل في الوجه الشخصي مقارنة بالعمل عن بعد، رغم أن التكنولوجيا ساهمت في تقليل بعض هذه الفجوة بين العملين.

2- دراسة (Burton Venessa ,2018) هدفت الدراسة إلى التعرف على الصعوبات التي تواجه المدراء المتخصصين بأمن المعلومات، استخدمت الدراسة المنهج النوعي وأسلوب المقابلات، وتضمنت عينة الدراسة (10) مدراء في ولاية واشنطن في امريكا، وتوصلت الدراسة إلى ضعف التشريعات المتبعة في حماية المعلومات والبيانات على شبكة الانترنت وضعف فاعلية الأنظمة الأمنية. تأخرها عن مواكبة طرق الاختراق المتطورة. وأوصت الدراسة إلى ضرورة تطوير القوانين بما يواكب الجرائم والاختراقات السيبرانية.

3- دراسة (Okoye,2017) : هدفت إلى استكشاف استراتيجيات القادة في الشركات الصغيرة والمتوسطة (SME) للحد من آثار تهديدات أمن المعلومات على أداء الأعمال، وذلك بناءً على قلق القادة التجاريين في نيجيريا من معدلات الفشل في الأعمال والخسائر الاقتصادية الناتجة عن حوادث الأمن، والتي قد لا يفهمون استراتيجيات لتقليل تأثيرات تهديدات أمن المعلومات على أداء الأعمال. وقد اعتمدت الدراسة على نظرية الأنظمة العامة ونظرية القيادة التحويلية. تم تنفيذ مقابلات شبه هيكلية مع 5 قادة من الشركات الصغيرة والمتوسطة العاملة في قطاع صناعة النفط والغاز في بورت هاركورت، نيجيريا، والذين لديهم خبرة لا تقل عن 2 سنة في دور قيادي، ولديهم استراتيجيات ملموسة لتقليل تأثيرات تهديدات أمن المعلومات في شركة SME. أظهر تحليل الموضوعات لمحتوى المقابلات وجود 10 استراتيجيات للحد من تأثيرات تهديدات أمن المعلومات، وهي: أمان الشبكة، والأمان البدني، وسياسة كلمات المرور القوية، وحماية مكافحة الفيروسات وتحديث البرمجيات، وسياسة أمن المعلومات، والتدريب والتوعية بالأمان، ورصد أمان الشبكة والتدقيق، واكتشاف الاختراق، ونسخ البيانات الاحتياطية، وإدارة الموارد البشرية. يمكن أن تُسهم النتائج في التغيير الاجتماعي من خلال تزويد قادة الشركات الصغيرة والمتوسطة بمزيد من الفهم حول الاستراتيجيات لتقليل تأثيرات تهديدات أمن المعلومات على أداء الأعمال، مما قد يؤدي إلى تحسين الأداء التجاري وزيادة تدفق الأموال إلى الاقتصاد المحلي وتقديم خدمات اجتماعية للمقيمين.

4- دراسة (Francois,2016): هدفت إلى تقديم تقييم كمّي للعوامل التي قد تؤدي إلى عدم فعالية برنامج أمن المعلومات في المؤسسات، من خلال استكشاف العلاقة بين الوعي بسياسات أمن المعلومات وتنفيذها وصيانتها، وفعالية البرنامج بشكل عام.

استخدمت الدراسة أداة استبيان بمقياس ليكرت من 5 نقاط، ونُفذت عبر بوابة الويب باستخدام خدمة Survey Monkey Audience، وتم جمع البيانات من 119 متطوعًا. تم طرح أسئلة تتعلق بفعالية برنامج أمن المعلومات في منظماتهم، ووعيهم بالسياسات، وتطبيقهم لتلك السياسات، وصيانتها. شملت العينة المؤسسات التي تعتمد بشكل كبير على تقنيات المعلومات في أنشطتها اليومية، وقدمت 119 متطوعًا للمشاركة في الدراسة. أظهرت النتائج أن الوعي بسياسات أمن المعلومات وتطبيقها وصيانتها له دورًا مهمًا في تحقيق فعالية برنامج أمن المعلومات في المؤسسات. وتبين أن متوسط الوعي بالسياسات ومتوسط تطبيق السياسات ومتوسط صيانة السياسات هم متغيرات متنبئة ذات دلالة إحصائية لفعالية البرنامج الإجمالية. بناءً على النتائج، يُوصى بتعزيز وعي الموظفين بسياسات أمن المعلومات وتعزيز تطبيقها وصيانتها كجزء أساسي من برامج أمن المعلومات في المؤسسات، للمساهمة في تحسين فعالية هذه البرامج وتقليل حالات انتهاكات أمن المعلومات.

5- دراسة (KELEMIE TEBKEW YIRDAW,2013)وقد جاءت هذه الدراسة تحت عنوان: " إدارة أمن المعلومات في البنوك الصناعية في أثيوبيا "، وعالجت هذه الدراسة إشكالية واقع أمن نظم المعلومات في القطاع البنكي الإثيوبي في ظل التحديات والتهديدات المتأتية من خلال التطور الكبير في قطاع الاتصالات التي تعتبر الوسط الحيوي نشاط هذه البنوك، وكان مجتمع الدراسة مكون من 20 بنك خاص وعام في إثيوبيا، أما العينة فتكونت من 5 بنوك لسنة 2013، واستعمل الباحث 3 طرق لجمع المعلومات: الاستبيان، تحليل الوثائق والمقابلة، واستطرد الباحث في تحليل البيئة التكنولوجية والاجتماعية وقد حاول ربط ذلك بعلاقة الأمن بالمعاملات البنكية، ليخلص في الأخير إلى أن الأمن أصبح مكوناً أساسي في النظام البنكي، ووجد مدى اهتمام البنوك به، وأوصى أن يعمم هذا الاهتمام على القطاعات الأخرى غير البنكية .

التعليق على الدراسات السابقة

من خلال عرض الدراسات السابقة، تبين أن هناك أوجه تشابه وأوجه اختلاف في جوانب كثيرة، كان أهمها: - من ناحية الموضوع، معظم الدراسات اشتركت في موضوع واحد وهو أمن نظم المعلومات مع اختلاف في قطاع التطبيق فبعضها اختار الشركات وبعضها اختار البنوك، ومن ناحية الهدف: اشتركت معظم الدراسات في هدف واحد وهو تقييم أمن نظم المعلومات في قطاعات مختلفة، وتحديد ما هي المخاطر وما هي الإجراءات الواجب اتخاذها أو مدى فعالية الإجراءات المتخذة؛ - من ناحية العينة: كان مجتمع الدراسة هو مجموع العاملين على نظم المعلومات سواء كانوا مستغلين للنظام أو الموظفين الذين يوفرون الدعم، وكانت العينة مختارة من هذا المجتمع؛ - الحد الزماني: هناك تباين زماني بين الدراسات، حتى ولو لم يكن كبير، إلا أن معامل الزمن في عالم التكنولوجيا يعتبر مهم جدا، كون هذا القطاع يشهد تطور متسارع، يستوجب في كل مرة مراجعة طرق وأساليب أمن نظم المعلومات، وقد قمنا باختيار مركز الطوارئ 933 لتطبيق دراستنا الحالية.

لذا نرى أنه توجد فجوة بحثية، في تناول موضوع تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 لذلك سوف تتناوله الدراسة ليكون مشكلة للبحث.

واتفقت هذه الدراسة بأنها تهدف إلى تعرف أثر سياسات أمن المعلومات إذ هناك دراسات عربية وأجنبية كثيرة تناولت هذا الموضوع، وتختلف هذه الدراسة من حيث مجتمع الدراسة فهي ربطت ما بين أمن المعلومات وأثرها على الأداء العام والكفاءة التشغيلية في مركز الطوارئ 933.

ما يميز الدراسة الحالية عن الدراسات السابقة:

- تناولها تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933.

- أهمية سياسات أمن المعلومات في المؤسسات حيث تمثل النظام العصبي لها.
- تحديد مشكلة الدراسة.

استخدمت هذه الدراسة دراسات ومراجع حديثة، العربية والأجنبية منها للاستفادة منها في الإطار النظري، مما سهل علينا من الحصول على معلومات ومفاهيم حديثة وبكثرة للدراسة ومتغيراتها، وفي رؤية أوضح وأحدث لهذه المفاهيم (الأمر الذي أثرى الدراسة الحالية من الناحية النظرية وهذا الميزة لم تتوفر في الدراسات السابقة .

3. الإطار النظري:

المبحث الأول: سياسات أمن المعلومات

1- مفهوم نظام أمن المعلومات:

المقصود بأمن المعلومات هو حماية المعلومات والعناصر الهامة ذات الصلة، بما في ذلك النظم والأجهزة التي تستخدم هذه المعلومات وتقوم بتخزينها ونقلها من أي اعتداء يقع عليها بقصد أو بدون قصد، ويشتمل أمن المعلومات على مجالات متعددة مثل الأمن الإداري أو التنظيمي، وأمن الأجهزة والبرامج، وأمن الشبكات. (Whitman and Mattord, 2013: 24)

أي أن أمن المعلومات يشمل الحفاظ على المعلومات وعناصرها بما في ذلك الأجهزة والمعدات المستخدمة في حفظ ونقل المعلومات. ولتحقيق أمن المعلومات يجب الأخذ بعين الاعتبار سياسة الأمن، أمن الأجهزة والمعدات، أمن الشبكات، والأمن القانوني (Whitman and Mattord,2011).

كما عرف نظام أمن المعلومات على أنها "العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغرض تحقيق سلامتها وتوافرها وسريتها وفق الصلاحيات والترتيبات المتعارف عليها". (الدنف،2013: 33)

ووضح أبو ذويب (2019) أن أمن المعلومات هو الأمن الذي يهتم بحماية المعلومة ومواردها من التهديدات والمخاطر التي قد تتعرض لها. وأضافت بطارسة (2019) أن أمن المعلومات يجب أن يغطي جميع موارد المعلومات على الشبكات السلكية واللاسلكية. ويساعد في ذلك استخدام تقنيات ووسائل على درجة عالية من الحماية تهدف إلى ضبط أنظمة المعلومات من الدخول غير المصرح بجميع أشكاله (مولود، واخرون، 2017).

عرفته لجنة أنظمة الأمن القومي الأمريكية (CNSS) بأنه: " حماية المعلومات وعناصرها المهمة (الحرجة) بما في ذلك الأنظمة والأجهزة التي تستخدم وتخزن وترسل هذه المعلومات " (طارش، 2015: 37).

إن مفهوم أمن المعلومات مشتق من الخصائص الأساسية لأمن المعلومات، ولكن هنا يجب توضيح الفرق بين أمن المعلومات وأمن تكنولوجيا المعلومات والاتصالات.

وضح المركز القومي لأمن المعلومات (2010) أن أمن تكنولوجيا المعلومات والاتصالات هو جميع الجوانب ذات العلاقة بتحقيق وتوضيح والحفاظ على السرية والنزاهة والتوافرية والموثوقية لمصادر المعلومات. وأكد القحطاني (2015) أن أمن تكنولوجيا المعلومات والاتصالات هو الذي يتعلق بحماية أنظمة المعلومات، وأنظمة الحصول عليها. ويتعدى أمن تكنولوجيا المعلومات والاتصالات ليشمل جوانب البنية التحتية والتقنية في منظمات الأعمال.

