المجلة الأكاديمية للأبحاث والنشر العلمي | الإصدار التاسع والأربعون | تاريخ الإصدار: 5-5-2023 م
ISSN: 2706-6495

إدارة مخاطر خصوصية المعلومات للخدمات الإلكترونية في وزارة المالية (دراسة حالة على قطاع الأفراد بالسعودية)

Information privacy risk management for the electronic portal in the Ministry of Finance (A case study on the individual sector in Saudi Arabia)

إعداد: الباحثة/ أمل محمد الوادعي
ماجستير إدارة مخاطر، جامعة الجميع الذكية، المملكة العربية السعودية
الباحثة/ هتون إبراهيم الوابل*
ماجستير إدارة مخاطر، جامعة الجميع الذكية، المملكة العربية السعودية
الباحث/ مرتضى صابر الشبعان
ماجستير إدارة مخاط، جامعة الجميع الذكية، المملكة العربية السعودية
إشراف: د. وليد سليمان
*Email: htoonwh@gmail.com

الملخص:
تأسيًا بالتحول الرقمي الذي تبنته المملكة العربية السعودية في قطاعات الدولة بما فيها القطاع العام أو الحكومي تحولت وزارة المالية من التعاملات الورقية إلى تعاملات إلكترونية عبر عدة قنوات منها البوابة الإلكترونية التي تخدم عدة قطاعات منها قطاع الأفراد سواء المواطن أو المقيم ولهذا التحول و التبديل مخاطر وسلبيات عدة منها انتهاك خصوصية المعلومات لذا جاءت هذه الدراسة لتسليط الضوء على إدارة مخاطر خصوصية المعلومات للمستخدم الفرد للبوابة الإلكترونية لوزارة المالية بالسعودية وتم استخدام المنهج الوصفي التحليلي لدراسة وتحليل إدارة مخاطر خصوصية المعلومات تحديدًا لوزارة المالية ومستخدم الفرد وتغطية السياسات والإجراءات والضوابط المقدمة من الدلائل الإرشادية وأسفرت عن هذه الدراسة حزمة نتائج منها أن ضوابط إدارة المخاطر المطبقة في البوابة الإلكترونية لوزارة المالية فعالة وذو أداء جيد وهناك ثقافة عالية لدى الفرد المستخدم اتجاه معلوماته الشخصية و الجهات الرقابية في الدولة متابعة ومهتمة بحماية المعلومات للمواقع الإلكترونية لكيانات الحكومة وتتمتع بحس أمني كبير بإنهاء انتهاك الخصوصية للمعلومات و وزارة المالية ملتزمة بتنفيذ سياسات حماية خصوصية المعلومات و موظفيها على دربة ودراية جيدة بآلية المحافظة على سرية المعلومات. وفي ضوء هذه النتائج، توصي الدراسة بضرورة تعيين فريق خبراء مختص في إدارة مخاطر خصوصية المعلومات وتحديد مسؤولياتهم، ووضع سياسات وإجراءات أكثر صرامة للحفاظ على حماية خصوصية المعلومات، وتكثيف التدريب للموظفين، وتطوير آلية التقييم الدوري لمخاطر خصوصية المعلومات والثغرات الأمنية. كما توصي الدراسة بضرورة استمرار وزارة المالية في تحديث سياسات وإجراءات إدارة المخاطر بشكل مستمر.

الكلمات المفتاحية: مخاطر خصوصية المعلومات، إدارة المخاطر، وزارة المالية، المملكة العربية السعودية.

ISSN: 2706-6495

Information privacy risk management for the electronic portal in the Ministry of Finance (A case study on the individual sector in Saudi Arabia)

Abstract:

Later the digital transformation adopted by the Kingdom of Saudi Arabia in the state sectors, including the public or government sector, the Ministry of Finance has shifted from paper-based transactions to electronic transactions through several channels, including the electronic portal, which serves several sectors, including the individual sector, whether citizen or resident. This transformation and switch has many risks and drawbacks. Including the violation of information privacy, so this study came to shed light on the management of information privacy risks for the individual user of the electronic portal of the Ministry of Finance in Saudi Arabia. A package of results, including that the risk management controls applied in the electronic portal of the Ministry of Finance are effective and perform well. There is a high culture among the individual user towards his personal information and the supervisory authorities in the country are following and interested in protecting the information of the websites of government entities and have a great sense of security by ending the privacy violation of information and the Ministry of Finance It is committed to implementing information privacy protection policies and its employees are well trained and aware of the mechanism for maintaining the confidentiality of information. Based on these results, the study recommends the necessity of appointing a team of experts specialized in managing information privacy risks and defining their responsibilities, developing stricter policies and procedures to maintain information privacy protection, intensifying training for employees, and developing a mechanism for periodic assessment of information privacy risks and security vulnerabilities. The study also recommends that the Ministry of Finance should continue to update risk management policies and procedures on an ongoing basis.

Keywords: Information Privacy Risks, Risk Management, Ministry of Finance, Kingdom of Saudi Arabia.

ISSN: 2706-6495

1. مقدمة البحث:

"التحول الرقمي أصبح من المواضيع المشتركة بين الحكومات والشركات التجارية في دول العالم نتيجة ثورة المعلومات والاتصالات التي أحدثت تغيير في المفاهيم والمصطلحات وطريقة تقديم الخدمة بشكل جذري سواء للمواطنين او العملاء، إلا أن التحول الرقمي يقابله مخاطر عديدة لذا يجب مواجهة بتطوير المنظومة لمواكبة الثورة التكنولوجية" (سلايمي، واخرون، 2019،ص 945)

و"يختلف مفهوم الخصوصية اختلافًا كبيرًا في مختلف البلدان أو الثقافات أو الولايات القضائية. التعريف المعتمد من قبل منظمة التعاون الاقتصادي والتنمية (OECD) هو "أي معلومات تتعلق بمعرف أو فرد يمكن التعرف عليه (موضوع البيانات). "تعريف آخر شائع مقدم من المعهد الأمريكي للشهادة المحاسبين العامين (AICPA) والمعهد الكندي للمحاسبين القانونيين (CICA) في المستوى المقبول عمومًا معيار مبادئ الخصوصية (GAPP) هو "حقوق والتزامات الأفراد والمنظمات فيما يتعلق بـجمع المعلومات الشخصية واستخدامها والاحتفاظ بها والكشف عنها" (هيئة الاتصالات وتقنية المعلومات السعودية،2023، مفهوم الخصوصية) https://www.cst.gov.sa/ar/Pages/default.aspx

"وتعتبر خصوصية المعلومات والتحديات التي تتعرض لها في نطاق عمليات الانترنت من أبرز مخاطر الحواسيب وبنوك المعلومات لتوفير حماية حياة الأفراد الخاصة وموجبات الاطلاع على شؤون الأفراد و حماية الأمن المعلوماتي والترتيبات الأمنية لسلامة الجهاز والمعلومات والتساؤلات" (محمود، 2022، العلاقة بين التحول الرقمي والخدمات المالية)

"وقد أسبغت التشريعات الداخلية من الدستور وقوانين لحماية بيانات الأفراد في ظل التقدم التكنولوجي وعصر المعلوماتية، كون تلك الخصوصية منبثقة من أحد الحقوق الدستورية الأساسية وهو الحق في الحياة الخاصة، وهو ما دعا الدول إلى الاهتمام بذلك الحق، وإصدار التشريعات الدولية لحمايته، مع وضع شرط الموازنة بين حق الأفراد في حماية خصوصيتهم، وضمان حفظ حق المجتمع في أمن وسلام، ومراعاة الأخذ بمبدأي الضرورة والتناسب في حال التعدي على خصوصية الفرد" (ريان، 2021، الحماية التشريعية للحق في خصوصية البيانات في العصر الرقمي)

1.1. مشكلة البحث:

"برغم العديد من المزايا التي يحققها استخدام تقنيات التحول الرقمي إلا أن هناك مخاطر جمة للتحول الرقمي قد تعيق تحقيق الأهداف المتمثلة في البقاء والنمو والتطور في بيئة الأعمال مما يستدعي الاهتمام بهذه المخاطر والعمل على إدارتها والتحكم فيها في حال حدوثها ووضع طرق وسياسات للحد من الخسارة" (النحاس، واخرون، 2022، ص 1501-1513)

حيث "تزايد الهجمات الإلكترونية من حين أزمة كورونا وتعتبر المخاطر الإلكترونية من أكبر خمس مخاطر عالمية من حيث الاحتمالية والتأثير"(IBM Security, 2021, Cost of data breach report –Risk Quanification)

"متوسط تكلفة اختراق البيانات هو 3.86 مليون دولار يجب على المؤسسات الاستثمار في أدوات الأمان مثل التشفير وحماية نقطة النهاية ومعلومات الأمن وحلول إدارة الأحداث بحكم ارتفاع متوسط تكلفة خرق البيانات"(عرب، 1972، المخاطر التي تهدد خصوصية المعلومات في العصر الرقمي)

"ويتوقف ذلك على مدى قدرة الدولة علي تقديم خدمات رقمية عالية القيمة في الوقت المناسب. كما تثير التحديات القائمة أمام عمليات الرقمنة وإمكانية التحول الرقمي أهمية كل من الدراسات النظرية والتجريبية المتعلقة بتطوير المؤشرات التي تسمح بتحليل المستوى الحالي لرقمنة التنمية الاجتماعية والاقتصادية للإقليم والإمكانات التحويلية، ونوعية الحياة الرقمية، وإيجاد طرق لتقييمها، وكذلك تحديد التوجهات المطلوبة لتطبيق سياسة الرقمنة. والتحول الرقمي هو عملية تؤثر بشكل كبير على جميع قطاعات المجتمع فهو مدفوع بوفرة التطبيقات الرقمية على الهواتف الذكية وأجهزة الكمبيوتر المحمولة وذلك بالإضافة إلى قدرة الفرد على الاتصال بـ 3.5 مليار شخص يستخدمون الإنترنت حاليًا."(العتيبي2020، تقييم مخاطر خصوصية المعلومات بوزارة العدل بالمملكة العربية السعودية)

2.1. أهمية البحث:

تأتي أهمية الدراسة حول آلية إدارة المخاطر لخصوصية المعلومات للأفراد مستخدمي الخدمات الإلكترونية من وزارة المالية في المملكة العربية السعودية لتتمكن الوزارة والحكومة من جني ثمار النفع والفائدة من العصر الرقمي الحديث، كما تنبع الأهمية أيضا من نتائج الدراسة التي ستشكل إضافة للقطاعات العامة في الدولة والوزارات الزميلة والحكومات المجاورة التي تتبنى التحول الرقمي آخذين من تجربة وزارة المالية بالمملكة العربية السعودية.

"مخاطر الحواسيب وبنوك المعلومات على الحق في الحياة الخاصة وشيوع (النقل الرقمي) للبيانات خلق مشكلة أمنية وطنية، إذ سهل استراق السمع والتجسس الإلكتروني. ففي مجال نقل البيانات تتبدى المخاطر المهددة للخصوصية في عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات وإمكانية استخدام الشبكات في الحصول بصورة غير مشروعة" (موقع وزارة المالية بالمملكة العربية السعودية،2023، التحول الرقمي بالوزارة)

https://www.mof.gov.sa/about/Pages/Enable.aspx

"كمية بيانات المستهلك التي يجمعها تجار التجزئة عبر نقاط اتصال العملاء المختلفة إلى تحقيق حماية خصوصية البيانات أولوية رئيسية. تتطلب خصوصية البيانات في سياقات البيع بالتجزئة التقارب بين ثلاثة أصحاب مصلحة رئيسيين: المستهلك، تاجر التجزئة، والجهة التنظيمية لكل منها أدوار ووجهات نظر فريدة. تؤكد هذه الموضوعات على العلاقات المتداخلة المعقدة بين المستهلكين وتجار التجزئة والقوى التنظيمية." " (IBM Security, 2021, Cost of data breach report –Risk Quanification) https://www.ibm.com/downloads/cas/OJDVQGRY

"أدى إلى وجود مسؤوليات جديدة فُرضت على المصارف ببذل الجُهود لتفادي المخاطر الرقمية التي تنجم عن استخدامها، والتي قد تنشأ عن أخطاء محتملة تحدث خلال مراحل التعامل مع البيئة الرقمية، والتي تؤثر على أمن المعلومات، مما يؤدي الأمر إلى الإضرار بمصالح مستخدمي المعلومات" (خنفر، كريم،2022، ص 502-522)

1.2.1. الأهمية العلمية:

تعتبر هذه الدراسة من الدراسات الحديثة في مجال قطاع الأفراد والتي تهدف إلى التعرف على إدارة مخاطر خصوصية المعلومات المهمة وذات سرية عالية للأفراد في وزارة المالية في المملكة العربية السعودية وتأتي أهمية البحث بضخ دراسة علمية جديدة

في مكتبة الأمة العربية بدعامة علمية رصينة لتكوين ثروة معرفية تفيد الأجيال القادمة والوزارات الأخرى داخل المملكة العربية السعودية وخارجها وفرصة لطلاب الدراسات العليا والباحثين في ذات التخصص للاستفادة منه.