يهدف أمن المعلومات في الأساس إلى حماية المعلومات والبيانات من التهديدات والحوادث الناجمة عن أخطاء الأجهزة والبرمجيات والأحداث الطبيعية والأحداث المتعمدة وغير المتعمدة من الأشخاص أو الإهمال، وكذلك الحماية من الوصول غير الشرعي وحصر ذلك فقط في الأشخاص المصرح لهم بذلك؛ وهذا ما يعرف بمثلث الحماية -confidentiality (CIA) integrity- Availability حيث حددت عناصر أمن المعلومات بثلاثة عناصر رئيسية هي: السرية، التوفر، السلامة .(Peltier, 2014,p53)

2- أهمية نظام أمن المعلومات:

ازداد استخدام الحاسوب في إدارة أعمال الأفراد في شئون حياتهم وكلما ازداد استخدام الحاسوب والاعتماد عليه ازدادت التهديدات وظهرت الحاجة إلى حماية البيانات الخاصة به التي قد يؤدي فقدانها أو تغييرها أو مجرد الاطلاع عليها إلى نشوء تهديد مباشر على الممتلكات أو حتى حياة صاحبها وتعتبر أهمية أمن المعلومات بالمقام الأول ونظرا لأن المعلومات هي الهدف والغاية لأغلب السرقات وفي ضوء ما تتعرض له دوماً من تهديدات واختراقات فإنه لابد من توفير الأمن والحماية لهذه المعلومات من الأخطار، وتعد المعلومات في عصر المعلوماتية من أكثر الأسلحة انتشارا و فعالية وتأثيره وسرعة ولذلك لابد من توفير أمن وحماية لهذه المعلومات. (صلاح الدين، 2005)

3- عناصر أمن المعلومات:

تشمل عناصر أمن المعلومات السرية أو الموثوقية والتكاملية وسلامة المحتوى واستمرارية توفير المعلومات والخدمة. (عوض الله،2017)

1. **السرية أو الموثوقية confidentiality**: وتعني التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين لذلك.
2. **التكاملية وسلامة المحتوى integrity**: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى او تغيره او العبث به في أي مرحلة من مراحل المعالجة او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات او عن طريق تدخل غير مشروع.
3. **استمرارية توفر المعلومات او الاتاحة Availability**: التأكد من استمرار عمل النظام المعلوماتي واستمرار والقدرة على التفاعل مع المعلومات وتقديم الخدمة المواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها او دخوله إليها.

4- مستويات أمن المعلومات:

يتم تحديد مستويات أمن المعلومات وتشمل الحماية المادية والإدارية وحماية المعلومات الإعلامية والمعرفية، وسوف نستعرضها بإنجاز فيما يلي:

1. **الحماية المادية**: تحتوي على جميع الوسائل التي تمنع الوصول إلى نظام المعلومات وقواعدها كالأقفال والحواجز التي تحد من الوصول إلى الأجهزة الحساسة.
2. **الحماية الشخصية**: وهي تشمل موظفين يعملون على الأنظمة التقنية ذات الصلة، وهم بحاجة إلى توفير وسائل تحديد الهوية لكل موظف، وتوفير التدريب والتأهيل للأفراد المشاركين في الأساليب الأمنية، بالإضافة إلى الوعي بالمسائل الأمنية ومخاطر المعلومات المتعلقة بالهجمات.

3. **الحماية الإدارية**: تهدف إلى سيطرة السلطة الإدارية المسؤولة عن نظام المعلومات وقواعده، مثل التحكم في البرامج الخارجية أو الخارجية من المنشأة، والتحقق من الانتهاكات الأمنية.
4. **الحماية الإعلامية المعرفية**: كما في السيطرة على المعلومات وعملية مصادر المعلومات الحساسة حول القرار حول عدم استخدامها. (عوض الله،2017)

5- نظام إدارة أمن المعلومات:

تعددت وتنوعت الآثار السلبية الناتجة عن حوادث أمن المعلومات والأضرار التي تقع على المنظمات مثل تعطيل العمليات الداخلية والاتصالات وفقدان الميزة التنافسية والآثار السلبية على سمعة المنظمة وحسن نواياها وقتها، ونتيجة لذلك أصبحت إدارة أمن المعلومات وظيفة مطلوبة في كل منظمة ويكاد أن يكون من المستحيل تسيير أعمال أي منظمة بدون نظم معلومات أمنة ((Qingxiong,et al, 2008

تتحقق الإدارة الفعالة لأمن المعلومات من خلال تنفيذ مجموعة مناسبة من الضوابط تسري على تطبيقات تكنولوجيا المعلومات والاتصالات، ويتعين وضع هذه الضوابط وتنفيذها ومراقبتها ومراجعتها وتحسينها باستمرار، إذ يمكن أن يؤدي التقاعس عن وضع وتطبيق ضوابط أمنية فعالة إلى عجز المنظمة عن تحقيق أهدافها الأمنية والتجارية أو الخدمية. (Alnatheer and Nelson,2009)

نتيجة لذلك فقد تم وضع نظم عامة لإدارة أمن المعلومات كجزء من النظام العام لإدارة تقنية المعلومات وحكومتها، حيث تتضمن هذه النظم مجموعة من المعايير والإرشادات العامة التي تساعد في توفير الحماية اللازمة للمعلومات ينبغي الالتزام بها وتطبيقها حرفياً في بيئة التعاملات الإلكترونية.

(Information Security Forum,2007, https://www.securityforum.org/,25/3/2021)

نظام إدارة أمن المعلومات هو جزء من النظام العام للمنظمة، يتناول عادة. سلوك الموظف وعملياته، فضلا عن البيانات والتكنولوجيا. ويمكن أن يكون موجها نحو نوع معين من البيانات، مثل بيانات العملاء، أو يمكن تنفيذه بطريقة شاملة تصبح جزءا من ثقافة المنظمة، ويعرف بأنه "مجموعة من السياسات والإجراءات لإدارة البيانات والمعلومات الحساسة والمنظمة بشكل منهجي، بهدف تقليل المخاطر وضمان استمرارية الأعمال من خلال الحد من تأثير الخرق الأمني بشكل استباقي". (whatIs.com-28-3-2021).

يقدم نظام إدارة أمن المعلومات نموذجا لحماية الأصول المعلوماتية لتحقيق أهداف الأعمال على أساس من إدارة المخاطر وتجنبها أو التقليل من حدتها، وتحديد المستويات المقبولة من المخاطر المعلوماتية، كما يتضمن تحليل متطلبات حماية الأصول المعلوماتية وتطبيق الضوابط المناسبة لضمان حماية هذه الأصول. (يحياوي، 2011)

6- أمن المعلومات في المنظمات الحكومية في المملكة العربية السعودية:

سعت المنظمات الحكومية في المملكة العربية السعودية كغيرها من المنظمات نحو تحقيق الاستثمار الأمثل في تكنولوجيا المعلومات منذ نهاية القرن الماضي، حيث قامت بتطوير العديد من نظم المعلومات لتسيير أعمالها وتقديم الخدمات للمواطنين شملت جميع القطاعات الصحية والتعليمية والخدمية ...الخ، سواء كانت نظم معلومات تشغيلية أو إدارية أو استراتيجية، وفي مجالات وظيفية مختلفة موارد بشرية، مالية، محاسبية، إنتاجية. الخ.

وبالرغم من تبني المنظمات الحكومية السعودية لتطبيقات تكنولوجيا المعلومات مبكرة، وتسخيرها التسيير الأعمال وتقديم الخدمات، إلا أن الاهتمام بوضع وتطبيق المعايير والمواصفات الخاصة بأمن المعلومات قد تأخر كثيرا، وفي الآونة الأخير بدأ التفكير الجاد في هذا الأمر إدراكا لأهميته وضمانة لنجاح مشاريع الحكومة الإلكترونية والتي تعتمد أساسا على معايير ومواصفات عالمية حيث صدرت الاستراتيجية الوطنية لأمن المعلومات في مطلع عام 2011 (وزارة الاتصالات وتقنية المعلومات، 2011)

صدرت هذه الاستراتيجية بعد صدور الأمر الملكي رقم (40) تاريخ1427/2/27هـ الموافق2006/03/27م، بشأن إقرار ضوابط تطبيق التعاملات الإلكترونية الحكومية في الجهات الحكومية والتي كان من بينها " أن تقوم كل جهة حكومية بحماية معلوماتها وبياناتها وأنظمتها المعلوماتية وفق المعايير العالمية ذات العلاقة، وحسب معايير استرشاديه يعدها البرنامج لهذا الغرض ".

وأيضا في عام (2011 م) أصدرت هيئة الاتصالات وتقنية المعلومات الطبعة الأولى من وثيقة إطار سياسات وإجراءات أمن المعلومات والتي تضمنت الدليل الإرشادي لسياسات وإجراءات أمن المعلومات للجهات الحكومية السعودية. (هيئة الاتصالات وتقنية المعلومات، 2011)

كما صدر قرار مجلس الوزراء رقم (185) تاريخ6/9/ 1433 والمتعلق بأمن المعلومات والاتصالات في الجهات الحكومية، وقد ألزم القرار كل جهة أن تقوم بإنشاء وحدة إدارية مختصة بأمن المعلومات عليها متابعة تنفيذ السياسات الأمنية المعتمدة ووفقا للمعايير المحلية والدولية في مجال أمن المعلومات.

تم تطوير الدليل الإرشادي لسياسات وإجراءات أمن المعلومات للجهات الحكومية السعودية لاستخدامه من قبل الجهات الحكومية لتحديد احتياجاتها الأمنية، ولاستخدام منهجية مبنية على المخاطر لتطوير سياسات وإجراءات أمن المعلومات لديها، وكذلك يساعد في انتقاء الخيار المناسب لوضع إدارة أمن المعلومات ضمن الهيكل التنظيمي للمنظمة. (الدليل الإرشادي لأمن المعلومات، 2011).

كما يشتمل الدليل على عدد من المكونات من بينها وثيقة عملية لآلية تطوير سياسات وإجراءات أمن المعلومات ووثيقة عملية لآلية تنفيذ هذه السياسات والإجراءات، ووثيقة خيارات تحديد موقع إدارة أمن المعلومات في الهيكل التنظيمي، كما يشتمل على قاعدة بيانات للسياسات والإجراءات.

المبحث الثاني: الأداء العام

يستكشف هذا المبحث مفهوم الأداء وعوامل تأثيره وأهميته في بيئة العمل.