2.2.1. الأهمية التطبيقية:

تتمثل الأهمية التطبيقية لدراسة قياس مدى تعرض الأفراد للسرقة والاحتيال وعدم المحافظة على الخصوصية لحماية بياناتهم وتعرضهم للخطر.

مما دفع الباحثين إلى إجراء هذه الدراسة لإدارة مخاطر خصوصية المعلومات لقطاع الأفراد عند استخدام البوابة الإلكترونية لوزارة المالية بالسعودية

3.1. أهداف البحث:

تهدف الدراسة إلى تحقيق الأهداف التالية:

1. تحديد التهديدات والمخاطر المتوقعة التي تسبب ضرر لوزارة المالية او المستفيد الفرد
2. التعرف على مخاطر خصوصية المعلومات للفرد عند استخدامه للخدمات الإلكترونية في البوابة الإلكترونية وزارة المالية بالسعودية
3. التعرف على ممارسات وضوابط إدارة مخاطر خصوصية المعلومات الحالية في وزارة المالية ومدى فاعليتها

4.1. فرضيات البحث:

1- تفترض الدراسة ان المستخدم الفرد يواجه مخاطر عند استخدامه البوابة الإلكترونية لوزارة المالية بالمملكة العربية السعودية.

2- تفترض الدراسة ان المستخدم الفرد يواجه خطر انتهاك خصوصية المعلومات بشكل أكبر جراء استخدامه للخدمات الإلكترونية من موقع الوزارة المالية الإلكتروني بالسعودية.

3- تفترض الدراسة ان ممارسات وضوابط إدارة المخاطر التي تتبعها وزارة المالية قادرة على تذليل خطر خصوصية المعلومات.

5.1. أسئلة البحث:

1- هل يواجه المستخدم الفرد مخاطر عند استخدامه البوابة الإلكترونية لوزارة المالية بالسعودية ؟

2- هل المستخدم الفرد يواجه خطر انتهاك خصوصية المعلومات بشكل أكبر جراء استخدامه للخدمات الإلكترونية من موقع الوزارة المالية الإلكتروني بالسعودية؟

3- هل ممارسات وضوابط إدارة المخاطر التي تتبعها وزارة المالية قادرة على تذليل خطر خصوصية المعلومات؟

6.1. منهج البحث:

المنهج العلمي المستخدم في هذه الدراسة هو المنهج الوصفي التحليلي لدراسة وتحليل إدارة مخاطر خصوصية المعلومات تحديدًا لوزارة المالية والمستخدم الفرد وتغطية السياسات والإجراءات والضوابط المقدمة من الدلائل الإرشادية واستخلاص النتائج

والمعطيات من الاستبيانات المطروحة لعينة البحث وهم الأفراد المستخدمين للبوابة الإلكترونية، علاوةً على الدراسات والتقارير السابقة التي تناولت متغيرات البحث.

7.1. مجتمع وعينة الدراسة:

المستخدمين الأفراد سواء المواطن او المقيم المستفيدين من الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية.

8.1. حدود البحث:

- **حدود مكانية:**

أجريت الدراسة في المملكة العربية السعودية لمستخدمي الخدمات الإلكترونية لقطاع الأفراد في الوزارة المالية

- **حدود زمانية:**

1- تناقش الدراسة الفترة ما بين سنة 2022م إلى نهاية الربع الأول لسنة 2023م

2- أجريت الدراسة الأساسية في الفترة من 2023/2/1 حتى 2023/4/10

9.1. المعالجات الإحصائية:

1- المتوسط الحسابي

2- الانحراف المعياري

3- التباين

4- اختبار ألفا كرو نباخ

5- النسب المئوية والتكرارات

2. الإطار النظري للدراسة

تمهيد

يشهد العالم تطورات تكنولوجية ضخمة وانتقالات إلى آفاق وآماد جديدة وإعادة لتصميم الأعمال للاستفادة من الرقمنة الحديثة والمملكة العربية السعودية تماشت مع العصر الحديث وأخذت بزمام التحول الرقمي وأنشئت قوة رقمية كعامل أساسي لتحقيق استراتيجيتها 2030م وهي حاسمة وعملية تهدف إلى تمكين وتسريع التحول الحكومي بكفاءة وفعالية وهذا التحول من خلال المشاريع والهيئات والمؤسسات الحكومية لتقديم الخدمات الحكومية بشكل رقمي، ومن تلك الجهات الحكومية التي تحولت رقميًا هي وزارة المالية حيث طبقت التعاملات الإلكترونية تفعيلًا لتوجه الدولة ومالها من ثقل واهمية في الاقتصاد الوطني و لاعب أساسي في اتخاذ القرارات الحكومية، واستخدمت وزارة المالية تطبيقات وحلول وبنى تحتية وخدمات إلكترونية تسهم في تطبيق منظومة رقمية متكاملة ويتم خدمة الصالح العام من الجهات الحكومية الأخرى في الدولة وخدمة القطاع الخاص من المنشآت التجارية والشركات المتعاقدة مع الدولة، كما تقدم الوزارة خدماتها لقطاع الأفراد وهو المستخدم الفرد سواء المواطن أو المقيم بشكل سريع وكفؤ. وحتى يتم الحصول على الخدمات من الموقع او المنصة الإلكترونية لابد من تسجيل وإدخال معلومات خاصة وسرية للفرد مثل رقم الهوية، الاسم الكامل، رقم الجوال وغيرها. هذه تعتبر معلومات هامة جدا ويجب توافر حماية كاملة لها لضمان عدم سرقتها او انتهاك خصوصيتها،

ووزارة المالية لديها السياسة لحماية المعلومات وأطر لسياسة الخصوصية ومطبقة لضوابط إدارة المخاطر الرقمية المسنة من قبل الهيئات الأخرى ذات العلاقة مثل هيئة الحكومة الرقمية، لذا جاء هذا البحث لتغطية الإجراءات وممارسات إدارة المخاطر لخصوصية المعلومة للمستفيد الفرد من الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية ومدى فعاليتها لتذليل التحديات والعراقيل، سنعرج في هذا الجانب على التحول الرقمي الحاصل في السعودية وفي وزارة المالية تحديدًا وأنواع المخاطر الرقمية التي قد تتعرض لها وبإسهاب سيتم ذكر مخاطر خصوصية المعلومات وإدارتها في وزارة المالية

المحور الأول: التحول الرقمي في المملكة العربية السعودية:

1- مفهوم التحول الرقمي:

تعد كلمة "رقمي" مرادفاً للتغير الحاد الذي يشهده العالم اليوم، والذي يتسارع بفعل اعتماد التكنولوجيا الرقمية الحديثة. بينما تتعلق كلمة "تحول" بقدرة المنظمة على التأقلم مع هذا التغيير والإبداع والابتكار الحاد في استخدام التكنولوجيا الرقمية، بدلاً من الاعتماد على الأساليب التقليدية في العمل: (الهادي، 2022،ص 166)

على الرغم من حداثة مفهوم التحول الرقمي، إلا أنه تم تعريفه بعدة طرق، ومن أبرز هذه التعريفات:

- هو استثمار الفكر وتغيير السلوك لتحقيق تحول جذري في طريقة العمل، وذلك عن طريق الاستفادة من التقدم التقني لخدمة المستفيدين بشكل أسرع وأفضل. يوفر التحول الرقمي فرصًا هائلة لبناء مجتمعات فعالة ومستدامة وتحسين تجربة المستهلكين والموظفين والمستفيدين، وذلك من خلال سلسلة من العمليات المناسبة وإعادة صياغة الإجراءات اللازمة للتفعيل والتنفيذ. ويتطلب التحول الرقمي إنشاء ثقافة إبداعية في بيئة العمل، ويشمل تغيير المكونات الأساسية للعمل، بدءًا من البنية التحتية ونماذج التشغيل وانتهاءً بتسويق الخدمات والمنتجات. (حاج، قاسم علي، 2020، إسهامات الاتحاد الإفريقي في عملية التحول الرقمي في إفريقيا قراءة في مشروع استراتيجية التحول الرقمي لإفريقيا) https://dspace.zu.edu.ly/handle/1/913
- يمثل التحول من النظام التقليدي إلى النظام الرقمي عملية تهدف إلى تطوير مختلف مجالات العمل بالاستفادة من التقنيات الحديثة، مما يتيح تحقيق أهداف المؤسسة بأقل تكلفة وفي أسرع وقت ممكن، ويتم ذلك عن طريق تحويل المعاملات الورقية إلى معاملات رقمية. (صيفي، حسنية، 2020، الإدارة الإلكترونية الصحية وتحديات التحول الرقمي في الدول العربية-دراسة حالة مملكة البحرين) https://dspace.zu.edu.ly/handle/1/914

وعرف ((Brysch. A,2017,Digital Transformation in Tourism Sector Challenges and Opportunities) https://www.researchgate.net/publication/323557395_Digital_Transformation_in_the_Tourism_Sector_-_Challenges_and_Opportunities

التحول الرقمي بأنه: يتمثل التحول الرقمي في استخدام التقنيات الرقمية الحديثة لإعادة صياغة نموذج الأعمال بشكل يسمح بتوفير فرص جديدة للدخل والقيمة المضافة، ويهدف إلى تحقيق الاقتصاد الرقمي بشكل تقني وإداري وتسويقي. ويماثل تعريف (البار، المرحبي، 2018، التحول الرقمي كيف ولماذا)

تمثل الثورة الرقمية تحولا جذريا في كيفية تشغيل المؤسسات الحكومية والخاصة، حيث تتمثل هذه العملية في انتقالها إلى نموذج عمل يعتمد بشكل كبير على التقنيات الرقمية في إبداع منتجات وخدمات جديدة. وتوفير قنوات جديدة للعائدات والفرص لزيادة قيمة المنتج، بهدف تحسين الكفاءة والجودة، وتيسير إجراءات الحصول على الخدمات المقدمة للعملاء، وذلك من خلال الاعتماد على الخدمات المبتكرة والإبداعية.