1- مفهوم الأداء العام

يعرف الأداء العام بأنه نظام شامل يشمل كل مستويات الإدارة وأنشطتها، وهدفه الرقي بالأداء إلى مستويات عالية تتفوق على المنافسين، وتصل إلى المستوى العالمي، ويحقق ذلك من خلال مجهود مختلف العاملين، كما أن من المهم المحافظة مستوى الأداء الذي تم التوصل إليه وتنميته باستمرار. (الحسيني، 2019) وكذلك يتم تعريف أداء المنظمة على أنه مدى نجاح الفرق المنظمة (الوحدات الإدارية) أو مجموعة الأشخاص في أداء وظيفة معينة. يقال إن أداء المؤسسة مرتفع عندما تعمل جميع مكونات وأجزاء المؤسسة معًا لتحقيق النتائج، والتي يمكن قياسها في سياق القيمة المقدمة للعميل (Masa’deh et al, 2018).

كما أن الأداء هو قدرة المنظمة على تحقيق أهدافها، من خلال التركيز على الأداء المؤسسي. كما ويشير الأداء المؤسسي إلى المصطلح الذي ينشأ للتمييز بين الإدارة على مستوى الفرد والمؤسسة، ويتطلب الأداء المؤسسي أن يتم وضع هذه العملية بما يتماشى مع تطوير بيئتهم، من أجل السماح بتطوير المنظمة ونظام إدارتها.(Felizardo e al., 2017, p. 9)

ونستطيع تعريف الأداء العام على أنه مصطلح يُستخدم لوصف مجموع النتائج والإنجازات التي تحققها المؤسسة أو الجهة في مجال عملها بشكل عام، والتي تعكس فعالية وكفاءة أدائها في تحقيق أهدافها ومهامها المحددة. يتضمن مفهوم الأداء العام العديد من العناصر، مثل الجودة، والكفاءة، والفعالية، والفاعلية، والاستجابة السريعة، والابتكار، والمرونة، وغيرها، بحيث يتم تقييم الأداء العام على أساس مجموعة متنوعة من المؤشرات والمعايير التي تعكس هذه الجوانب المختلفة من الأداء.

2- أهمية الأداء

يعد تحقيق أهداف المنظمة انعكاسا لأداء الأقسام أو المنظمة ذاتها كوحدة واحدة فهو يعد أيضا انعكاس لأداء الإفراد العاملين في تلك الأقسام أو المنظمة والذي يعد من العوامل الأساسية في تحقيق هدف المنظمة الذي وجدت من أجله (عذارى، 148:2013). لذلك يقع ضمن توجهات البحث الحالي الاعتقاد بأن دراسة الأداء العام سواء على مستواه الفرعي أو الإجمالي سيمكننا من تشخيص قدرات ومهارات ومعرفة الإفراد العاملين في المنظمة أو الأقسام المكونة لها وتحين الموجود منها وإدخال ما هو جديد وبما يسهم في تحسين الأداء.

3- العوامل المؤثرة في الأداء العام

هناك العديد من العوامل التي قد تؤثر على الأداء العام لأي منظمة أو مؤسسة، ومن بين هذه العوامل:- (عذاري،2013)

- استخدام التكنولوجيا وتوفر البنية التحتية المناسبة يمكن أن يحسن من كفاءة العمل ويزيد من الإنتاجية.
- جودة التخطيط والاستراتيجية التي تتبعها المؤسسة تلعب دورًا حاسمًا في تحديد اتجاهاتها وتحقيق أهدافها.
- كفاءة القيادة ومهارات الإدارة تؤثر بشكل كبير على الأداء العام، حيث تقود القيادة القادرة والمؤهلة المؤسسة نحو التحقيق والتفوق.
- مستوى كفاءة وتدريب الموظفين يؤثر بشكل كبير على قدرتهم على تحقيق الأداء العالي.
- فعالية العمليات الداخلية والإجراءات العملية تسهم في تحقيق الأداء العام الممتاز.
- تأثير التغييرات في البيئة الخارجية والسوقية يمكن أن يؤثر بشكل كبير على الأداء العام للمؤسسة.
- توفر الموارد المالية والبشرية الكافية والمناسبة تعزز من قدرة المؤسسة على تحقيق الأداء العالي.
- الثقافة التنظيمية وقيم المؤسسة تلعب دورًا مهمًا في تشجيع التعاون والابتكار وتحسين الأداء العام.

ونرى أن الأداء العام يتأثر بجملة من العوامل التي تشمل الإدارة والقيادة، والثقافة التنظيمية، والموارد البشرية، والعمليات الداخلية، والتكنولوجيا والبنية التحتية، والتفاعل بين الأقسام والأفراد، والتغييرات التنظيمية. هذه العوامل تشكل جزءًا أساسيًا من بنية وعمل المؤسسة، وتؤثر بشكل كبير على قدرتها على تحقيق الأداء المرتفع والمستدام. ومن خلال إدارة هذه العوامل بشكل فعّال، يمكن للمؤسسة تعزيز أدائها العام وتحقيق النجاح في بيئة الأعمال المتغيرة.

4- تقييم الأداء العام

لتقييم الأداء العام لمركز الطوارئ 933 يجب مراعاة ما يلي:

1. زمن الاستجابة والاستعداد: يشمل هذا الجانب تقييم مدة الاستجابة لفرق الطوارئ في المركز، بدءاً من استلام البلاغ وحتى وصول الفرق إلى موقع الحادث وبدء العمليات المطلوبة. كما يُمكن تقييم مدى جاهزية المركز والفرق لمواجهة مختلف الحالات الطارئة.
2. جودة الخدمات الفنية: يُحلَّل جودة الخدمات الفنية المقدمة في مجال الكهرباء، ومدى فعالية الإصلاحات والصيانة التي يتم تقديمها في حالات الطوارئ.
3. التواصل والإشعارات العامة: يُقيَّم كفاءة التواصل مع الجمهور والجهات المعنية أثناء حالات الطوارئ، بما في ذلك آليات الإشعار وتقديم المعلومات الضرورية للجمهور.
4. التدريب والتطوير المستمر: يُحلل مدى فعالية برامج التدريب والتطوير المستمرة لموظفي المركز، وتقييم مدى استعدادهم وكفاءتهم في مواجهة الطوارئ.

هذه بعض العوامل التي يمكن مراعاتها في تقييم الأداء العام لمركز الطوارئ 933 التابع لشركة الكهرباء السعودية. تحليل هذه العوامل يساعد في تحسين الأداء وضمان تقديم خدمات طوارئ عالية الجودة وفعّالة.

5- تأثير سياسات أمن المعلومات على الأداء العام لمركز الطوارئ 933:

1. سياسات أمن المعلومات تضمن حماية البيانات والمعلومات الحساسة المتعلقة بالمشتركين والشركة ضد الاختراقات والتسريبات. بتوفير بيئة آمنة للبيانات، يمكن تعزيز الثقة لدى المشتركين وتقليل مخاطر فقدان البيانات أو الوقوع في أنشطة احتيالية.
2. من خلال تطبيق سياسات أمن المعلومات المناسبة، يمكن ضمان توافر الخدمات بشكل مستمر ودون انقطاع، وهو أمر حيوي في حالات الطوارئ والحالات الطارئة التي قد يعتمد عليها العديد من الأفراد والمؤسسات.
3. سياسات أمن المعلومات تساهم في تحديد وتقليل المخاطر الأمنية المحتملة والتهديدات السيبرانية، مما يحسن الاستجابة للهجمات الإلكترونية ويقلل من تأثيرها على أداء المركز.
4. من خلال اعتماد سياسات أمن المعلومات الملائمة، يمكن للمركز الامتثال للتشريعات والمعايير الصارمة المتعلقة بحماية البيانات والخصوصية، مما يحد من المخاطر القانونية ويحسن الثقة لدى العملاء والشركاء.
5. بتوفير بيئة آمنة وموثوقة للبيانات، يمكن للمركز تعزيز سمعته ومصداقيته بين العملاء والشركاء والمجتمع بشكل عام، مما يؤدي إلى تعزيز الثقة وتحقيق الأداء العام الممتاز.

المبحث الثالث: الكفاءة التشغيلية

الكفاءة هي مصطلح نستطيع قياسه عن طريق تشكيل نسبة الناتج التشغيلية إلى المدخلات الإجمالية وتعد الكفاءة معياراً على قياس درجة الأداء الذي يوضح الوسيلة التي تستخدم أدنى حد من المدخلات لإنتاج أعلى حد من النتائج المخرجات (زاهد،2023).

تبعاً لهذا فإن الكفاءة تتشابك مع استخدام جميع المدخلات في إخراج أي منتجات مستهدفة سابقاً، ويشمل هذا طاقة الأشخاص والمدة الزمنية. وهو يرتبط بالتقليل من هدر الموارد مثل الطاقة، والموارد المادية والوقت ويسعى نحو الوصول إلى نتائج محببة بشكل فعال (Hollo and Nage, 2010).

عرف (السواط والحربي، 2022،661) الكفاءة بأنها «وسيلة قياس الحدود الفعالة وتفسير الفروقات من هذه الحدود بما يتناسب مع عدم الكفاءة وقد حددت هذه الطرق على مبدأ الإجراءات المقامة بهدف توضيح الحدود والفرضيات التي طرحت،

ويمكن تحقيق الكفاءة التقنية عندما تكون المنظمة قد وصلت إلى مرحلة عالية من الكفاءة لتوليد أعلى درجة من المخرجات السليمة وتحقيق الأهداف المنشودة بكل احترافية وبجودة عالية، كما أن الكفاءة هي إتقان العمل بصورة عالية وذات جودة مرتفعة مع الحرص على التحديث بالإمكانيات المتوفرة من المؤسسة والتصدي للصعوبات والتحديات التي تقف في طريق التقدم والوصول إلى الأهداف، وهذا يتحقق بالتقليل من التكلفة المالية والاقتصادية».

لذا تعرف الكفاءة التشغيلية بأنها العلاقة بين كمية الموارد المستخدمة والنتائج المحققة، من خلال تعظيم المخرجات أو تخفيض الكمية المستخدمة من المدخلات للوصول إلى حجم معين من المخرجات، وتقاس بالنسبة التالية: (إبريهي، 2019)

الكفاءة التشغيلية = المخرجات الفعلية/ المخرجات القصوى من الموارد المتاحة.(Ogundari, 2015,)

كما تعرف الكفاءة التشغيلية بأنها استخدام الموارد المتاحة للحصول على أقصى إنتاج ممكن بطريقة ملائمة يراعى فيها تقليل التكاليف وتحقيق رغبات المستفيدين، كما تعرف بأنها العلاقة بين المدخلات والمخرجات وتتحقق عندما يتساوى الناتج الحدي لعوامل الإنتاج مع تكلفة كل عامل أي تحقق كفاءة في الإنتاج والتوزيع والتخصيص(مسعودي ولنصاري، 2020)

ونرى أن الكفاءة التشغيلية هي مفهوم يُستخدم في مجال إدارة الأعمال والاقتصاد لقياس قدرة المؤسسة أو المنظمة على استخدام الموارد المتاحة بكفاءة لتحقيق أهدافها. تتعلق الكفاءة التشغيلية بكيفية إدارة الموارد مثل العمالة والمعدات والمواد الخام والطاقة بشكل فعال لتحقيق أقصى قدر من الإنتاجية بأقل تكلفة ممكنة وفي أقل وقت ممكن.

يُعتبر تحسين الكفاءة التشغيلية هدفًا مهمًا للشركات والمؤسسات لزيادة ربحيتها وتنافسيتها في السوق. ويتضمن ذلك تحسين عمليات الإنتاج وإدارة سلسلة التوريد، وتحسين الجودة، وزيادة الإنتاجية، وتقليل التكاليف، وتحسين استخدام الموارد، تُقيس الكفاءة التشغيلية عادة بمؤشرات مثل نسبة الإنتاجية، ومعدل استخدام القدرات، ومتوسط التكاليف الإجمالية للإنتاج. ويمكن تطبيق تقنيات مثل تحليل العمليات وتقنيات إدارة الجودة الشاملة ونماذج تحسين الإنتاجية لتحقيق تحسين في الكفاءة التشغيلية.

أهمية الكفاءة التشغيلية في الشركات والمؤسسات.

تُعد الكفاءة التشغيلية أحد العوامل الرئيسية لضمان نجاح الشركات والمؤسسات في بيئة الأعمال اليومية، حيث تتمتع بعدة فوائد تشمل: (زاهد،2023)

1. تقليل التكاليف: من خلال تحسين استخدام الموارد المتاحة وتحسين عمليات الإنتاج والتسليم، تُسهم الكفاءة التشغيلية في تقليل التكاليف العامة وزيادة هامش الربح.
2. زيادة الإنتاجية: بتحسين عمليات الإنتاج واستخدام الموارد بكفاءة، يتسنى للشركات والمؤسسات تحقيق مزيد من الإنتاج دون زيادة في التكاليف.
3. تحسين جودة المنتجات والخدمات: من خلال تحسين عمليات الإنتاج والتسليم، يمكن للشركات تحسين جودة منتجاتها أو خدماتها، مما يعزز رضا العملاء ويساهم في بناء سمعة قوية في السوق.
4. زيادة التنافسية: بتحسين الكفاءة التشغيلية، تتمكن الشركات من المنافسة بفعالية أكبر في السوق، وتقديم منتجات عالية الجودة بتكاليف منافسة، مما يعزز مكانتها ويحافظ على استمراريتها في البيئة التنافسية.
5. تعزيز قدرة الاستجابة للتغيرات: تجعل الكفاءة التشغيلية الشركات والمؤسسات أكثر قدرة على التكيف مع التغيرات في البيئة الخارجية، مما يمكنها من الاستجابة بفعالية للتحديات الاقتصادية والتكنولوجية وتغيرات متطلبات العملاء.

ونرى مما سبق أن الكفاءة التشغيلية تُعتبر عاملاً أساسياً لتعزيز النجاح والاستدامة للشركات والمؤسسات على المدى الطويل.

يمكن للباحثين من خلال ما سبق تفسير أهمية الكفاءة التشغيلية لمركز الاتصال 933، لعدة أسباب:

1. ضمان استمرارية التشغيل: يعتمد قطاع الكهرباء على استمرارية التشغيل بشكل كبير، وخاصة في حالات الطوارئ. الكفاءة التشغيلية تضمن تشغيل المعدات والأنظمة بكفاءة عالية، مما يحافظ على توفير الكهرباء للمناطق المتضررة في حالات الطوارئ.
2. استجابة سريعة للأعطال والاضطرابات: يساعد تحقيق الكفاءة التشغيلية في الكهرباء في تحديد وإصلاح الأعطال بسرعة وفعالية، مما يقلل من مدة التوقف ويحد من الانقطاعات في التيار الكهربائي، وبالتالي يقلل من تأثيرات الطوارئ على المستخدمين.
3. تحسين استخدام الموارد والطاقة: من خلال تحسين عمليات الإنتاج والتوزيع، يمكن للكفاءة التشغيلية في قطاع الكهرباء تحسين استخدام الموارد والطاقة، مما يقلل من التكاليف ويزيد من الكفاءة العامة للنظام.
4. تقليل المخاطر البيئية والصحية: بتحقيق الكفاءة التشغيلية، يمكن لمركز الطوارئ 933 في قطاع الكهرباء تقليل انبعاثات الغازات الضارة وتقليل مخاطر التلوث البيئي والصحي، مما يسهم في تحسين جودة البيئة وصحة المجتمع المحيط.
5. بناء الثقة وتعزيز السمعة: تحقيق الكفاءة التشغيلية في توفير الكهرباء خلال الطوارئ يعزز الثقة بقدرة مركز الطوارئ 933 على التعامل مع المواقف الطارئة بشكل فعّال وموثوق، مما يعزز سمعته ويجعله مصدرا موثوقا للخدمات الكهربائية في البلدان المعنية.

مؤشرات الكفاءة التشغيلية.

تختلف المؤشرات بناءً على نوع الصناعة وطبيعة الشركة، ويتعين على الشركات اختيار المؤشرات التي تتناسب مع أهدافها التشغيلية والاستراتيجية. كما ينبغي مراقبة وتحليل هذه المؤشرات بانتظام لتحسين الكفاءة التشغيلية بشكل مستمر.

وفيما يلي بعض المؤشرات الشائعة وكيفية قياسها: (مسعودي،2020)

1. نسبة الإنتاجية :(Productivity Ratio) تقيس كفاءة استخدام الموارد في تحقيق الإنتاج. يتم حسابها عن طريق مقارنة الإنتاج المحقق بالموارد المستخدمة.
2. نسبة الاستخدام الكامل للقدرات :(Capacity Utilization Ratio) تُعكس كيفية استخدام الشركة لقدراتها الإنتاجية الكاملة. إذا كانت هذه النسبة مرتفعة، فإن ذلك يشير إلى استخدام كفء للموارد.
3. معدل الفاقد :(Wastage Rate) يُقيس كمية المواد أو الوقت أو الموارد التي تضيع أثناء العمليات التشغيلية. يجب أن يكون هذا المؤشر منخفضًا لتحسين الكفاءة.
4. مؤشرات الجودة :(Quality Indicators) تقيس جودة المنتجات أو الخدمات التي تقدمها الشركة. تشمل هذه المؤشرات نسبة المنتجات المعيبة أو معدلات الاسترداد.
5. متوسط التكاليف الإجمالية للإنتاج :(Total Cost per Unit Produced) يُقيس كلفة إنتاج وحدة من المنتج. يمكن استخدام هذا المؤشر لتحديد كفاءة استخدام الموارد في عملية الإنتاج.
6. نسبة العمالة المستخدمة بكفاءة :(Labor Efficiency Ratio) تقيس كفاءة استخدام العمالة في العمليات التشغيلية، وتشمل عدد الوحدات التي تنتجها كل عامل أو عدد الساعات الإنتاجية لكل عامل.

7. مؤشرات الفعالية في إدارة المخزون (Inventory Management Efficiency Indicators): تقيس كيفية إدارة المخزون وتقليل تكاليف التخزين والتكاليف المرتبطة بالمخزون.

يُعتبر قياس الكفاءة التشغيلية في مركز الطوارئ 933 أمراً هاماً لضمان استمرارية توفير الخدمات الكهربائية بكفاءة في حالات الطوارئ. وتوجد بعض مؤشرات الكفاءة التشغيلية الرئيسية وكيفية قياسها كما سنوردها فيما يلي:

1. نسبة الاستجابة السريعة:(Rapid Response Rate)

يتم قياس هذا المؤشر عن طريق حساب الوقت المستغرق لاستجابة فرق الطوارئ في مركز الطوارئ 933 للحالات الطارئة. يجب أن يكون هذا الوقت قصيرًا للغاية لضمان الاستجابة الفورية للمشكلات الكهربائية.

2. نسبة التشغيل السليم:(Proper Operation Ratio)

يُعرف هذا المؤشـــر بكمية الوقت التي يعمل فيها النظام الكهربائي بدون أعطال أو انقطاعات. يتم قياســـه عن طريق تحديد الفترات التي كانت فيها الخدمة متاحة بشكل سلس ومستمر.

3. معدلات الصيانة الوقائية:(Preventive Maintenance Rates)

يقيس هذا المؤشـــر التزام مركز الطوارئ 933 بالصـــيانة الوقائية للمعدات والأنظمة الكهربائية. يمكن قياســـه بمعدل الصيانة الدورية والتفتيشات التي تُجرى بانتظام.

4. معدلات الاستجابة للأعطال:(Fault Response Rates)

يقيس هذا المؤشـــر فاعلية اســـتجابة فرق الصـــيانة في مركز الطوارئ 933 لحالات الأعطال الكهربائية المفاجئة. يتم حسابه عن طريق تحديد الوقت اللازم لإصلاح الأعطال بعد تقديم البلاغ.

5. نسبة الاستخدام الكامل للقدرات:(Capacity Utilization Ratio)

يُقيس هذا المؤشـــر كيفية اســـتخدام مركز الطوارئ 933 لقدراته الكهربائية الكاملة في الحالات الطارئة. يتم قياســـه بمقارنة القدرة الإنتاجية المستخدمة مع القدرة الإنتاجية الكلية المتاحة.

6. مؤشرات الفعالية في التواصل:(Communication Effectiveness Indicators)

يقيس هذا المؤشـــر كفاءة الاتصـــالات داخل مركز الطوارئ 933 ومع الجهات الخارجية مثل العملاء والجهات الحكومية والشركات الأخرى المعنية. يمكن قياسه عن طريق تقييم جودة التواصل وسرعة الاستجابة للاستفسارات والمشكلات.

تأثير سياسات أمن المعلومات على الكفاءة التشغيلية

يمكن أن يؤثر تطبيق سياسات أمن المعلومات بشكل كبير على كفاءة التشغيلية في المؤسسات والشركات من خلال ما يلي:

7. تنفيذ سياسات أمن المعلومات الصارمة، يمكن للمؤسسات تقليل مخاطر الهجمات الإلكترونية وانتهاكات البيانات التي قد تؤدي إلى انقطاعات في الخدمة. بتقليل هذه المخاطر، يمكن الحفاظ على استمرارية العمل وتجنب الخسائر المحتملة المرتبطة بالتوقفات غير المخطط لها.
8. بتوفير بيئة عمل آمنة ومحمية، يمكن للموظفين التركيز على أداء واجباتهم بشكل أفضل دون التوقف المستمر للقلق حول أمن المعلومات. هذا يمكن أن يؤدي إلى زيادة الإنتاجية وتحسين الكفاءة التشغيلية بشكل عام.

9. سياسات أمن المعلومات الجيدة تسهم في حماية البيانات الحساسة للعملاء وضمان خصوصيتها. بتحسين جودة البيانات وحمايتها من الاختراقات والتسريبات، يمكن للمؤسسات تحسين جودة الخدمات والمنتجات التي تقدمها، مما يعزز رضا العملاء ويحسن سمعتها في السوق.
10. تنفيذ سياسات أمن المعلومات يمكن أن يساعد المؤسسات على الامتثال للتشريعات والمعايير الصارمة المتعلقة بحماية البيانات والخصوصية، مما يقلل من المخاطر القانونية والغرامات المحتملة التي قد تؤثر على كفاءتها التشغيلية.
11. الاستثمار في سياسات أمن المعلومات يمكن أن يؤدي إلى تقليل التكاليف المتعلقة بالاختراقات والاختراقات الأمنية، مثل تكاليف استعادة البيانات، وتعويض العملاء، وإصلاح الأضرار التي يمكن أن تحدث جراء الهجمات السيبرانية.