2- التحول الرقمي في المملكة العربية السعودية:

نجحت المملكة العربية السعودية في تعزيز دورها كمحرك للتحول الرقمي، وتجاوز ذلك ليصل إلى إعادة تحديد وتعريف مهمة الحكومة بشكل جذري. وفي ظل التطور الضخم الذي يشهده العالم في مجال التكنولوجيا وانتقالها إلى آفاق جديدة، فإن التحول الرقمي يشكل استراتيجية متكاملة وحاسمة للحكومة السعودية تماشياً مع رؤية 2030، وتهدف إلى تمكين وتسريع التحول الحكومي بكفاءة وفعالية. تم تنفيذ هذا التحول الكبير من خلال تنفيذ الحكومة لعدة برامج ومشاريع لتطوير الحكومة الإلكترونية، وذلك بتمكين ودعم المؤسسات والجهات الحكومية المختلفة، بهدف توفير جميع الخدمات الحكومية بشكل رقمي وسهل الوصول إليها. وتم تصميم استراتيجية التحول وتنفيذها بالاعتماد على الهندسة المعمارية الحديثة والمدعومة بالمهارات والقدرات والأدوات الرقمية، وتتضمن رؤية 2030 برنامج تحول فعال يتم تخطيطه بشكل جيد ويُعرف باسم برنامج التحول الوطني، والذي يسعى إلى تحسين البنية التحتية وخلق بيئة تُمكّن القطاعات العامة والخاصة وغير الربحية من تحقيق مستهدفات رؤية 2030. (هيئة الحكومة الرقمية،2021، التحول الرقمي)

3-استراتيجيات الحوكمة والتحول الرقمي: (هيئة الحكومة الرقمية،2021، التحول الرقمي)

بناء على (المنصة الوطنية الموحدة) تتركز استراتيجية التحول الرقمي في المملكة العربية السعودية في أربع خطط استراتيجية:

- **الخطة الاستراتيجية الرقمية الأولى (2006-2010)**

تم إصدار الخطة الاستراتيجية الرقمية الأولى من قبل الحكومة عام 2006، حيث تم التركيز على تقديم خدمات إلكترونية عالية الجودة للمواطنين وجعلها سهلة الوصول إليها من أي مكان وفي أي وقت، وتحسين الكفاءة والفاعلية في القطاع الحكومي. تتضمن هذه الخطة تفاصيل فنية حول مكونات إطار عمل الحكومة الإلكترونية، التي تم استخدامها في النسخة السابقة من هيئة الخدمات عبر الإنترنت المسماة "يسر".

- **خطة العمل الثانية: (2012 - 2016)**

تم تطوير خطة العمل الثانية للحكومة الإلكترونية (2012-2016) كتحديث للخطة الاستراتيجية الرقمية السابقة، حيث تم التركيز على ثلاثة أهداف رئيسية. تهدف الأهداف الرئيسية إلى بناء قوة عاملة مستدامة للحكومة الإلكترونية وتحسين تجربة المواطنين مع الجهات الحكومية، كما يتضمن التطوير في ثقافة التعاون والابتكار لتعزيز كفاءة الخدمات الحكومية المقدمة. تم تضمين الاستراتيجية الأسس الخاصة بالمشاركة الإلكترونية والخدمات الإلكترونية والتطبيقات الوطنية المشتركة والبنية التحتية وإدارة التغيير. نفذت الحكومة الاستراتيجية بالتعاون مع الجهات الحكومية والجامعات والقطاع الخاص وممثلي المجتمع المدني، وتم دعم الحكومة من قبل الشركات الاستشارية والمستشارين الدوليين في هذا المجال.

- **الخطة الاستراتيجية الأولية للحكومة الذكية: (2020 – 2022)**

تم إقرار الخطة الاستراتيجية الأولية للحكومة الذكية في المملكة العربية السعودية للفترة من 2020 إلى 2022، بهدف تحقيق أهداف التنمية المستدامة ورؤية المملكة 2030. تم وضع العديد من المبادرات لتحقيق هذه الأهداف من خلال تبني إجراءات وطرق مبتكرة. تسعى هذه الخطة لتحقيق قفزة نوعية في التحول الرقمي للجهات الحكومية وإنشاء قدرات حكومية ذكية عالمية المستوى. كما تهدف الخطة إلى توفير تجربة خدمة ذكية موحدة وعالمية المستوى للمواطنين، وتمكين جميع موظفي الخدمة العامة من القدرات الذكية والمبتكرة، وتمكين القوى العاملة الرقمية وتقديم المستقبل، وتحقيق التحول الرقمي السريع والواضح من خلال بيئة تعاونية قوية بين الشركاء واستخدام الموارد المشتركة لتحقيق أقصى استفادة بأقل تكلفة.

- **الاستراتيجية الوطنية للحكومة الرقمية (2022- 2025)**

تم تطوير استراتيجية الحكومة الرقمية في المملكة العربية السعودية للفترة 2022-2025، بناءً على رؤية المملكة 2030. الهدف الأسمى من الاستراتيجية هو بناء حكومة رقمية متقدمة تعمل على تحقيق التميز في الخدمات الحكومية الرقمية، وتم تقسيمها إلى مرحلتين؛ المرحلة الأولى تهدف إلى بناء حكومة المستقبل الرقمية وتطبيق الحوكمة والتنظيم، فيما تستهدف المرحلة الثانية تحقيق الريادة العالمية في الخدمات الحكومية الرقمية. تشمل الاستراتيجية إرساء بنية رقمية قوية ومتطورة وتطوير حلول مبتكرة ومرنة لتقديم الخدمات الحكومية الرقمية والاستفادة من التقنيات في عملية صنع القرار وإشراك المستفيدين.

4 -قواعد التحول الرقمي في المنظمات العامة الخدمية:

وتتلخص قواعد التحول الرقمي في المنظمات العامة الخدمية في التالي: (شديد،2021، تأثير التحول الرقمي على مستوى أداء الخدمة المقدمة بالتطبيق على موظفي الإدارة العامة للمرور بمحافظة القاهرة)

- تحسين تنظيم الخدمات وتسهيل عملية الوصول إليها، بالإضافة إلى تعزيز الوعي حول كيفية الاستفادة منها.
- تفصيل دور كل من مقدم ومتلقي الخدمة، والترويج لاستخدام الخدمات الإلكترونية.
- تحسين سرعة وأمان العمليات والخصوصية في جمع وتحليل المعلومات.
- تقليل تدخل العنصر البشري في عمليات الخدمة لتحسين جودتها وتفادي الأخطاء.
- تطوير قابلية التحديث من خلال التعاون لتحسين جودة الخدمات.
- تطبيق معايير حوكمة شفافة ومنصفة لزيادة الثقة في الخدمات الحكومية

5 - مميزات التحول الرقمي: (حاج، قاسم علي، 2020، إسهامات الاتحاد الإفريقي في عملية التحول الرقمي في إفريقيا قراءة في مشروع استراتيجية التحول الرقمي لإفريقيا)

إعادة صياغة الشكل الذي يعيش ويعمل فيه الأفراد، باستخدام التقنيات المتاحة، مع التخطيط المستمر والتطوير المستمر لتجربة المستخدم.

- تحقيق تغيير جذري في الخدمات الصحية والتعليمية والأمنية والسلامة المقدمة للأفراد، وتحسين تجاربهم وزيادة إنتاجيتهم.

- الاستفادة من التقنيات الحديثة بشكل أكثر تفهما ومرونة في العمل والقدرة على التنبؤ والتخطيط للمستقبل.
- تمكين الابتكار بشكل أسرع لتحقيق النتائج المرجوة والتحرك نحو النجاح.
- تطوير استراتيجية لتحقيق قيمة تنافسية أعلى، وفرق عمل متطورة، وثقافة دائمة للإبداع

6 - التحول الرقمي باستخدام المنهجية المرنة: (أجيال، 2023. التحول الرقمي باستخدام المنهجية المرنة)

تعددت التقنيات التي يمكن الاعتماد عليها في التحول الرقمي وتختلف هذه التقنيات كل حسب الرؤية

والاستراتيجية التي تم وضعها، وبناء على المنصة الوطنية الموحدة فإن أهم هذه التقنيات هي:

1. إنترنت الأشياء (IoT)
2. استراتيجية حماية البيانات والخصوصية
3. الذكاء الاصطناعي
4. البيانات الضخمة والبيانات المفتوحة
5. تطبيقات سلسلة الكتل (Block chain)
6. سياسات التقنية القائمة على محرك الجيل الخامس
7. وضع الحماية التنظيمي (Sandboxes)
8. الروبوتات والأتمتة
9. التطبيقات السحابية الحكومية كخدمة (IAAS)

7- ضرورة التحول الرقمي:

أصبحت الحاجة إلى التحول الرقمي ضرورية لجميع المؤسسات والهيئات التي تسعى للتحسين وتسهيل الوصول إلى خدماتها من قبل المستفيدين. وليس التحول الرقمي مجرد تطبيق التكنولوجيا داخل المؤسسة، بل هو برنامج شامل يشمل جميع جوانب المؤسسة وطريقة عملها الداخلية والخارجية، لتحسين وتسريع تقديم الخدمات للجمهور المستهدف. بالإضافة إلى ذلك، يسهم التحول الرقمي في ربط القطاعات الحكومية والخاصة ببعضها البعض، مما يسمح بسلاسة تنفيذ الأعمال المشتركة. ونظرًا للتطور المستمر في استخدام وسائل تكنولوجيا المعلومات في جميع جوانب الحياة، فقد أصبح التحول الرقمي أكثر إلحاحًا لجميع المؤسسات والهيئات والشركات. لذلك، توجد ضغوط من كافة شرائح المجتمع لتحسين خدماتها وتوفيرها على جميع القنوات الرقمية. (صيفي، حسنية، 2020، الإدارة الإلكترونية الصحية وتحديات التحول الرقمي في الدول العربية-دراسة حالة مملكة البحرين)

وتتجلى أهمية التحول الرقمي حسب (رشوان وقاسم، 2020، دور التحول الرقمي في رفع كفاءة أداء البنوك وجذب الاستثمارات) في في النقاط الآتية:

- تحسين كفاءة وتنظيم العمليات وتوفير التكلفة والجهد بشكل كبير.
- تشجيع التقديم على خدمات مبتكرة وإبداعية بعيدًا عن الطرق التقليدية لتحسين تجربة المستفيدين.
- تحسين جودة الخدمات وتبسيط الإجراءات لتسهيل الحصول على الخدمات المقدمة.

- دعم التوسع والانتشار للوصول إلى فئات أكبر من العملاء والمستفيدين.
- زيادة كفاءة وفعالية الوظائف والخدمات الحكومية، والحد من الازدواجية غير الضرورية ومكافحة الاحتيال والفساد.
- تعزيز الأمن وتتبع المعاملات وتحسين المشاركة والمساءلة المدنية.
- توفير منصات تجارية فعالة لمساعدة الشركات على توسيع وصولها إلى الأسواق وتبادل السلع والاستفادة من الأصول والموارد البشرية غير المستغلة، مما يساهم في خلق المزيد من الوظائف وتعزيز الاقتصاد.

8 - فوائد التحول الرقمي:

يقدم التحول الرقمي فوائد عديدة بالنسبة للأفراد وللمنظمات أبرزها: (الهادي، 2022، ص 166)

- استبدال العمليات التقليدية بالرقمية.
- زيادة وقت التفكير في التطوير.
- تغيير نماذج العمل وتغيير العقليات.
- زيادة كفاءة سير العمل وتقليل الأخطاء.
- تسريع طريقة العمل اليومية.
- تطبيق خدمات جديدة بسرعة ومرونة.
- تحسين الجودة وتطوير الأداء.
- زيادة رضا المستفيدين.
- تقديم خدمات بوقت أقصر وجودة أفضل.

وبمجرد تطبيق هذه المفاهيم ستكون كم هائل من البيانات والمعلومات التي ستساعد بدورها متخذي القرار في هذه المؤسسات على مراقبة الأداء وتحسين جودة خدماتها بالإضافة إلى تحليل هذه البيانات والمعلومات التي ستسهل اتخاذ القرار وتحديد الأهداف والاستراتيجيات.