4. الإطار التطبيقي:

1.4. منهج الدراسة:

سوف يستخدم في هذه الدراسة المنهج الوصفي التحليلي، لأن هذا المنهج يصف الظاهرة بشكل واضح من خلال المعلومات التي ستجمع وسيتم تحليلها بالطرق الإحصائية المناسبة.

2.4. مجتمع الدراسة:

يتكون مجتمع الدراسة من موظفي مركز الطوارئ 933 التابع لشركة الكهرباء السعودية بمختلف درجاتهم الوظيفية، ويبلغ عددهم (503) موظف، حيث يضم هذا المجتمع مديري المركز والمشرفين والفنيين والموظفين الإداريين والعمال في مجالات مختلفة. تتنوع خبرات ومهارات أفراد هذا المجتمع، مما يجعله مثاليًا لدراسة تأثير سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية. يمثل هؤلاء الموظفون العمود الفقري للمركز، حيث يعملون بشكل متواصل على تقديم الخدمات في ظل الظروف الطارئة، وبالتالي يعتبرون مصدرًا غنيًا بالبيانات والمعلومات المهمة لفهم تأثير سياسات أمن المعلومات على كفاءتهم وأدائهم العام.

3.4. عينة الدراسة:

تم اختيار عينة الدراسة باستخدام أسلوب العينة العشوائية البسيطة من مركز الطوارئ 933، حيث تم اختيار الأفراد بشكل عشوائي مباشرة من قائمة العاملين في المركز دون تقسيمهم إلى فئات أو طبقات. بناءً على هذا الاختيار، بلغ حجم العينة الإجمالي 252 فردًا. يعتبر هذا الحجم مناسبًا لتمثيل مجتمع الدراسة بشكل كافٍ، ويسمح بجمع البيانات وإجراء التحليلات الإحصائية اللازمة لتحقيق أهداف الدراسة.

4.4. أداة الدراسة:

لتحقيق أهداف الدراسة تم استخدام الاستبانة أداةً لجمع البيانات؛ وذلك نظرًا لمناسبتها لأهداف الدراسة، ومنهجها، وللإجابة عن أسئلتها، وتم استخدام الاستبانة ضمن الخطوات الآتية:

1. الاطلاع على الأدب النظري والدراسات السابقة ذات الصلة بموضوع الدراسة الحالية وفي ضوء أسئلة الدراسة وأهدافها تم بناء استبيان، ثم تحديد المجالات المتعلقة بمحاور الاستبانة وصياغة فقراتها .
2. وقد تكونت الاستبانة من ثلاثة أجزاء :

الجزء الأول: يقيس إجراءات أمن المعلومات لدى مركز الطوارئ 933 من وجهة نظر الموظفين يتكون من (25) فقرة موزعة على خمسة أبعاد هي:

- البعد الأول: سياسة أمن المعلومات
- البعد الثاني: تقنيات أمن المعلومات
- البعد الثالث: تنظيم أمن المعلومات
- البعد الرابع: أمن المعلومات للموارد البشرية
- البعد الخامس: بيئة أمن المعلومات

الجزء الثاني: يقيس مستوى الأداء العام والكفاءة التشغيلية لدى مركز الطوارئ 933 من وجهة نظر الموظفين يتكون من (10) فقرة.

الاتساق الداخلي لأداة الدراسة:

تم التحقق من صدق البناء الداخلي للفقرات والأبعاد بحساب - معامل ارتباط بيرسون- بين كل فقرة من فقرات الأداة، والأداة ككل، بعد تطبيق أداة الدراسة على عينة استطلاعية قوامها (30) من الموظفين مركز الطوارئ 933 من مجتمع الدراسة ومن خارج عينتها الأساسية، كما في الجدول (1) الآتي:

جدول (1) معاملات ارتباط الفقرة بالمجال والدرجة الكلية للمقياس الذي تنتمي إليه في محور مستوى تطبيق سياسات أمن المعلومات لدى مركز الطوارئ 933 من وجهة نظر الموظفين

البعد الأول		البعد الثاني		البعد الثالث		البعد الرابع		البعد الخامس	
سياسة أمن المعلومات		تقنيات أمن المعلومات		تنظيم أمن المعلومات		أمن المعلومات للموارد البشرية		بيئة أمن المعلومات	
م	معامل الارتباط	م	معامل الارتباط	م	معامل الارتباط	م	معامل الارتباط	م	معامل الارتباط
1	.702**	6	.529*	11	.824**	16	.500*	21	.583*
2	**632.	7	.738**	12	.879**	17	.724**	22	.713**
3	.792**	8	.784**	13	.650**	18	.786**	23	.796**
4	.491*	9	.458	14	.792**	19	.849**	24	.733**
5	.689**	10	.739**	15	.724**	20	.694**	25	.513*

* دالة إحصائياً عند مستوى الدلالة (0.05)

** دالة إحصائياً عند مستوى الدلالة (0.01)

تشير النتائج في جدول (1) أن جميع معاملات الارتباط للفقرات دالة إحصائياً عند مستوى الدلالة (0.01) ودالة إحصائياً عند مستوى الدلالة (0.05) وقد تراوحت بين (0.792- 0.491)، وهي قيم موجبة ودالة إحصائياً وتشير إلى تمتع الأداة بصدق مقبول.

جدول (2) معاملات ارتباط الفقرة والدرجة الكلية للمقياس الذي تنتمي إليه في محور مستوى الأداء العام والكفاءة التشغيلية

الأداء العام		الكفاءة التشغيلية	
م	معامل الارتباط	م	معامل الارتباط
1	.514*	6	.776**
2	.532**	7	.617**
3	.695**	8	.793**
4	.787**	9	.839**
5	.441*	10	.856**

** دال إحصائياً عند مستوى الدلالة (0.01)

* دال إحصائياً عند مستوى الدلالة (0.05)

تشير النتائج في الجدول (2) أن جميع معاملات ارتباط الفقرات بالدرجة الكلية لمحور الأداء العام والكفاءة التشغيلية جاءت دالة إحصائياً عند مستوى الدلالة (0.01)، (0.05)، وتراوحت بين (0.839- 0.441)، وهي قيم موجبة ودالة إحصائياً مما يشير إلى تمتع الفقرات بمعاملات صدق عالية يمكن الوثوق بها لإجراء الدراسة.

ثبات أداة الدراسة:

تم التحقق من ثبات الاستبانة بحساب ثبات الاتساق الداخلي للفقرات باستخدام معامل كرونباخ- ألفا، كما في جدول (3).

جدول (3) معاملات ثبات أداة الدراسة

المقياس	عدد الفقرات	ثبات ألفا كرونباخ
أمن المعلومات	25	0.977
الأداء العام والكفاءة التشغيلية	10	0.928

**** دال إحصائياً عند مستوى الدلالة (0.01)**

تشير النتائج في الجدول (3) أن معامل ثبات الاتساق الداخلي بطريقة كرونباخ ألفا لمحور أمن المعلومات من وجهة نظر العاملين والمدراء بلغ (0.977) في حين أن معامل ثبات كرونباخ ألفا لمحور أمن المعلومات من وجهة نظر العملاء بلغ (0.928)، وهي قيم مرتفعة وتشير إلى تمتع الأداة بثبات عالٍ يسمح باستخدامها كأداة للدراسة.

جدول رقم (4) أوزان الإجابات حسب مقياس ليكرت الخماسي.

الإجابات	الوزن	المتوسط المرجح
غير موافق بشدة	1	1 إلى < 1.80
غير موافق	2	1.80 إلى < 2.60
محايد	3	2.60 إلى < 3.40
موافق	4	3.40 إلى < 4.20
موافق بشدة	5	4.20 إلى 5

وتم حساب المتوسطات الحسابية المرجحة لكل عبارة من عبارات أداة الدراسة ومقارنتها مع المدى الموجود في الجدول أعلاه وتعطى الإجابة المقابلة للمدى الذي يقع بداخله متوسط العبارة.

5.4. المعالجة الإحصائية:

بناءً على طبيعة الدراسة والأهداف التي سعت إلى تحقيقها، تم تحليل البيانات باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS) ، وتم استخراج النتائج وفقاً للأساليب الإحصائية التالية:

- التكرارات والنسب المئوية: للتعرف على خصائص أفراد عينة الدراسة وفقاً للبيانات الشخصية.
- المتوسطات الحسابية والانحرافات المعيارية: لحساب المتوسطات الحسابية لفقرات محاور الاستبانة وكذلك الدرجات الكلية والدرجات الفرعية لأبعادهما بناء على استجابات أفراد العينة.
- معامل ارتباط بيرسون: لحساب صدق البناء الداخلي وكذلك لحساب ارتباط درجة سياسات أمن المعلومات على الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933.
- معامل ألفا كرونباخ: لحساب ثبات الأداة.

5. نتائج التحليل لمحاور الدراسة:

السؤال الأول: ما مستوى تطبيق سياسات أمن المعلومات وأبعادها في مركز الطوارئ 933 من وجهة نظر الموظفين فيه؟

تضمنت استمارة الاستبانة 25 عبارة تتعلق بسياسات أمن المعلومات، وعند احتساب المتوسطات الحسابية والانحرافات المعيارية، لإجاباتهم عن تلك العبارات الموضحة بالجدول (5)، أمكن التعرف على مستوى سياسات أمن المعلومات.

جدول (5): المتوسطات الحسابية والانحرافات المعيارية لاستجابات عينة الدراسة لأبعاد أمن المعلومات مرتبة تنازلياً حسب متوسطاتها الحسابية من وجهة نظر الموظفين فيه.

أبعاد أمن المعلومات	المتوسط الحسابي	الانحراف المعياري	الترتيب حسب الأهمية	المستوى حسب المتوسط
تقنيات أمن المعلومات	4.06	.502	1	مرتفعة
تنظيم أمن المعلومات	4.02	.552	2	مرتفعة
أمن المعلومات للموارد البشرية	3.86	.523	3	مرتفعة
سياسة أمن المعلومات	3.28	.873	4	متوسطة
بيئة أمن المعلومات	2.95	.620	5	متوسطة
المتوسط الكلي	3.64	.476	-	مرتفعة

يبين جدول رقم (5) أن المتوسط الحسابي الإجمالي لأهمية أبعاد تطبيق سياسات أمن المعلومات من وجهة نظر الموظفين بمركز الطوارئ 933 واقع ضمن الحالة المرتفعة والبالغة (3.64)، بما يفيد بأن تصورات المبحوثين، ذات نسب إيجابية إزاء هذا المتغير الأساسي، حيث حاز بُعد (تقنيات أمن المعلومات) الأهمية الأولى بمتوسط حسابي مقداره (4.06)، وتلاه بُعد (تنظيم أمن المعلومات) بمتوسط حسابي مقداره (4.02)، و(أمن المعلومات للموارد البشرية) بمتوسط حسابي (3.86)، و(سياسة أمن المعلومات) بمتوسط حسابي (3.28)، وأخيرا بُعد (بيئة أمن المعلومات) بمتوسط حسابي وقدره (2.95).