المحور الثاني: التحول الرقمي في وزارة المالية بالمملكة العربية السعودية:

"تفعيلًا وتأسيًا بتوجه المملكة العربية السعودية للتعاملات الإلكترونية والتحول الرقمي لتقديم الخدمات التي تقدمها الجهات الحكومية دأبت وزارة المالية إلى التحول الرقمي وتطوير خطتها لذلك عبر برنامج متكامل من التطبيقات والحلول والبنى التحتية التي تسهم في تحقيق منظومة رقمية متكاملة، ولتعزيز هذا التحول أطلقت المالية منصة خدمات الأفراد "المواطن والمقيم" لتنفيذ معاملات الأفراد إلكترونيا في الوزارة لتقليص الوقت والجهد لمراجعي الوزارة وأصحاب المصلحة تحقيقًا للأهداف الاتية:

- التحول الرقمي لمعاملات الأفراد
- تحسين تصنيف المملكة العربية السعودية في المعايير الدولية
- قياس مؤشرات الأداء لخدمات الأفراد بالوزارة
- توفير البيئة الآمنة للخدمات الرقمية

وله عدة مزايا:

- إبراز الخدمات الإلكترونية بشكل أكبر
- سهولة الاستخدام وسرعة في التصفح
- سهولة الوصول والتسجيل في خدمات الوزارة
- تقديم الدعم من خلال المحادثات المباشرة
- تطبيق المعايير العالمية
- تطوير التصميم حسب التوجهات العالمية للبوابات الإلكترونية

حيث تقدم منصة الأفراد حزمة من الخدمات وهي:

أ- خدمة استعلام مراجعي الإدارة العامة للمصروفات: حيث تسمح هذه الخدمة لمراجعي الإدارة العامة الاستعلام عن حالة الطلب "مساعدات واضرار وأخرى" وهي خدمة خارجية مقدمة من الوزارة لجميع المستفيدين أفراد وشركات تسهل الاستخبار عن طلب مساعدة او تعويض عن أضرار وذلك بإدخال رقم الهوية وتاريخ الميلاد وسنة الطلب حتى تظهر تفاصيل حالة الطلب

ب- نموذج أعفاء المتوفين: هذه الخدمة لتقديم طلب اعفاء المتوفين من القروض المتبقية لكل من صندوق التنمية العقارية او التنمية الزراعي او الاجتماعي وذلك بحسب المعلومات المطلوبة مثل: رقم الهوية، نوع القرض، اسم المقترض رباعيًا، رقم الحفيظة ومصدرها وتاريخها ورقم العقد، مكان القرض وغيرها

ت- الاستعلام عن أوامر الدفع: خدمة خارجية لجميع المستفيدين منهم الأفراد لتسهيل معرفة أوامر الدفع الصادرة لهم وذلك بإدخال رقم امر الدفع

ث- رفع مسوغات صرف العوائد السنوية: هذه الخدمة تتيح رفع مسوغات صرف العوائد وتفاصيل صرف العوائد ومعرفة حالة الطلب مقبول ومرفوض وذلك بإدخال رقم الهوية لصاحب العادة المتوفي

ج- الاستعلام عن العوائد السنوية: خدمة متاحة للاستعلام عن نظام وتفاصيل المقررات والعوائد

ح- حجز موعد لمراجعي الإدارة العامة للمقررات والقواعد: وهي خدمة متاحة لـ "لاعتباري، قاصر، عائلة و..الخ" من مراجعي الإدارة لحجز موعد بما يتناسب مع شهر الصرف

خ- خدمة الاستعلام عن إعفاءات القروض: وهي لمعرفة البيانات الخاصة بالإعفاء مثل رقم طلب الاعفاء وتاريخ التقديم وحالته إذا مرفوض او مقبول وأسباب الرفض

د- متابعة المعاملات المقدمة للوزارة: حيث تمكن المستخدمين من متابعة المعاملات المقدمة للوزارة بواسطة رقم القيد ورقم الخطاب دون زيارة الوزارة

من جانب اخر تدعما للتحول الرقمي يوجد لدى وزارة المالية (برنامج ذكاء الأعمال) بحكم ان المالية ركيزة أساسية ومحور مهم في دعم اتخاذ القرار مما يجعل دقة المعلومة والتقارير الإحصائية حولها عامل محوري، وهذا البرنامج يعمل على توظيف في استخدام المعلومات اللحظية الدقيقة ذات قيمة نوعية عالية متعلقة بأعمال الوزارة وبيانات ذات اعتمادية "موثوقية" كبيرة متوفرة من عدة مصادر مما يساعد على اتخاذ القرار الصحيح في الوقت المناسب لتطبيقه بالشكل والأسلوب الصحيح. " (هيئة الاتصالات وتقنية المعلومات،2023، التحول الرقمي في وزارة المالية في المملكة العربية السعودية)

المحور الثالث: مخاطر التحول الرقمي:

مخاطر التحول الرقمي:

أ- هناك مجموعة من المخاطر المرتبطة بعملية التحول الرقمي التي تستحق الانتباه، ومن بينها:

- الاعتماد الكبير على التقنيات الرقمية، وهو ما يؤدي إلى زيادة الضعف الأمني وفتح الباب أمام الهجمات السيبرانية.
- ازدياد حجم المواقع المستهدفة بسبب ارتفاع عدد الأجهزة المتصلة، مما يزيد من احتمالية الهجمات السيبرانية.
- تعقيد الهجمات السيبرانية، حيث تصبح هذه الهجمات أكثر تطوراً وإتقاناً، ما يزيد من صعوبة مكافحتها.
- تجاوز الابتكار الرقمي لتدابير الأمن السيبراني، حيث تتم تطوير تقنيات جديدة ومبتكرة بوتيرة أسرع من تطوير الإجراءات الأمنية المتبعة.
- الاندماج بين النظم تكنولوجيا المعلومات والتكنولوجيا التشغيلية وانترنت الأشياء، وهو ما يؤدي إلى تزايد تعقيد الأمور وتحديات جديدة.

وبناءً على ذلك، يتبين أن الأمن السيبراني يلعب دورًا حاسمًا في ضمان نجاح عملية التحول الرقمي، إذ يتضمن حماية المعلومات والخدمات والأجهزة الحاسوبية من التهديدات السيبرانية. تتم هذه العملية بواسطة تطبيق مجموعة من الوسائل التقنية والإدارية والتنظيمية، حيث تهدف جميعها إلى حماية البيانات الإلكترونية وأنظمة الاتصالات والمعلومات من الاستخدام غير المصرح به وضمان سلامتها. وعليه، فإن الفضاء السيبراني يمتد إلى شبكات عالمية وخاصة أخرى / GPS ACARS/Swift/GSM/PSTN، ولا يقتصر فقط على شبكة الإنترنت. (الربيعة، 2013، الأمن الرقمي وحماية المستخدم من مخاطر الانترانت).

ب- والهدف المنشود من الأمن السيبراني يتمثل في: (الربيعة، 2013، الأمن الرقمي وحماية المستخدم من مخاطر الانترانت).

- تأمين توافر مستمر لأنظمة المعلومات وتشغيلها بشكل فعال.
- حماية أنظمة التشغيل من أي محاولات غير مصرح بها للوصول إليها واستخدامها لأغراض خبيثة.
- العمل على حماية البنية التحتية الحساسة ومصالح الدولة والأمن الوطني.
- اتخاذ كافة التدابير اللازمة لحماية المستخدمين والمستهلكين من المخاطر المحتملة عبر استخدامهم للإنترنت.
- تعزيز حماية الشبكات وتأمينها بطرق فعالة.
- تعزيز السرية والخصوصية للبيانات الشخصية وضمان عدم وصولها لأطراف غير مصرح بها.
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها، بما في ذلك الأجهزة والبرمجيات والخدمات والبيانات التي تحتويها.

ج- وتزايدت التحديات في البيئة الرقمية، وبالتالي انبثقت الحاجة لتطوير حلول فعالة لمواجهتها، ومن هذه التحديات:

- استهداف قطاع الخدمات المالية بالهجمات الإلكترونية
- الجرائم الإلكترونية التي تستهدف الحكومات وتركز على تدمير البنية التحتية لمواقعها وأنظمة شبكاتها، وكذلك جريمة الاختراق والبقاء غير المشروع.

- جرائم الإلكترونية التي تستهدف الملكية الفكرية، مثل التعدي على التصميم والنموذج.
- جرائم الاحتيال والاعتداء على الأموال، مثل إدخال بيانات غير صحيحة أو تعليمات من غير المصرح بها، أو استخدام بيانات وعمليات غير مسموح بها بغية السرقة من قبل موظفين فاسدين في الشركات والمؤسسات المالية.
- جرائم الابتزاز الإلكتروني.
- الاستخدام غير المشروع لأدوات الدفع الإلكتروني.
- اختراق المواقع التجارية وتسبب الخسائر المادية الضخمة.
- جرائم سرقة البطاقات الائتمانية.
- جرائم النصب والاحتيال في التجارة الإلكترونية.

أثرت الهوية والقيمة المعلوماتية بشكل جذري بفعل التقنية الرقمية الحديثة، حيث أصبح من السهل تخطي الحواجز الأمنية التي تحمي المعلومات الرقمية، مما يجعل إجراءات الأمن المعلوماتي والحماية شرطًا أساسيًا للوقاية من الهجمات الإلكترونية الفيروسية والتجسسية التي تستهدف المؤسسات والشركات. يعمل الاعتماد على البيانات الضخمة والتحليلات التنبؤية على تقليل معدلات ارتكاب الجرائم بشكل كبير، وبذلك تساهم التكنولوجيا الرقمية في إدارة المخاطر بشكل جديد.

ونظراً للمخاطر الناتجة عن التحول الرقمي، يتعين على الدول إعادة النظر في تدابير الأمن الإلكتروني، خاصةً وأن الابتكار الرقمي تفوق تلك الإجراءات. ومن ناحية أخرى، يتعين أن تكون المنظومة التشريعية متطابقة مع هذه التحولات، لضمان مكافحة الجرائم والهجمات الإلكترونية. وبما أن الانتقال إلى عالم الاقتصاد الرقمي يتطلب بيئة تشريعية مناسبة لتوفير الحماية والأمان، فإنه من الضروري تطوير هذه البيئة التشريعية بالتوازي مع التحول الرقمي. (جميلة سلايمي، واخرون، 2019،ص 945)

المحور الرابع: إدارة المخاطر الرقمية

"الرقمية الحديثة وتكنولوجيا المعلومات قدمت منافع و فوائد جمّة على كافة الاصعدة سواء للفرد او الكيانات الاعتبارية او الدول من ناحية العمل والانتاجية والكفاءة وغيرها وأصبحت لاعب أساسي في التنافس والابتكار وتحسين اسلوب الحياة، الا انه لكل شيء ضريبة والرقمية ضريبتها هي المخاطر الناجمة عنها لذا تمخض مفهوم إدارة المخاطر الرقمية واصبح موضع الكثير من البحث و التطوير، ويمكن تعريف إدارة المخاطر الرقمية حسب الجمعية المهنية الدولية لحوكمة تكنولوجيا المعلومات [ISACA]: "عملية تحديد نقاط الضعف والتهديدات لموارد المعلومات التي تستخدمها اي جهة او مؤسسة في تحقيق أهدافها وتحديد الاجراءات المضادة التي يجب اتخاذها للحد من المخاطر المستوى مقبول بناء على قيمة موارد المعلومات للمؤسسة" فكما هو موضح بأن يتم تحديد الاحداث والأخطار المتوقعة جراء استخدام التقنية ويتم اتخاذ القرار في ضوء المعرفة المسبقة للخطر لتقليل الأثر السلبي إلى اقل حد والأخطار التي تحصل من العصر الرقمي متنوعة ومتجددة بحكم النمو المطرد والمتغير للرقمية." (الموسوي، 2013، الخصوصية المعلوماتية واهميتها والتقنيات الحديثة عليها)

"حتى يتم إدارة خطر الترقيم يجب تحليل النظام وتحديد الأخطار المتوقع حدوثها واحتمالاتها وتأثيرها حسب نسق علمي معين وعلى الخبرة السابقة في ظل عدم وجود معلومات كافية بعدها يتم تعيين الأساليب المتبعة للقضاء بشكل شامل او جزئي على

الخطر من أجل اتخاذ قرار مناسب، إدارة المخاطر الرقمية تمر بعدة خطوات بهدف تفادي الخسارة وحدوثها وتمويلها في حالة وقوعها ونشر التوعية لجميع الأطراف المتعاملة:

أ- تحديد أسباب الخطر وتحليلها: في هذه المرحلة يتم ذكر جميع الأحداث والمواقف التي ينتج عنها خسارة وتحديد الأسباب الأخرى للخسارة ومؤثرات الخسارة، فمخاطر التحول الرقمي عديدة وكثيرة مثل انتهاك خصوصية المعلومات، خطر عدم كشف الهوية، العزلة الاجتماعية، اختراق المواقع الإلكترونية، الإرهاب الإلكتروني، التجسس الإلكتروني، ويتم تحديد أيضا العوامل التي تزيد من حجم الخسارة والتي منها: الاعتماد الكلي على التقنية، ازدياد حجم المواقع المستهدفة بسبب كثرة الاتصال بالأجهزة، ازدياد اعقد الهجمات الإلكترونية، تجاوز الابتكار الرقمي لتدابير الأمن الإلكتروني، الاندماج بين نظم التكنولوجيا وإنترنت الأشياء و تكنولوجيا التشغيل

ب- تقييم المخاطر الرقمية: بعد تحديد التهديدات في هذه المرحلة يتم حساب احتمال حدوث التهديد وحجم الخسارة المحتملة وتحديد التكاليف لكل حدث بحيث ترتب تنازليًا لأسباب الخسارة حسب درجة الخطر ولحساب درجة الخطر هناك أساليب كمية ووصفية بحكم عدم توافر المعلومات الكمية او عدم صلاحيتها دائما بسبب حدوث تغيرات جوهرية يتم الاعتماد على الأسلوب الوصفي وهو التقدير الشخصي حيث تصنف المخاطر حسب محورين:

- معدل تكرار الحوادث
- حجم الخسارة المتوقعة

ويتم استخدام مقياس وصفي تصاعدي او تنازلي-ثلاثي او خماسي او غير ذلك-على ان يتم اعطاء قيم رقمية لكل حالة تعكس الخطورة النسبية لها حتى يتم تحديد الالية المناسبة للتعامل مع الخطر

ج- سياسات إدارة المخاطر الرقمية: بناء على الخطوتين السابقتين والمعلومات المتحصل منها يتم في ضوئها تحديد ما يلزم من تعديل او تغيير في نموذج العمل واختيار المناسب من الأدوات التي تمكن من تنفيذ مهام العمل على الانترنت والقيام بكل العمليات ويتم عن طريق عدة عوامل مثل: تكلفة، السهولة، الأمان، المقدرات التقنية للفريق والفئات المستهدفة على حد سواء، والتغيرات التي تحصل قد تكون في الرؤية والرسالة والاهداف وخطة العمل والميزانية حيث ان هذه التعديلات تنسجم مع التسارع والسباق التقني المحموم لتحقيق الأهداف بواسطة الرقمية وتقليل الاثار السلبية والاضرار إلى اقل قدر ممكن، نستنتج ان التحول الرقمي والتقنية الحديثة يؤدي إلى رفع مستوى وظيفة إدارة المخاطر واستحداث مسمى وظيفي جديد "مدير المخاطر الرقمية" تعنى بالعمليات الرقمية لتوفير الدعم اللازم من اجل ديمومية نشاط الجهة دون تعثر تقني وتحسين تحليل الخطر الذي يؤثر على الأداء المالي والتشغيلي للجهة التي قد تعيق عن تحقيق الاستراتيجية او تطوير الأداء او تحسين جودة العمليات الرقمية، لذا العمل على إدارة المخاطر الرقمية ضروري لتقليل الأثر السلبي المترتب على استخدام التقنية وتحديد الضوابط والسياسات لتعزيز كفاءة الكيان بشكل سبّاق ومن هذا المنطلق يجب الاعتناء بتطوير نظام إدارة المخاطر الرقمية بشكل كفء لتحديد وتحليل المخاطر الرقمية المستقبلية جيدًا، وهناك متطلبات للجهات الراغبة بإنشاء إدارة المخاطر الرقمية وهي ما يلي:

- فهم نطاق عمل الجهة ومسؤولياتها
- تعريف صلاحيات ومسؤوليات أصحاب المصلحة
- تحديد نطاق وأهداف إدارة المخاطر بوضوح

- اختيار مؤشرات الأداء الرئيسية
- تحديد وتيرة إعداد التقارير والتواصل
- المواءمة مع أنظمة الحوكمة
- إدراك وتلبية احتياجات أصحاب المصلحة

في المملكة العربية السعودية دأبت هيئة الحكومة الرقمية على تسخير الطريق للجهات الحكومية حتى توفر الأخيرة خدمات رقمية ذات جودة وكفاءة عالية تسهم بقيمة مضافة على الاقتصاد الوطني، فهذه الهيئة هي المرجع الأساسي لشؤون التحول الرقمي حيث وضعت المعايير والضوابط التنظيمية للتحول الرقمي للكيانات العامة واعداد ضوابط لإدارة المخاطر الرقمية للتحقيق الاستدامة، وضوابط إدارة المخاطر الرقمية على النحو التالي:

1- الضوابط الخاصة بمرحلة بناء إدارة المخاطر

أ- بناء سياسة وحوكمة إدارة المخاطر وتحديد أدوار ومهام الأشخاص المعنيين والاقسام المعنية لتخطيط وتنفيذ ومراجعة وتطوير إدارة المخاطر والمواءمة مع استراتيجية الجهة. وعلى من يقدم خدمة رقمية الالتزام بالآتي:

- تعيين مدير إدارة مخاطر ذو كفاءات وجدارات مناسبة لإتمام مهامه
- تعيين فريق لإدارة المخاطر مؤهلين لإتمام المسؤوليات ومهام العمل بشكل كافي
- التأكد من ان مدير المخاطر يعمل على بناء وتشغيل إدارة مخاطر متسقة مع سياسة الإدارة العليا
- تعيين لجنة توجيهية مشرفة عن نظام إدارة المخاطر بالكيان برئاسة رئيس المنظمة وتوثيق الميثاق مع الالتزام بنطاق اللجنة، تحديد الرئيس والأعضاء، تحديد صلاحيات اللجنة، تحديد أدوار ومسؤوليات اللجنة، مراجعة ميثاق اللجنة بشكل دوري
- إرفاق سجل إدارة المخاطر للإدارة العليا أو اللجنة التوجيهية
- بناء سياسة إدارة المخاطر وعمل تحديث بشكل مستمر، حيث تتضمن السياسة المنظور الاستراتيجي، دعم رؤية 2030م، تعريف إدارة الخطر، نطاق إدارة المخاطر، آلية حوكمة إدارة المخاطر، هيكل وموارد إدارة المخاطر، بيان سياسة إدارة المخاطر، توضيح مهام الأطراف ذات العلاقة، تبيين طريقة مراجعة السياسة، اعتمادها من الرئيس، تطبيقها على الجهة، يلزم تكوين نظام نشط لإدارة المخاطر ويشمل ما يلي: هيكل وسياسة واستراتيجية إدارة المخاطر، حدود تحمل المخاطر، إجراءات المخاطر، تقييم المخاطر، معالجة المخاطر، مراقبة المخاطر، التدريب والتوعية، التحسين

ب- إعداد استراتيجية إدارة المخاطر لتسهيل عملية تنسيق الأهداف الاستراتيجية وعلى الجهة الالتزام بما يلي:

- تقييم مستوى إدارة المخاطر وبناء خطة عمل لرفع مستوى نضج المنظمة في إدارة المخاطر
- إنشاء واعتماد استراتيجية إدارة المخاطر واتساقها مع استراتيجية الكيان بالتقيد بالآتي: رؤية ورسالة إدارة المخاطر، أهداف إدارة المخاطر، انسجام استراتيجية إدارة المخاطر مع استراتيجية الجهة واستراتيجية الرؤية 2030م، الاعتماد من الرئيس، تطبيقها على الكيان كامل، مراجعتها مرة في السنة على اقل تقدير او عند حدوث تغيير جوهري في الجهة، تحديد الموارد لتنفيذها

ت- تحديد قدرة الجهة على تحمل المخاطر وتمكينها من تحديد الأولوية للعلاج وعمل توثيق لحدود تقبل المخاطر مع الالتزام بما يلي: تعريف درجة تحمل الخطر، تحديد منهجية حدود تقبل المخاطر، تحديد درجة الخطر، الاتساق بين درجة تقبل

ISSN: 2706-6495

الخطر ومصفوفة المخاطر، الاعتماد من الرئيس والتطبيق على المنشأة ككل، المراجعة مرة واحدة على الأقل او حدوث تعديل جوهري في المنظمة، المواءمة بين درجة تحمل الخطر مع استراتيجية الجهة

ث- إجراءات إدارة المخاطر لتحديد وتقييم وتحليل التهديدات الداخلية والخارجية مع الآليات المستخدمة للتخفيف من الاحتمالية والعلاج من الآثار، ويعمل تحديث مستمر مع الالتزام بالتالي:

- تحديد نطاق وأهداف وسياق ومعايير إدارة المخاطر في الكيان
- تعيين درجات احتمالية الحدوث وأثرها على الجانب التشغيلي او المالي او القانوني او السمعة وغيرها
- تحديد مصفوفة المخاطر
- تحديد نهج لتحليل وتقييم المخاطر الداخلية والخارجية
- اختيار طرق لمعالجة المخاطر او التقليل من الأثر السلبي
- تحديد مقاييس تأثير المخاطر على عمليات الجهة
- تصنيف التهديدات بما يتوافق مع هيكلة المنظمة
- اختيار نهج المراجعة والمتابعة
- التوافق بين إطار إدارة المخاطر والخدمات المقدمة من الجهة
- التعميد من الرئيس والتنفيذ على المنشأة ككل
- مراجعة الإطار مرة واحدة على الأقل

2- ضوابط مرحلة تقييم ومعالجة المخاطر:

أ- تقييم التهديدات واحتمالية وقوعها وأثرها المتوقع على الأهداف والاستراتيجيات والجهة التي تطرح خدمة رقمية تكن ملزمة بالتالي:

- تحديد الأخطار الداخلية والخارجية بشكل مستمر التي قد تؤثر على الغايات والاستراتيجيات
- تحديد كل من المسببات الرئيسية والنتائج المتحصلة من المخاطر والأحداث
- ذكر وربط الأخطار والحوادث بالغايات الاستراتيجية والتشغيلية للكيان
- رصد مالك الخطر
- تسجيل تاريخ تحديد الخطر
- توثيق تصنيفات الخطر
- ذكر تفاصيل التهديد في سجل المخاطر
- تحديد المخاطر بشكل مستمر
- تحليل المخاطر بشكل مستمر ويتطلب التقيد بالآتي:
  - ❖ رصد رتبة الخطر الكامنة بواسطة الاحتمال والأثر
  - ❖ تحديد الضوابط الرقابية
  - ❖ تقييم فعالية الضوابط الرقابية

- ❖ توثيق درجة الخطر المتبقية بواسطة الاحتمال والاثر
- ❖ تحديد أولوية واهمية المخاطر
- ❖ تحديد آلية معالجة المخاطر
- ❖ توثيق مؤشرات المخاطر الرئيسية KRI
- ❖ جمع المعلومات وذكرها في سجل المخاطر
- ❖ تحليل التهديدات بشكل دوري
- ❖ رصد إثر الخطر على عمليات الجهة
- ❖ عرض متحصلات تحديد وتقييم المخاطر على اللجنة التوجيهية لإدارة المخاطر

ب- وضع العلاج الأمثل للمخاطر لتذليل احتمال الحدوث أو تخفيض الاثار، وحتى يتسنى للجهة من تحديد طرق الاستجابة الفعالة يجب العمل بما هو آت:

- تحديد الاستراتيجية المناسبة للاستجابة للخطر
- وضع خطط الاستجابة بالتفصيل
- تعيين مالك خطط الاستجابة للخطر
- ذكر مصاريف وفوائد عند تحديد استراتيجيات الاستجابة
- عرض نتيجة تحليل ومعالجة للخطر على اللجنة التوجيهية لإدارة المخاطر
- مراقبة وتقصي خطط الاستجابة بشكل دوري لضمان فعاليتها

ت- مراقبة الأخطار ومتابعتها لضمان تطوير جودة وفعالية عملية تقييم ومعالجة المخاطر مع التقيد بما يأتي:

- متابعة المتغيرات الداخلية والخارجية وتأثيرها على المخاطر للجهة بشكل دوري
- مراقبة الضوابط الرقابية وخطط الاستجابة وتقييم فعاليتها
- مراقبة مؤشرات المخاطر الرئيسية KRI ورفع التقارير الخاصة بها
- مراقبة المدة الزمنية المحددة لتطبيق آلية التفاعل مع المخاطر دوريًا

3- الضوابط الخاصة بمرحلة التدريب والتطوير

أ- تدريب الموظفين وأصحاب المصلحة ورفع الوعي بإدارة المخاطر للتأكد من تحقيق الأهداف واستراتيجيات المنظمة مع العمل بالآتي:

- تحليل الاحتياجات التدريبية بالتنسيق مع الموارد البشرية لدى الجهة
- تطبيق آلية للتدريب تناسب مسؤوليات الموظف في نظام إدارة المخاطر لدى الجهة
- نشر وإطلاق حملات توعية وثقافة إدارة المخاطر من خلال التدريب وورش العمل او اللافتات او الاجتماعات المفتوحة والتعلم القائم على الحاسوب ويجب على الموظفين يكونون على دراية بـ:
  - ❖ سياسة إدارة المخاطر
  - ❖ الأدوار والمسؤوليات ضمن نظام إدارة المخاطر
  - ❖ الأثر الناتج عن عدم دعم إدارة المخاطر

ب- توثيق الدرس المستقصي من تطبيق نظام إدارة المخاطر وتطوير الإجراءات والعمليات للكيان لتحديد الخطر مسبقًا وتعديل عملية تقييم ومعالجة الخطر لترقية رتبة فعالية نظام إدارة المخاطر من خلال تنفيذ الممارسات والمعايير لعمل التطوير يكن مرة في السنة أو حصول تغيير جوهري للشؤون الداخلية للجهة والمخاطر الداخلية والخارجية للكيان ويتم رفع نتائج أعمال التدقيق الشامل إلى الإدارة العليا او الإشرافية لأخذ القرارات السليمة ولضمان ان تكون عملية التحسن مستمرة يكن عبر مدقق داخلي أو خارجي ذو كفاءات عالية بواسطة:

- التدقيق
- تقييم الأداء
- التقييم الذاتي
- المراجعة الإدارية "(موقع وزارة المالية بالمملكة العربية السعودية،2023، الضوابط الخاصة بالوزارة)

المحور الخامس: خصوصية المعلومات عموماً:

الخصوصية بصفة عامة، هي مقياس غير موضوعي، أي يختلف تعريفها وحدودها من بيئة إلى أخرى والصفة المشتركة في جميع التعريفات فهي منظور أن الخصوصية إحدى حقوق الإنسان في حياته، ولكنها تعتمد بشكل أساسي على البيئة والسياق. اما من وجهة نظر روجر كلارك، الاستشاري والخبير في خصوصية البيانات والأعمال الإلكترونية، عرف الخصوصية "بأنها قدرة الأشخاص على المحافظة على مساحتهم الشخصية في مأمن من التداخل من قبل منشأت او أشخاص آخرين" وقد قام بتحديد 4 مستويات لأبعاد من الخصوصية:

أ- خصوصية الشخص: وتعتبر المعنية بالفرد نفسه وموافقته على ما يرفق او يشارك من معلوماته وبياناته الخاصة.

ب- خصوصية السلوك الشخصي: ويتصل بكل من الجوانب السلوكية وبشكل خاص الأمور السياسية وغيرها وما يشار إلية في وسائل الخصوصية كما يطلق عليه.

ت- خصوصية الاتصالات الشخصية: يعرف بأنه مطابقة الأشخاص بالقدرة على الاتصال فيما بينهم دون المراقبة الروتينية من قبل أشخاص او منظمات، وهو ما يشار إليه احياناً باعتراض الخصوصية.

ث- خصوصية البيانات الشخصية: كما تعتبر بأن مطابقة الأشخاص بمعنى انه لا يمكن للشخص الحصول على بيانات ومعلومات خاصة للأفراد او المنظمات تلقائياً، وتعرف بأنها خصوصية المعلومات او خصوصية البيانات، كما عرفها روجر (بأنها رغبة الشخص بالتحكم، او على الأقل التأثير بشكل كبير في كيفية التعامل مع بياناته. (الموسوي،2013، الخصوصية المعلوماتية واهميتها والتقنيات الحديثة عليها)

وفي السنوات الأخيرة، أصبحت البيانات الضخمة موضوع بحث في غاية الأهمية فإن زيادة كمية البيانات الضخمة يزيد أيضًا من فرصة انتهاك خصوصية الأفراد، لذا يتم استخدام الأنظمة الموزعة ونظرًا لأن العديد من الأطراف متورطة في هذه الأنظمة، فإن ذلك يزيد خطر انتهاك الخصوصية. هناك عدد من آليات الحفاظ على الخصوصية التي تم تطويرها لحماية الخصوصية في مراحل مختلفة (على سبيل المثال، إنشاء البيانات وتخزين البيانات ومعالجة البيانات) لدورة حياة البيانات والهدف هو تقديم نظرة عامة شاملة عن الحفاظ على الخصوصية آليات البيانات الضخمة وعرض التحديات أمام الآليات القائمة.

على وجه الخصوص، لذا ستتضح البنية التحتية للبيانات الضخمة وآليات الحفاظ على الخصوصية الحديثة في كل مرحلة من دورة حياة البيانات الضخمة. (Chen.D , Zhao.H,2012, Data security and privacy protection issues in cloud computing)

ولا سيما بأن خصوصية البيانات لها أهميتها البالغة في كل النواحي والأجزاء لذا أدى النمو الهائل غير المسبوق في كمية بيانات المستهلك التي يجمعها المسؤولين عبر نقاط اتصال العملاء المختلفة إلى تحقيق حماية خصوصية البيانات أولوية رئيسية ,لذا تتطلب خصوصية البيانات على سبيل المثال في سياقات البيع بالتجزئة التقارب بين ثلاثة أصحاب مصلحة رئيسيين -المستهلك، تاجر التجزئة، والتنظيمية -لكل منها أدوار ووجهات نظر فريدة. مع منظور عالمي ونهج جمع البيانات متعدد الأساليب، والجمع بين مقابلات الخبراء المتعمقة، ومسح المستهلك على نطاق واسع عبر أربعة بلدان، ودراسات الحالة العالمية، لفهم تقارب اهتمامات أصحاب المصلحة الثلاثة هؤلاء: (1) البيانات الضخمة كمحرك لأداء علاقات العملاء، (2) التأثيرات العميقة للتنظيم، (3) حماية الخصوصية كاستراتيجية استباقية قد تؤدي فرص البحث المحددة بدورها إلى تعزيز فهم أعمق لأصحاب المصلحة هؤلاء، وجهات نظرهم وتقاربهم. (KellyD, and others,2020, Date Privacy in Retail)

يوجد العديد من الأنواع للمعلومات ولكن يعتبر الاهم هي الخاصة كونها تحمل بيانات خاصة جداً وتتعلق بالشخص ذاته ويطلق عليها خاصة كونها تنتمي إلى كيانه كإنسان مثل البيانات الشخصية الخاصة ذات خصوصية عالية للأفراد كالاسم والعنوان والحساب البنكي وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلتصق بكل شخص فتعتبر عالية الخصوصية بعضها قابله للتعريف والآخرئ غير معرفه للأخرين. وتعتبر المعلومات النوعية طبقاً للتحول الرقمي وفي وقتنا الحاضر لها دور كبير وضخم جداً من الأهمية في ظل فلسفة المعلوماتية المعاصرة، لا يمكن لها السير في التطور ومواكبة اهتمامات الإنسان سوى باستخدام المعلومات لذا أصبح لدينا ما يعرف بالخصوصية المعلوماتية. ولذا فأن مبدأ الخصوصية المعلوماتية ما يقصد به حق الشخص في أن يتحكم بالمعلومات التي تخصه من المبادئ القديمة للحفاظ عليها من التجسس الإلكتروني أو الاحتيال لها سوا كانت معلومات سرية جداً او ذات مدلولات شخصية كالصور الشخصية وغيرها وغالباً ما يتم ذلك إلا لمعرفة معلومات سرية لدى مؤسسات كبرى او شخصيات مثيرة للجدل، وايضاً يتم بين الدول بعضها لبعض، ويستخدم عادة احدث الوسائل والتقنيات المتطورة للقيام بالتجسس الإلكتروني والوصول إلى الاحتيال للحصول على ما يراد معرفته والحصول عليها بطرق غير نظامية ما يمثل مخاطر كبيرة للدول و الوزارات والمؤسسات والأفراد ايضاً ويكون اكثر عرضه لها من المنافسين. وعليه يمكننا القول أن خصوصية المعلومات هي:

بوجه عام قائم ما بين اصطلاح خصوصية المعلومات وحماية البيانات، فأما شيوع استخدام اصطلاح الخصوصية مستقلا ومنفردا دون دمجه بالبيانات في العالم الإلكترونية للدلالة على حماية البيانات واستخدامه، لذلك هذا الامر يرجع إلى ان مصطلح الخصوصية شاع وظهر واصبح عالي الأهمية بوقعه هذا في ظل تزايد المخاطر التقنية إلى مدى ارتبط بها في الاستخدام وكأنه ينحصر في نطاقها وبيئتها، وهو طبعا ليس كذلك، لكن ربما لأن أشد ما يمكن أن يمثل تشابه على هذا الحق وانتهاكا له، هو الوسائل التقنية ومخاطر المعالجة الآلية للبيانات، ويعتبر ايضاً ان استخدام اصطلاح الخصوصية في بيئة مواقع الإنترنت ومسائل عقود التقنية او خدمات التقنية عموما يشير إلى حماية الخصوصية المعلوماتية او حماية البيانات.

لذا فتعتبر الخصوصية حق للشخص أساسي، طبقاً لذلك فأنهم يعتقدون ان القوانين مازالت قادرة على حماية الأفراد من ان تنتهك خصوصيتهم من خلال الانتهاكات الإلكترونية، وحتى ان كانوا يقرون بالصعوبات التي تحول دون حماية هذا الحق بشكل مطلق. (الموسوي،2013، الخصوصية المعلوماتية واهميتها والتقنيات الحديثة عليها)

لذلك فإن سبل حماية الخصوصية في العالم الرقمي لذا تعد الشبكة العنكبوتية (الإنترنت) وسيلة الاتصال الأولى بالعالم في هذا العصر وبسبب انتشارها وتنوع خدماتها وانخفاض تكلفة الوصول إليها نسبيًا، أصبح العالم مجتمعًا افتراضيًا، ويمكن أفراده من التفاعل مع بعضهم ومشاركة معارفهم ومع تزايد إقبال الناس للاستفادة من إيجابيات استخدام الإنترنت، ظهر الشعور بمخاطر وتهديداتها ايضًا، وتنامى هذا الشعور مع زيادة حالات الاعتداء على البيانات الشخصية للمستخدمين واستخدامها بشكل غير قانوني.