وتعكس هذه النتيجة قناعة الإدارة بأهمية تقنيات أمن المعلومات ومراجعة تنظيم أمن المعلومات، ودور أمن المعلومات للموارد البشرية وأهمية سياسة أمن المعلومات وأثر بيئة أمن المعلومات.

وعليه يخلص للقول إن توفر الإجراءات التنظيمية لضبط نظم المعلومات هي مؤثر فاعل في إدارة أمن نظم المعلومات فهي بمثابة الراعي والمنظم لعمليات تبادل ونقل المعلومات ومدخل الإدارة العليا للحفاظ على عمل نظم المعلومات، حيث تضع خطط الطوارئ والاستعادة، وتعتني بضرورات التوفر والسلامة والسرية للمعلومات وفق رؤيتها وسلامة مساراتها، ووفق ما لديها من إمكانات مالية وبشرية وفنية.

أما بالنسبة لكل بعد من أبعاد أمن المعلومات، فقد تم حساب المتوسطات الحسابية والانحرافات المعيارية لجميع فقرات كل بعد وعلى النحو الآتي:

جدول (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات كل بعد من أبعاد نظام أمن المعلومات من وجهة نظر الموظفين فيه

رقم	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
1	هناك ضوابط للدخول إلى نظام المعلومات في المركز.	4.39	.715	1	**مرتفعة جداً**
2	تتوفر إمكانية معرفة إحصـــائية للدخول على النظام من قبل العاملين بالمركز وأماكن وأوقات الدخول على النظام الخاص بالمركز.	4.35	.784	2	**مرتفعة جداً**
4	يتم استخدام الوسائل البيولوجية (بصمة العين، وبصمة الإصبع، وبصمة الصوت، للسماح بمرور المصرح لهم فقط.	3.81	.740	3	**مرتفعة**
3	يوجد للأنظمة الحساسة بيئة حاسب خاصة بها (معزولة).	3.78	.781	4	**مرتفعة**
5	هناك سـجل رقابي يتضـمن أنشـطة المسـتخدم، وحوادث أمن المعلومات	3.65	.709	5	**مرتفعة**
	المتوسط الكلي لبعد تقنيات أمن المعلومات	4.06	.502	-	**مرتفعة**
7	يتم تطبيق إجراءات واضـحة لاسـتمرارية الخدمة في كافة أنحاء المركز.	4.26	.729	1	**مرتفعة جداً**
6	يتم تحديد المخاطر التي يمكن أن تهدد معلومات المركز.	4.06	.574	2	**مرتفعة**
8	يطلب من الموظفين والمتعاقدين والأطراف الخارجية الإبلاغ عن أية نقاط ضعف يلاحظوا في الأنظمة الإلكترونية.	3.89	.701	3	**مرتفعة**
9	يتم تحديد الحوادث المتوقعة التي يمكن أن تتســبب في انقطاعات العمل.	3.88	.841	4	**مرتفعة**
10	يتم تصنيف المعلومات وفقا لقيمتها بالنسبة للمركز.	3.74	.855	5	**مرتفعة**
	المتوسط الكلي لبعد تنظيم أمن المعلومات	4.02	.552	-	**مرتفعة**

11	يتم التوعية بأمن المعلومات وأهميتها لجميع العاملين بالمركز.	4.00	.632	1	**مرتفعة**
12	هناك توفر دعم فني من الكوادر الوطنية في مجال أمن المعلومات في المركز.	3.99	.741	2	**مرتفعة**
13	هناك ضوابط بعدم دخول العاملين بالمركز للأماكن غير المصرح بها.	3.77	.852	3	**مرتفعة**
14	هناك قواعد لدخول وتنقل عمال الخدمة المعاونة داخل المركز.	3.69	.695	4	**مرتفعة**
15	الوسائل الأمنية المستخدمة في نقل الوثائق خارج المركز عن طريق المراسلين الخارجيين كافية لتحقيق ضمان وسلامة أمن الوثائق.	3.61	.761	5	**مرتفعة**
	المتوسط الكلي لبعد أمن المعلومات للموارد البشرية	3.86	.523	-	**مرتفعة**
16	تدرك الإدارة العليا للمركز أهمية حماية أمن المعلومات.	3.58	.886	1	**مرتفعة**
17	توجد وثيقة لبيئة أمن المعلومات في المركز.	3.26	1.032	2	**متوسطة**
18	يتم مراجعة وثيقة سياسة أمن المعلومات دورياً	3.26	1.032	3	**متوسطة**
19	يتم تعميم وثيقة سياسة أمن المعلومات من قبل الإدارة.	3.23	1.146	4	**متوسطة**
20	هناك إدارة مستقلة تهتم بأمن المعلومات داخل المركز.	3.10	1.193	5	**متوسطة**
	المتوسط الكلي لبعد سياسة أمن المعلومات	3.28	.873	-	**متوسطة**
22	يتم فحص أنظمة المعلومات للتحقق من الالتزام بمعايير أمن المعلومات.	3.03	.875	1	**متوسطة**
23	يطبق المديرون الإجراءات الأمنية كل في حدود الجهة المسؤول عنها	3.01	.948	2	**متوسطة**
21	الأجهزة والمعلومات والبرمجيات والوثائق لا تخرج من المركز إلا بتصريح	3.00	.894	3	**متوسطة**
24	يتم استخدام المحيطات الأمنية (الحواجز مثل: الجدران، الأبواب، الأقفال، استخدام البطاقات.. إلخ) لحماية المناطق التي تحوي المعلومات.	2.69	.816	4	**متوسطة**
25	يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها	2.68	.909	5	**متوسطة**
	المتوسط الكلي لبعد بيئة أمن المعلومات	2.95	.620	-	**متوسطة**
	المتوسط الكلي لمحور سياسات أمن المعلومات	3.64	.476	-	**مرتفعة**

يلاحظ من الجدول رقم (6) لسياسات أمن المعلومات، على النحو التالي:

أولاً: بعد تقنيات أمن المعلومات:

أن المتوسط الكلي لبعد تقنيات أمن المعلومات بلغ (4.6) وانحراف معياري (0.502) وبدرجة تقدير مرتفعة.

وقد جاءت الفقرة رقم (1) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " هناك ضوابط للدخول إلى نظام المعلومات في المركز " بمتوسط حسابي بلغ: (4.39)، وانحراف معياري (0.715)، وبدرجة تقدير مرتفعة جداً.

الفقرة (2) والتي نصت على" تتوفر إمكانية معرفة إحصائية للدخول على النظام من قبل العاملين بالمركز وأماكن وأوقات الدخول على النظام الخاص بالمركز " احتلت المرتبة الثانية بمتوسط حسابي بلغ: (4.35)، وانحراف معياري (0.784)، وبدرجة تقدير مرتفعة جداً.

ويأتي ذلك في الترتيب لتوفير المعلومات المطلوبة بالنسبة للعاملين مما يضمن قدر كبير من أمن المعلومات.

الفقرة (3) والتي نصت على" يوجد للأنظمة الحساسة بيئة حاسب خاصة بها (معزولة)." احتلت المرتبة قبل الاخيرة بمتوسط حسابي بلغ: (3.78)، وانحراف معياري (0.781)، وبدرجة تقدير مرتفعة

أما المرتبة الأخيرة والأقل متوسط فكانت للفقرة (5)، والتي نصت على: " هناك سجل رقابي يتضمن أنشطة المستخدم، وحوادث أمن المعلومات "، بمتوسط حسابي بلغ: (3.65) وانحراف معياري (0.709)، وبدرجة مرتفعة.

ومن هنا نجد أن مركز الطوارئ 933 لديه القدرة على الحفاظ على أفضل التقنيات الحديثة من خلال توافر: ربط معلومات إلكتروني وضوابط للتصوير وضوابط لعدم تصوير المستندات وتوافر الوسائل البيولوجية (بصمة العين، وبصمة الإصبع، وبصمة الصوت، للسماح بمرور المصرح لهم فقط. كما يوجد سجل رقابي يتضمن أنشطة المستخدم، وحوادث أمن المعلومات.

ثانياً: بعد تنظيم أمن المعلومات

أن المتوسط الكلي لبعد تنظيم أمن المعلومات بلغ (4.02) وانحراف معياري (0.552) وبدرجة تقدير مرتفعة.

وقد جاءت الفقرة رقم (7) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " يتم تطبيق إجراءات واضحة لاستمرارية الخدمة في كافة أنحاء المركز " بمتوسط حسابي بلغ: (4.26)، وانحراف معياري (0.729)، وبدرجة تقدير مرتفعة جداً.

كما جاء في المرتبة الاخيرة والاقل متوسط الفقرة (10)، والتي نصت على: " يتم تصنيف المعلومات وفقا لقيمتها بالنسبة للمركز " بمتوسط حسابي بلغ (3.74)، وانحراف معياري (0.855)، وبدرجة تقدير مرتفعة.

ثالثاً: بعد أمن المعلومات للموارد البشرية

أن المتوسط الكلي لبعد أمن المعلومات للموارد البشرية بلغ (3.86) وانحراف معياري (0.523) وبدرجة تقدير مرتفعة.

وقد جاءت الفقرة رقم (11) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " يتم التوعية بأمن المعلومات وأهميتها لجميع العاملين بالمركز " بمتوسط حسابي بلغ: (4.00)، وانحراف معياري (0.632)، وبدرجة تقدير مرتفعة.

أما المرتبة الأخيرة والاقل متوسط فكانت للفقرة (15)، والتي نصت على: " الوسائل الأمنية المستخدمة في نقل الوثائق خارج المركز عن طريق المراسلين الخارجيين كافية لتحقيق ضمان وسلامة أمن الوثائق "، بمتوسط حسابي بلغ: (3.61) وانحراف معياري (0.761)، وبدرجة مرتفعة.

رابعاً: بعد سياسة أمن المعلومات

أن المتوسط الكلي لبعد سياسة أمن المعلومات بلغ (3.28) وانحراف معياري (0.873) وبدرجة تقدير متوسطة.

وقد جاءت الفقرة رقم (16) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " تدرك الإدارة العليا للمركز أهمية حماية أمن المعلومات " بمتوسط حسابي بلغ: (3.58)، وانحراف معياري (0.886)، وبدرجة تقدير مرتفعة.

أما المرتبة الأخيرة والأقل متوسط فكانت للفقرة (20)، والتي نصت على: " هناك إدارة مستقلة تهتم بأمن المعلومات داخل المركز "، بمتوسط حسابي بلغ: (3.10) وانحراف معياري (1.193)، وبدرجة متوسطة.

مما يعني حاجة المركز إلى توافر وثيقة محددة لبيئة أمن المعلومات في المركز ويتم مراجعة هذه الوثيقة وربطها بسياسة أمن المعلومات بشكل دوري، والحاجة الملحة إلى تعميم وثيقة سياسة أمن المعلومات من قبل الإدارة الحاجة الى توافر إدارة مستقلة تهتم بي أمن المعلومات داخل المركز.