وإن مفهوم خصوصية المعلومات يعني حق الإنسان في التحكم بوصول الآخرين واطلاعهم على معلوماته الشخصية حتى وإن كانت هذه المعلومات لدى جهات أخرى مخولة بحفظها أو حفظ بعضها (مثل الحسابات البنكية)، وتشمل البيانات الشخصية للمستخدم كل المعلومات المتعلقة بجوانب حياته الخاصة كاسمه وعمره ومكانه وسجلاته الطبية والمالية وغيرها مما يتعلق بشخصه. ومما يدخل في نطاق الخصوصية للإنسان مراعاة الشركات والمؤسسات لخصوصية معلومات موظفيها وعملائها، فهذه المؤسسات مسؤولة قانونيًا عن حماية المعلومات الشخصية التي تحفظها من المتطفلين أو غير المخولين، ويجب اقتصار استخدامها على الخدمات التي تم الاتفاق مع العميل على تقديمها له إن معرفة سبل حماية خصوصية معلوماتك أثناء استخدامك للإنترنت يقلل من احتمال تعرضها لمخاطر الاستخدام غير المشروع والذي يلحق الضرر بك معنويًا أو ماديًا. (هيئة الاتصالات وتقنية المعلومات،2023، التحول الرقمي في وزارة المالية في المملكة العربية السعودية)

المحور السادس: خصوصية المعلومات في وزارة المالية:

يوجد لدى وزارة المالية سياسة حماية خصوصية المعلومات

(Information Privacy Protection Policy)

للبوابة والأنظمة والحلول التابعة لها، متوافقة مع تشريعات حماية البيانات الشخصية للمستخدمين تخضع لقانون حماية البيانات الشخصية، والتي تهدف إلى تحديد الضوابط المتعلقة بخصوصية معلومات تحديد الهوية الشخصية والمعلومات الحساسة وحمايتها لعملاء وزارة المالية ومعلوماتهم المحفوظة. (موقع وزارة المالية بالمملكة العربية السعودية،2023، الخصوصية وسرية المعلومات بالوزارة)

ومن التشريعات ذات الصلة والمهمة لدى وزارة المالية السعودية 4 تشريعات: ومنها نظام التعاملات الإلكترونية ونظام مكافحة جرائم المعلوماتية والضوابط الأساسية للأمن السيبراني وايضاً سياسات حوكمة البيانات الوطنية.

حيث تميزت وزارة المالية في سرية معلومات مستخدميها وزوارها على رأس قائمة الأولويات، وتبذل إدارة البوابة كل جهودها لتقديم خدمة ذات جودة عالية لجميع مستخدمي البوابة للخدمات الإلكترونية، وتعتبر الخصوصية وسرية المعلومات الموضحة في بوابة الوزارة جزءاً مهماً وايضاً يعتبر من شروط استخدام البوابة الإلكترونية لوزارة المالية وأحكامها.

يجب على زوار البوابة والمستفيدين من خدماتها الاطلاع بشكل مستمر على شروط ومبادئ الخصوصية وسرية المعلومات لمعرفة أية تحديثات او تغيرات تتم عليها، وبأن إدارة البوابة غير مطالبة بالإعلان عن أية تحديثات تتم على تلك الشروط والمبادئ، ويعني استخدامك للبوابة اطلاعك وموافقتك على تلك الشروط والمبادئ وما يتم عليها من تعديلات مستمرة.

وعلماً ان وزارة المالية غير مسئولة تحت أي ظرف من الظروف عن أي أضرار مباشرة أو غير مباشرة أو عرضية أو تبعية أو خاصة أو استثنائية تنشأ عن استخدامك للخدمات أو عدم القدرة على استخدام هذه البوابة.

وعند جمع البيانات الشخصية للمستفيدين من البوابة بمجرد زيارة المستخدم للبوابة الإلكترونية لوزارة المالية يقوم الخادم الخاص بالوزارة بتسجيل عنوان بروتوكول شبكة الإنترنت الخاص بالمستخدم وتاريخ ووقت الزيارة والعنوان الموحد الخاص بأي موقع إلكتروني تتم منه إحالتك إلى بوابة وزارة المالية

إذا قمت باستخدام تطبيق مباشر أو أرسلت للوزارة بريداً إلكترونيًا عبر البوابة الإلكترونية لوزارة المالية تزويدهم في كل من ببيانات شخصية مهمة، وقد يتم مشاركة البيانات الضرورية مع جهات أو إدارات أخرى وذلك تكون الخدمة المقدمة بصورة أكثر فعالية، ولن يتم مشاركة بياناتك الشخصية مع الجهات غير الحكومية مطلقاً إلا في حال كانت من الجهات المصرح لها من الجهات المختصة بأن تقوم بأداء خدمات حكومية محددة.

وبتقديمك لبياناتك ومعلوماتك الشخصية من خلال البوابة الإلكترونية لوزارة المالية، فإنك موافق تمامًا على تخزين ومعالجة واستخدام تلك البيانات الخاصة بك من قبل السلطات السعودية، وان وزارة المالية تحتفظ بالحق في كل الأوقات في الكشف عن أي معلومات للجهات المختصة، عندما يكون ذلك ضروريا للالتزام بأي قانون أو نظام أو طلب حكومي وان المستفيد مسئول عن جميع البيانات المدخلة وصدقها وصحتها.

ويعتبر امن المعلومات الشخصية ذات سرية عالية لدى وزارة المالية لذلك اعدت البوابة الإلكترونية وثيقة الخصوصية وسرية المعلومات لمساعدة الزوار والمستفيدين والمستخدمين على تفهم طبيعة البيانات التي يتم جمعها منهم عند زيارة البوابة وكيفية التعامل معها

تقوم إدارة البوابة باتخاذ الإجراءات والتدابير وتعتبر مناسبة وملائمة للمحافظة على جميع المعلومات الشخصية لدى البوابة الإلكترونية بشكل آمن وسرية تامه وحماية كل من البيانات الشخصية المدخلة من الفقدان أو الدخول غير المصرح به أو إساءة الاستخدام، أو التعديل والإفصاح غير المصرح بهما، ومن أهم التدابير المعمول بها في الوزارة لحماية معلومات الزائر الشخصية الإجراءات والتدابير المشددة لحماية أمن المعلومات والتقنية التي نستخدمها للوقاية من عمليات الاحتيال والدخول غير المصرح به إلى أنظمة الوزارة المعمول بها و التحديث المنتظم والدوري لإجراءات وضوابط الحماية التي تفي أو تزيد عن المعايير القياسية وموظفو وزارة المالية مؤهلون ومدربون على احترام سرية المعلومات الشخصية للمستفيدين وزوار البوابة. (موقع وزارة المالية بالمملكة العربية السعودية،2023، الخصوصية وسرية المعلومات بالوزارة)

وتعتمد البوابة الإلكترونية لوزارة المالية على مجموعة من معايير الأمان التي كونها تتضمن سرية جميع المعلومات والبيانات التي يتم عرضها أو تخزينها أو تبادلها مع جهات أخرى مع الحفاظ عليها. ومن آليات الأمان المطبقة في البوابة الإلكترونية الخاصة لوزارة المالية:

أ- تعتبر شهادات الرقمية المعتمدة من أهمها، فإن تطبيق الشهادات الرقمية المعتمدة من قبل جهات ذات وثوقية عالية يزيد من الأمان لتبادل آمن لجميع المعلومات بين أنظمة البوابة الإلكترونية لوزارة المالية حيث يتم تشفير جميع البيانات المرسلة والمستقبلة من وإلى أنظمة البوابة وهذا يمنع إمكانية الحصول على البيانات التي يتم ارسالها واستقبالها وبذلك يتضمن حماية لسرية المعلومات كاملة ، وحرصت الوزارة حرصاً تاماً على المعلومات الهامة فقد تم تزويد البوابة الإلكترونية لوزارة المالية من أفضل الشركات العالمية باستخدام خوارزميات تشفير معقدة لتعمية هذه المعلومات بشكل كامل، كما ان الشركة زودت الوزارة بشهادة موثوقة ليتم وضعها ضمن البوابة كما انها تعد من الشهادات التي تحمل وتوضح درجة الأمان العالية التي تعمل بها البوابة الإلكترونية لوزارة المالية في المملكة العربية السعودية.

ب- تشفير المعلومات المخزنة لدى البوابة، كما هو معمول في تشفير المعلومات أثناء إرسال واستقبال المعلومات من قبل المستفيدين والزوار إلى البوابة، فإنه يتم تعمية وتشفير المعلومات المخزنة في جميع قواعد البيانات، على سبيل المثال كلمات المرور والمعلومات التي تحمل السرية والخصوصية العالية للأفراد، وهذا يمنع حتى من لديه حق الوصول إلى قواعد بيانات جميعها من معرفة وقراءة أو تغيير هذه المعلومات المرفقة في البوابة.

ت- حيث ان البوابة الخاصة في وزارة المالية تفرض قيود عالية على كلمات المرور، تعتمد البوابة الإلكترونية لوزارة المالية على تقنيات تضمن استخدام كلمات مرور ذات تعقيد مناسب لذلك لضمان عدم استخدام كلمات مرور ضعيفة في معلومات التسجيل، لضمان عدم استخدام كلمات المرور من قبل الأشخاص الغير مخولين بذلك كل هذه القيود تمنع الوصول إلى معلومات الآخرين بدون الإذن والصلاحيات المناسبة.

ث- كما فرضت البوابة الإلكترونية لوزارة المالية درجة عالية من الأمان على جميع تجهيزات وخوادم البوابة في مركز معلومات الوزارة، حيث تم تجهيز المركز بأحدث أجهزة الحماية إضافة إلى نشر أفضل أنواع برامج مضادات الفيروسات على جميع الخوادم التي تعمل عليها البوابة. (موقع وزارة المالية بالمملكة العربية السعودية، 2023، معايير السرية والأمان في البوابة)

المحور السابع: إدارة مخاطر خصوصية المعلومات في وزارة المالية:

الخصوصية وبيان سريّة المعلومات لذا وضعت البوابة الإلكترونية في وزارة المالية سياسة لمساعدة المستفيدين في معرفة وتفهم لطبيعة البيانات التي تقوم الوزارة بجمعها من قبلهم عند زيارة البوابة او للاستفادة من خدماتها عبر الموقع الإلكتروني.

تحافظ البوابة الإلكترونية للوزارة في كافة الأوقات على خصوصية وسرية كافة البيانات الشخصية التي يحصل عليها من قبل المستفيدين. وتفادياً للمخاطر عدم إفشاء هذه المعلومات إلا إذا كان ذلك مطلوباً بموجب أي قانون أو عندما نعتقد بحسن نية أن مثل هذا الإجراء سيكون مطلوباً أو مرغوباً فيه للتمشي مع القانون، أو للدفاع عن أو حماية حقوق الملكية الخاصة بهذا الموقع أو الجهات المستفيدة منه.

للحفاظ على الأفراد من المخاطر لذا طلبت البوابة الإلكترونية تنفيذ المعاملات المطلوبة من قبل المستفيدين لخدماتها، لذلك فرضت البوابة في حال حاجتها إلى بيانات خاصة، فإنها ستطلب منه تقديمها بمحض إرادته.

حيث انها ستساعد هذه المعلومات في الاتصال به وتنفيذ طلبات الفرد حيثما كان ذلك ممكناً. لن يتم اطلاقاً بيع البيانات المقدمة من قبلهم إلى أي طرف ثالث بغرض تسويقها لمصلحته الخاصة دون الحصول على موافقة المسبقة من قبلهم والمكتوبة ما لم يتم ذلك على أساس أنها ضمن بيانات جماعية تستخدم للأغراض الإحصائية والأبحاث دون اشتمالها على أية بيانات من الممكن استخدامها للتعريف.

يشمل الموقع الإلكتروني الخاص بالوزارة على روابط بالمواقع الأخرى على شبكة الانترنت

قد يشتمل موقعنا على روابط بالمواقع الأخرى على شبكة الإنترنت او علانات من مواقع اخرى مثل Google AdSense

ولا تعتبر البوابة مسئولة عن أساليب تجميع البيانات من قبل تلك المواقع، فيلزم المستفيدين الاطلاع على سياسات السرية والمحتويات الخاصة بتلك المواقع التي يتم الدخول إليها من خلال أي رابط ضمن هذا الموقع. وذلك لتفادي أي مخاطر ممكن ان تحصل، قد نستعين الوزارة بشركات إعلان لأطراف ثالثة لعرض الإعلانات عندما تزور موقعنا على الويب.