خامساً: بعد بيئة أمن المعلومات

أن المتوسط الكلي لبعد بيئة أمن المعلومات بلغ (2.95) وانحراف معياري (0.620) وبدرجة تقدير متوسطة.

وقد جاءت الفقرة رقم (22) في المرتبة الأولى، والتي نصت على: " يتم فحص أنظمة المعلومات للتحقق من الالتزام بمعايير أمن المعلومات " بمتوسط حسابي بلغ: (3.03)، وانحراف معياري (0.875)، وبدرجة تقدير متوسطة.

أما المرتبة الأخيرة فكانت للفقرة (25)، والتي نصت على: " يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها "، بمتوسط حسابي بلغ: (2.68) وانحراف معياري (0.909)، وبدرجة متوسطة.

يعني ذلك من خلال النتائج أعلاه وجود بعض القصور في توافر خطة طوارئ لأمن المعلومات ضد الكوارث وضوابط للأرشيف الورقي من حيث الاطلاع والتصوير والاتلاف، تقليص إجراءات رسمية للتخلص من الوسائط القابلة للإزالة مثل (الأقراص) بشكل آمن وسليم، حماية التمديدات الخاصة بالكهرباء والاتصالات ضد عمليات إساءة الاستخدام يتم منع المستخدمين من استخدام الأجهزة الأغراض غير المصرح بها.

السؤال الثاني: والذي نصه: ما مستوى الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين؟

تضمنت استمارة الاستبانة 10 عبارة تتعلق بمستوى الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933، وعند احتساب المتوسطات الحسابية والانحرافات المعيارية، لإجاباتهم عن تلك العبارات الموضحة بالجدول (7)، أمكن التعرف على مستوى الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين.

جدول (7): المتوسط الكلي لمستوى الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 مرتبة تنازلياً حسب متوسطاتها الحسابية.

الأداء العام والكفاءة التشغيلية	المتوسط الحسابي	الانحراف المعياري	الترتيب حسب الأهمية	المستوى حسب المتوسط
الأداء العام	3.9645	.90373	1	**مرتفعة**
الكفاءة التشغيلية	3.8594	.93910	2	**مرتفعة**
المتوسط الكلي	3.8828	.85546	-	**مرتفعة**

يبين جدول رقم (7) أن المتوسط الحسابي الإجمالي لأهمية الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين واقع ضمن الحالة المرتفعة والبالغة (3.88)، بما يفيد بأن تصورات المبحوثين، ذات نسب إيجابية إزاء هذا المتغير الأساسي، حيث حاز متغير (الأداء العام) الأهمية الأولى بمتوسط حسابي مقداره (3.96)، وتلاه متغير (الكفاءة التشغيلية) بمتوسط حسابي مقداره (3.85).

تعكس هذه النتائج أن الأداء العام في مركز الطوارئ يُعتبر مرتفعًا. حيث أن المتوسط الحسابي الإجمالي لأهمية الأداء العام والكفاءة التشغيلية بلغ 3.88 من أصل 5، مما يشير إلى أن الموظفين يرون الأداء العام في المركز بشكل إيجابي ومهم بالنسبة لعملية تقديم الخدمات والتعامل مع الطوارئ. بالإضافة إلى ذلك، يعزز التصنيف الأعلى لمتغير الأداء العام بمتوسط حسابي يبلغ 3.96 من 5 الفكرة القائلة بأن الموظفين يعتبرون الأداء العام بالمركز أكثر أهمية، مما يشير إلى أن هناك رؤية موحدة ومتفق عليها بين الموظفين بشأن أهمية تحقيق الأداء العام المرتفع في العمليات اليومية للمركز

يمكن القول بأن النتائج تعكس اعتقاد الموظفين بأن الكفاءة التشغيلية في مركز الطوارئ هي عالية، وهذا يشير إلى أن هناك تركيزًا شاملاً على تحقيق الأداء العام المرتفع والكفاءة التشغيلية المحسّنة في مركز الطوارئ.

أما بالنسبة لكل من الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين، فقد تم احتساب المتوسطات الحسابية والانحرافات المعيارية لجميع فقرات كل محور وعلى النحو الآتي:

جدول (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات الأداء العام والكفاءة التشغيلية لمركز الطوارئ 933 من وجهة نظر الموظفين

رقم العبارة	العبارة	المتوسط الحسابي	الانحراف المعياري	الرتبة	الدرجة
4	يقدم مركز الطوارئ 933 يقدم خدماته بشكل فعّال ومؤثر	4.07	1.115	1	**مرتفعة**
1	يستجيب مركز الطوارئ 933 للحالات الطارئة بطريقة سريعة وملائمة	4.06	1.122	2	**مرتفعة**
3	يتمتع مركز الطوارئ 933 بتنظيم جيد وإدارة فعالة	4.02	1.152	3	**مرتفعة**
2	تشعر بالرضا عن جودة الخدمات التي يقدمها مركز الطوارئ 933	3.98	1.130	4	**مرتفعة**
5	يستخدم مركز الطوارئ 933 الموارد بشكل فعّال لتحقيق أهدافه	3.85	1.137	5	**مرتفعة**
	المتوسط الكلي للأداء العام	3.9645	.90373	-	**مرتفعة**
9	يتم استخدام التكنولوجيا والأنظمة بشكل فعّال في مركز الطوارئ 933 لتحسين كفاءة العمليات	3.97	1.149	1	**مرتفعة**
10	يوجد تنسيق جيد بين مختلف الأقسام والفرق داخل مركز الطوارئ 933	3.95	1.121	2	**مرتفعة**

6	الموظفين في مركز الطوارئ 933 لـديهم المعرفـة والمهارات اللازمة لأداء مهامهم بكفاءة	3.91	1.133	3	**مرتفعة**
7	العمليات الداخلية في مركز الطوارئ 933 مُنظّمة ومُنفذة بكفاءة	3.84	1.197	4	**مرتفعة**
8	يتم تطبيق السياسات والإجراءات بشكل متسق وفعّال في مركز الطوارئ 933.	3.63	1.130	5	**مرتفعة**
	المتوسط الكلي لمتغير الكفاءة التشغيلية	**3.8594**	**.93910**	-	**مرتفعة**

يلاحظ من الجدول رقم (8) ما يلي:

أولاً: بالنسبة للأداء العام

أن المتوسط الكلي للأداء العام بلغ (3.96) وانحراف معياري (0.903) وبدرجة تقدير مرتفعة.

وقد جاءت الفقرة رقم (4) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " يقدم مركز الطوارئ 933 يقدم خدماته بشكل فعّال ومؤثر " بمتوسط حسابي بلغ: (4.07)، وانحراف معياري (1.199)، وبدرجة تقدير مرتفعة.

أما المرتبة الأخيرة والأقل متوسط فكانت للفقرة (5)، والتي نصت على: " يستخدم مركز الطوارئ 933 الموارد بشكل فعّال لتحقيق أهدافه "، بمتوسط حسابي بلغ: (3.85) وانحراف معياري (1.137)، وبدرجة مرتفعة.

ثانياً: بالنسبة الكفاءة التشغيلية

أن المتوسط الكلي لمتغير الكفاءة التشغيلية بلغ (3.85) وانحراف معياري (0.939) وبدرجة تقدير مرتفعة.

وقد جاءت الفقرة رقم (9) في المرتبة الأولى والأعلى متوسط، والتي نصت على: " يتم استخدام التكنولوجيا والأنظمة بشكل فعّال في مركز الطوارئ 933 لتحسين كفاءة العمليات " بمتوسط حسابي بلغ: (3.97)، وانحراف معياري (1.149)، وبدرجة تقدير مرتفعة.

أما المرتبة الأخيرة والأقل متوسط فكانت للفقرة (8)، والتي نصت على: " يتم تطبيق السياسات والإجراءات بشكل متسق وفعّال في مركز الطوارئ 933 "، بمتوسط حسابي بلغ: (3.63) وانحراف معياري (1.130)، وبدرجة مرتفعة.

تعكس هذه النتائج إلى أن مركز الطوارئ 933 يتمتع بمستوى عالٍ من الكفاءة التشغيلية والأداء العام. يُظهر الاستجابة السريعة والفعّالة للحالات الطارئة، جنبًا إلى جنب مع التنظيم الجيد والإدارة الفعّالة، أن المركز يدير عملياته بكفاءة ومؤثرية. بالإضافة إلى ذلك، يُشير الرضا العام للمستخدمين واستخدام الموارد بشكل فعّال إلى جودة الخدمات المقدمة وقدرة المركز على تحقيق أهدافه بنجاح. هذه النتائج تؤكد على التزام المركز بتقديم خدمات عالية الجودة والاستجابة السريعة لاحتياجات المجتمع والعملاء بشكل ملائم ومؤثر.

السؤال الثالث: والذي نصه: هل تؤثر سياسات أمن المعلومات بأبعادها (تقنيات أمن المعلومات، تنظيم أمن المعلومات، أمن المعلومات للموارد البشرية، سياسة أمن المعلومات، بيئة أمن المعلومات) على الأداء العام والكفاءة التشغيلية من وجهة نظر الموظفين؟

تم استخدام اختبار T للعينة الواحدة والنتائج مبينة في جدول رقم (9) والذي يبين آراء أفراد عينة الدراسة من الموظفين بمركز الطوارئ 933 لجميع المحاور.

جدول رقم (9): تأثير (تقنيات أمن المعلومات، تنظيم أمن المعلومات، أمن المعلومات للموارد البشرية، سياسة أمن المعلومات، بيئة أمن المعلومات) على الأداء العام والكفاءة التشغيلية بمركز الطوارئ 933.

م	المحاور	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة T	القيمة الاحتمالية
1	تقنيات أمن المعلومات	4.06	%81	19.312	0.000
2	تنظيم أمن المعلومات	4.02	%80	16.162	0.000
3	أمن المعلومات للموارد البشرية	3.86	%77	4.518	0.000
4	سياسة أمن المعلومات	3.28	%66	4.318	0.000
5	بيئة أمن المعلومات	2.95	%59	4.309	0.000
-	جميع الفقرات	3.64	%73	14.149	0.000

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "308" تساوي 1.98

ويتبين بصفة عامة أن المتوسط الحسابي لجميع المحاور الفرعية للمحور الأول تساوي 3.64، و المتوسط الحسابي النسبي يساوي 73 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 14.149 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و القيمة الاحتمالية تساوي 0.000 وهي اقل من 0.05 مما يدل على أن محاور (تقنيات أمن المعلومات، تنظيم أمن المعلومات، أمن المعلومات للموارد البشرية، سياسة أمن المعلومات، بيئة أمن المعلومات) تؤثر بصورة ايجابية على الأداء العام والكفاءة التشغيلية عند مستوى دلالة إحصائية 0.05

ونرى بأنه يتوفر لدى مركز الطوارئ 933 تقنيات مقبولة إلى حد ما على الأقل في شقيها (البرمجي، والمادي) وعلى الرغم من ذلك فهي أيضا بحاجة إلى تطوير لأن حماية النظم المعلومات مسألة في غاية الأهمية، كونها تضع الأساس الذي سيقوم عليه بناء النظام الأمني من الناحية المادية والفنية والبشرية.

6. النتائج والتوصيات:

1.6. النتائج:

1. تبين أن هناك إدراكاً إيجابياً لأهمية سياسات أمن المعلومات في مركز الطوارئ 933، حيث تم تقدير أبعادها المختلفة بمتوسط حسابي مرتفع وذلك بمتوسط حسابي (3.64) حيث تم منح الأولوية لتقنيات أمن المعلومات وتنظيم أمن المعلومات، مع اعتراف بأهمية أمن المعلومات للموارد البشرية وسياسات أمن المعلومات، وتباين في تقدير بيئة أمن المعلومات.
2. توضح النتائج أن مستوى الأداء العام والكفاءة التشغيلية في المركز مرتفع، مما يعكس جاهزيته لتقديم الخدمات والتعامل مع الحالات الطارئة بشكل فعّال.
3. يشير التحليل إلى أن تطبيق سياسات أمن المعلومات يؤثر بشكل إيجابي على الأداء العام والكفاءة التشغيلية، حيث يسهم في تعزيز التنظيم واستخدام الموارد بشكل فعال
4. يظهر من الدراسة أن مركز الطوارئ يحتاج إلى استمرارية التحسين والتطوير، خاصة فيما يتعلق بتقنيات أمن المعلومات واستخدام الموارد بشكل أكثر فعالية.

5. توضح النتائج أن جميع الأبعاد المدروسة لسياسات أمن المعلومات تؤثر بشكل إيجابي على الأداء العام والكفاءة التشغيلية للمركز، مما يدعم الحاجة إلى تطوير تلك السياسات وتعزيزها.
6. يعتبر تحسين تقنيات أمن المعلومات ضروريًا لضمان حماية النظم والبيانات، والارتقاء بجودة الخدمات المقدمة في المركز.

2.6. التوصيات:

1. يجب تعزيز برامج التدريب والتوعية بشأن سياسات أمن المعلومات بمركز الطوارئ 933، لضمان تطبيق السياسات بفعالية من قبل جميع الموظفين.
2. ينبغي الاستمرار في تطوير وتحسين التقنيات المستخدمة في مركز الطوارئ لضمان أنظمة الأمان والتشغيل تعمل بكفاءة عالية وفعالية.
3. ينبغي مراجعة سياسات أمن المعلومات بشكل دوري ومستمر لضمان تحديثها ومواءمتها مع التطورات التكنولوجية والتهديدات الأمنية الجديدة.
4. يجب تعزيز التواصل الداخلي في المركز من خلال الاجتماعات الدورية والتوجيهات الواضحة لتحقيق فهم مشترك لأهداف المركز والتحديات التي قد تواجهه.
5. يجب إجراء تقييمات دورية لأداء المركز العام والفردي لتحديد نقاط القوة والضعف واتخاذ الإجراءات اللازمة لتحسين الأداء بشكل مستمر.
6. يُفضل تعزيز مراقبة الأداء والتقييم المستمر للعمليات والخدمات المقدمة من المركز، بهدف ضمان الجودة والفعالية في تقديم الخدمات والعمليات.

7. قائمة المراجع:

1.7. المراجع العربية:

ابريهي، أسامة، (2019). حاسبة الإنجاز وأثرها في قياس الكفاءة التشغيلية بحث تطبيقي في شركة مصافي الوسط – مصفى الدورة"، مجلة دراسات محاسبية ومالية (JAFS)، المجلد (14)، العدد (46): 81-87، بغداد، العراق، 2019.

أبو ذويب، قتيبة عاهد (2019). مدى الالتزام بسياسات أمن وحماية المعلومات المحاسبية في البنوك التجارية الأردنية، رسالة ماجستير، جامعة آل البيت، المفرق، الأردن.

أحمد، معاذ أحمد عبد الرازق (2016). أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة، رسالة ماجستير، جامعة أم درمان الإسلامية، السودان.

البركي، أحمد محمد حمد (2020). واقع تطبيق متطلبات نظم إدارة أمن المعلومات المتوافقة مع المواصفة ISO 27001: 2005 بالمصارف العاملة بمدينتي بنغازي والبيضاء، مجلة الاقتصاد الدولي والعولمة، جامعة زيان عاشور بالجلفة، الجزائر، 3(2): 143 – 162.

تادرس، إبراهيم حربي هاشم (2017). مخاطر الأمن المعلوماتي وسبل مواجهتها في المصارف التجارية العاملة في محافظة البلقاء، مجلة مركز صالح عبدالله كامل للاقتصاد الاسلامي، جامعة الازهر، مصر،21(63): 175 – 213.

الذنيبات، معاذ يوسف. (2018). الممارسة الفاعلة لإدارة أمن المعلومات في المنظمات الحكومية السعودية وفقاً للمواصفة ISO IEC 27002 : 2013 /.مجلة البحوث التجارية المعاصرة، 32(1) , 272 - 308

زاهد، أمل فريد. (2023). دور استراتيجيات التحول الرقمي في رفع الكفاءة التشغيلية والتسويقية لخدمات الاتصالات بالمملكة العربية السعودية: دراسة تطبيقية على شركة الاتصالات السعودية، المجلة العربية للإدارة، 45(2) 1-18

السواط طلق عوض الله والحربي، ياسر ساير (2022) أثر التحول الرقمي على كفاءة الأداء الأكاديمي (حالة دراسية لهيئة أعضاء التدريس بجامعة الملك عبد العزيز بجده المجلة العربية للنشر العلمي (AISP)، العدد (43)، ص.647-686.

الشمالي، حسين علي قاسم (2017)" أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن" مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، (2) 188-201.

صيام، آمال نمر حسن. (2016). الأداء المؤسسي، تطبيق التخطيط الإستراتيجي وعلاقته بأداء المؤسسات الأهلية، رسالة ماجستير، جامعة الأزهر، غزة.

العتيبي، غانم بن غزاي الروقي (2013) أمن نظم المعلومات وعلاقته بمستويات الإبداع للعاملين في شركة الاتصالات السعودية بالرياض، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية السعودية.

عوض الله، طارق أحمد العوض (2017) أُثر البرمجيات الحديثة على أمن المعلومات: دراسة حالة هيئة الجوازات والسجل المدني السودانية، رسالة دكتوراه، جامعة أم درمان الاسلامية.

الغثبر، خالد بن سليمان (2012). حال أمن المعلومات في المملكة العربية السعودية، مجلة دراسات المعلومات، جمعية المكتبات والمعلومات السعودية، (1) 189-205.

فيلالي، أسماء ويحياوي، سليمان (2019). واقع أمن المعلومات في المؤسسة الوطنية للأشغال البترولية الكبرى. مجلة المالية والأسواق، 5(10)354-374.

مسعودي، فتحية؛ ولنصاري، فاطمة.(2020)."قياس الكفاءة التشغيلية باستخدام النسب المالية لعينة من المؤسسات المالية في الجزائر: دراسة حالة بنك الخليج الجزائر"، رسالة ماجستير، جامعة أحمد دراية، أدرار، الجزائر.

الهاجري، ماجد (2013). واقع تطبيق معايير أمن المعلومات في القطاع الحكومي بدولة الكويت - دراسة ميدانية، مجلة كلية التجارة للبحوث العلمية - جامعة الاسكندرية، (50) 263-307.

الحسيني، زيد اياد علي. (2019). أثر إدارة المعرفة على الأداء التنظيمي في شركات الاتصالات في الأردن. رسالة ماجستير منشورة. جامعة آل البيت. كلية الاقتصاد والعلوم الإدارية. المفرق. الأردن.

عذاري، جاسم رحيم. (2013). أثر الاستقرار الوظيفي في الأداء التنظيمي للوحدات المالية في المؤسسات التعليمية، مجلة العلوم الاقتصادية، 9(33) 137 – 165

2.7. المراجع الأجنبية:

Al-Hamar, A. (2018). Enhancing Information Security in Organisations in Qatar (Doctoral Dissertation, Loughborough University.)

Alkahtani, H. K. (2018). Raising The Information Security Awareness Level in Saudi Arabian Organizations Through an Effective, Culturally Aware Information Security Framework (Doctoral Dissertation, Loughborough University).

Bogale, M., Lessa, L., & Negash, S. (2019). Building An Information Security Awareness Program for A Bank: Case from Ethiopia. Completed Research Paper Presented to Twenty-Fifth Americas Conference on Information Systems, Cancun, Retrieved16/02/2021 From Https://Www.Researchgate.Net/Publication/336133212 Building an Information Security Aware Ness Program for A Bank Case from Ethiopia.

Felizardo, A., Elisabete, F., & Thomaz, J. (2017). Organizational Performance Measurement and Evaluation Systems in Smes: The Case of the Transforming Industry in Portugal. Centro de Estudos e Formação avançada em Gestão e Economia (CEFAGE).

Francois, M. T. (2016). A quantitative study on the relationship of information security policy awareness, enforcement, and maintenance to information security program effectiveness (Order No. 10252444). Available from ProQuest Dissertations & Theses Global. (1868428830). Retrieved from https://www-proquest-com.sdl.idm.oclc.org/dissertations-theses/quantitative-study-on-relationship-information/docview/1868428830/se-2

Hollo, D, & Nagy, M. (2010). Rank Efficiency in The Enlarged European Union. Magyar Nemzeti Bank, Bis Papers No. 28, 217-235. Http://Www.Bis.Org/Publ/Bppdf/Bispap28m.Pdf.

Kelemie Tebkew Yirdaw, (2013) « Information Security Management Framework for Banking Industry in Ethiopia», Thesis of Master Degree of Science in Information Science, Ethiopia.

Masa'deh, R., Al-Henzab, J., Tarhini, A., & Obeidat, B. (2018). The Associations among Market Orientation, Technology Orientation, Entrepreneurial Orientation and Organizational Performance. Benchmarking: An International Journal, 25 (8), 3117-3142.

Mui, J. Y. (2023). In-person and remote employees and information security policy compliance (Order No. 30692417). Available from ProQuest Dissertations & Theses Global. (2894315906). Retrieved from https://www-proquest-com.sdl.idm.oclc.org/dissertations-theses/person-remote-employees-information-security/docview/2894315906/se-2

ISSN: 2706-6495

Ogundari. K, S.O.Ojo"(2015)An Examination Of Technical Economic, Allocative Efficiency Of Small Farms In Osun State Of Nigeria", Journal Of Central Of European Agriculture, Vol7, No3, Zagreb, Croatia.

Okoye, S. I. (2017). Strategies to minimize the effects of information security threats on business performance (Order No. 10606454). Available from ProQuest Dissertations & Theses Global. (1944007406). Retrieved from https://www-proquest-com.sdl.idm.oclc.org/dissertations-theses/strategies-minimize-effects-information-security/docview/1944007406/se-2

Doi: doi.org/10.52132/Ajrsp/v6.71.5