وكما ذكرت البوابة الإلكترونية لوزارة المالية يحق لهذه الشركات أن تستخدم معلومات حول زياراتك لهذا الموقع ولمواقع الويب الأخرى (باستثناء الاسم أو العنوان أو عنوان البريد الإلكتروني أو رقم الهاتف)، وذلك من أجل تقديم إعلانات حول البضائع والخدمات التي تهم الأفراد.(سياسة الاستخدام والخصوصية / موقع وزارة المالية)،فقد فرضة الوزارة في الدليل الاسترشادي لإدارة المخاطر الخاص بها بأنه يجب أن تتوفر لإدارة المخاطر افضل المعلومات والخبرات والموارد المتاحة، حيث ينبغي على الأفراد والجهات تصميم إطار عمل لإدارة المخاطر يدعم الرؤية الشاملة لمخاطر الأفراد والجهات ومتطلبات صنع القرار والحوكمة، وتنفيذ اجراءات إدارة المخاطر بشكل منتظم وتعاوني بالاعتماد على معرفة أراء الخبراء وأصحاب المصلحة.(الدليل الاسترشادي لوزارة المالية،2021، الدليل الاسترشادي لإدارة المخاطر والمبادئ الأساسية والممارسات التوجيهية)

3. الإطـــار العمـلي للدراسة

المحور الأول: الإطار المنهجي

أولاً: تمهيد:

يهدف هذا الفصل إلى عرض خطوات تصميم الدراسة، وذلك من حيث طبيعة الدراسة، ومجتمع وعينة الدراسة، وأداة الدراسة الميدانية، والمقاييس المستخدمة في الدراسة، وأساليب جمع البيانات، وأساليب التحليل الإحصائي، لغرض تحقيق أهداف الدراسة.

ثانياً: مجتمع وعينة الدراسة:

اعتمد الباحثون على المنهج الوصفي التحليلي لوصف وبيان إدارة المخاطر خصوصية المعلومات في وزارة المالية، ويتكون مجتمع الدراسة من الأفراد سواء المواطن او المقيم من مستخدمي الخدمات الإلكترونية لوزارة المالية في (المملكة العربية

السعودية) محل الدراسة، وقد وزع الباحثون الاستبانة الإلكترونية على عدد (384) فرد بحكم أن عدد مستخدمين البوابة الإلكترونية يتجاوز 500 ألف مستخدم حسب احصائيات البوابة لسنة 2022م

ثالثاً: أداة الدراسة الميدانية:

اعتمدت الدراسة على وسيلة الاستبانة الإلكترونية كأداة رئيسية للحصول على البيانات والمعلومات اللازمة لموضوع الدراسة وتحقيقاً للغرض السابق للاستبانة قام الباحثون بتصميم استمارة استبيان تهدف إلى قياس رأى أفراد العينة حول إدارة المخاطر خصوصية المعلومات للبوابة الإلكترونية بوزارة المالية حيث تم التصميم على النحو التالي:

القسم الأول: البيانات الشخصية:

هذا القسم اشتمل على البيانات والمعلومات العامة (المتغيرات الديموغرافية) لأفراد عينة الدراسة، حيث تضمن خمسة متغيرات هي (الجنس، العمر، الحالة الاجتماعية، المستوى التعليمي، المهنة).

القسم الثاني: متغيرات الدراسة:

يتضمن هذا القسم المعلومات الفنية لجوانب الدراسة، وينقسم إلى مجالين:

المجال الأول: حماية خصوصية المعلومات:

ويتضمن هذا المجال (5) فقرات تقيس مستوى تطبيق "حماية خصوصية المعلومات" للبوابة الإلكترونية لوزارة المالية خاصة الخدمات المقدمة للفرد

المجال الثاني: مخاطر خصوصية المعلومات:

ويتضمن هذا المجال (5) فقرات تقيس مستوى "إدارة مخاطر خصوصية المعلومات" للبوابة الإلكترونية لوزارة المالية خاصة الخدمات المقدمة للفرد

رابعاً: صدق وثبات أداة الدراسة:

صدق أداة الدراسة:

الاداة التي استخدمت في جمع البيانات الأولية من عينة الدراسة قام الباحثون بالاقتباس والاسترشاد والاستشهاد باستبيانات لدراسات سابقة تناولت ذات المشكلة محل الدراسة ولكن بجوانب أخرى، حيث ان الأبحاث المسترشد دراسة **"محمد العتيبي 2020م"** وعنوانها: **"تقييم مخاطر خصوصية البيانات في وزارة العدل في المملكة العربية السعودية"** ودراسة **"منى تركي وجان سيريل 2013م"** وعنوانها: **"الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها"**

ثبات أداة الدراسة:

أجرى الباحثون اختبار الثبات بعد جمع البيانات باستخدام معامل (Cronbach's Alpha) للاتساق الداخلي، حيث بلغت قيمة ألفا كرو نباخ لجميع متغيرات الدراسة (0.856) وهو معامل مناسب يجعل من الاستبانة أداة مناسبة للبيانات التي تم جمعها بواسطتها، وكما هو موضح في الجدول (1).

جدول رقم (1) معامل ثبات اداة الدراسة

المحاور	عدد الفقرات	معاملAlpha Cronbach's
المجال الأول: حماية خصوصية المعلومات	**4**	**0.687**
المجال الثاني: إدارة مخاطر خصوصية المعلومات	**5**	**0.813**
جميع الفقرات	**9**	**0.856**

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

من خلال الجدول أعلاه نجد أن المجال الأول حماية خصوصية المعلومات حصل على نسبة معامل ثبات (0.687)، بينما حصل المجال الثاني إدارة مخاطر خصوصية المعلومات على نسبة معامل ثبات (0.813)، وحصل المحور الكلي لجميع الفقرات على نسبة ثبات (0.856)، وجميع هذه النسب تجعل من الاستبيان أداة موثوق الاعتماد عليها لأغراض البحث العلمي.

خامساً: مقاييس وأساليب التحليل الإحصائي:

مقياس الاستبانة:

تم استخدام مقياس ليكرت الخماسي في الاستبانة للتعبير عن آراء أفراد العينة حول فقرات المحاور والمجالات وقد تم ترميز هذا المقياس كما يلي:

جدول رقم (2): يوضح مقياس ليكرت الخماسي

مستوى الموافقة	موافق بشدة	موافق	موافق إلى حد ما	غير موافق	غير موافق بشدة
درجة الموافقة	5	4	3	2	1

المصدر: محمودي، محمد بشير، قدة، & حمزة. (2021)

ولغرض تحليل البيانات المجمعة ميدانياً، تم استخدام برنامج التحليل الإحصائي (SPSS) وتم ترميزها وفقاً لمقياس (ليكرت الخماسي)، واستخدم الرقم (3) كمتوسط فرضي للدراسة ويحتسب من الصيغة:

$$M= [1+2+3+4+5]/5=15/5=3$$

كما تم إيجاد المدى للمقياس وهو الفرق بين أكبر قيمة وأصغر قيمة في المقياس، أي أن المدى (5-1 = 4)، كما تم إيجاد طول الخلية وهو عبارة عن قسمة المدى على عدد فقرات المقياس ويساوي (0.80) أي أن طول الخلية = 5/4=0.80) ولمعرفة الحدود الحقيقية للمقياس تم إضافة طول الخلية إلى أدنى درجة في المقياس كما هو موضح في الجدول الآتي:

جدول رقم (3): يوضح الميزان التقديري وفقا لمقياس ليكرت الخماسي

الاستجابة	المتوسط المرجح الموزون	طول الفترة	مستوى التوافر
غير موافق بشدة	من 1 إلى 1.79	0.80	منخفض جدا

غير موافق	من 1.80 إلى 2.59	0.80	منخفض
محايد	من 2.60 إلى 3.39	0.80	متوسط
موافق	من 3.40 إلى 4.19	0.80	عال
موافق بشدة	من 4.20 إلى 5.00	0.80	عال جدا

المصدر: إعداد الباحثين

من الجدول أعلاه يتضح الآتي:

إذا وقع الوسط الحسابي المحتسب من البيانات في المدى(1-1.79) فهذا يشير إلى عدم توافر الفقرة تماماً – منخفض جدا للفقرة (غير موافق بشدة).

إذا وقع الوسط الحسابي المحتسب من البيانات في المدى (1.80-2.59) فهذا يشير إلى توافر منخفض للفقرة (غير موافق).

إذا وقع الوسط الحسابي المحتسب من البيانات في المدى (2.60-3.39) فهذا يشير إلى توافر متوسط للفقرة (محايد).

إذا وقع الوسط الحسابي المحتسب من البيانات في المدى (3.40-4.19) فهذا يشير إلى توافر عال للفقرة (موافق).

إذا وقع الوسط الحسابي المحتسب من البيانات في المدى (4.20-5) فهذا يشير إلى توافر عال جداً للفقرة (موافق بشدة).

سادساً: أساليب التحليل الإحصائي

لغرض الإجابة عن أسئلة الدراسة واختبار فرضياتها تم الاعتماد على الحزمة الإحصائية للعلوم الاجتماعية (SPSS) في التحليل وكذلك تم استخدام مجموعة من الأساليب الإحصائية منها ما يلي:

مقياس الاحصاء الوصفي (Measures (Descriptive Statisticsوذلك لوصف خصائص عينة الدراسة، اعتماداً على النسب المئوية والتكرارات.

للإجابة على أسئلة الدراسة وترتيب أبعاد الدراسة حسب أهميتها النسبية تم الاعتماد على المتوسطات الحسابية والانحرافات المعيارية.

اختبار الفا كرو نباخ (Alpha cronbach) لقياس ثبات أداة الدراسة.

المحور الثاني: عرض وتحليل البيانات واختبار فرضيات الدراسة

اولاً: خصائص عينة الدراسة:

يعرض هذا الجزء التحليل الوصفي للمتغيرات الديموغرافية والوظيفية لعينة الدراسة المتمثلة بـ (الجنس، العمر، المؤهل التعليمي، المهنة، المستوى الوظيفي)، وذلك كما يلي:

الجنس:

تم سؤال المبحوثين عن الجنس وأعطوا إجابات عن ذلك مبينة في الجدول رقم (4)

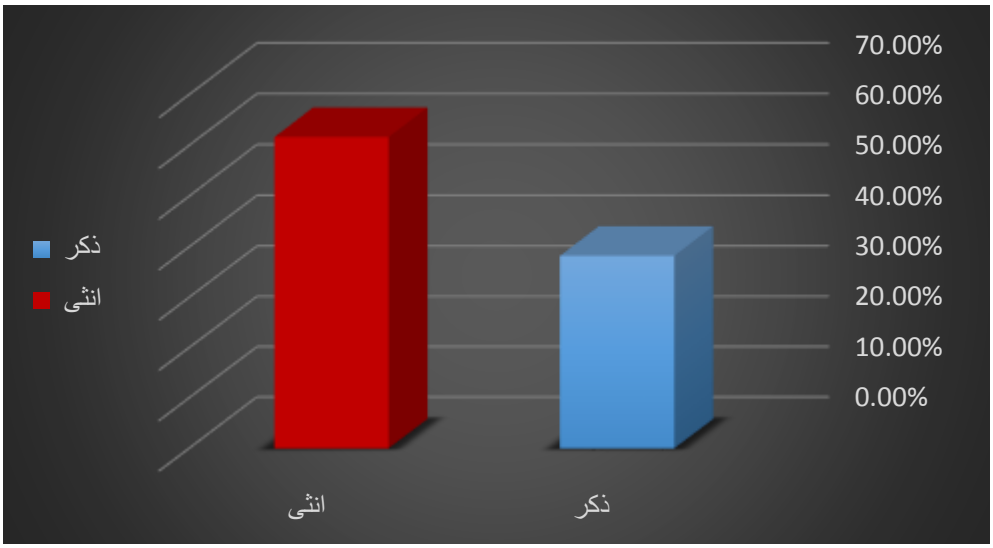
جدول رقم (4): يوضح توزيع أفراد عينة الدراسة حسب الجنس

الجنس	العدد	النسبة المئوية %
ذكر	147	38.3%
أنثى	237	61.7%
الإجمالي	384	100 %

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

من خلال الجدول رقم (4) يلاحظ أن نسبة (61.7%) من إجمالي أفراد عينة الدراسة جنسهم انثى وهي أعلى فئة من فئات النوع المدروسة، ونسبة (38.3%) من إجمالي أفراد عينة الدراسة نوعهم (ذكر).

الشكل رقم (1): يوضح توزيع أفراد عينة الدراسة حسب النوع الجنس



المصدر: إعداد الباحثين

العمر:

تم سؤال المبحوثين عن أعمارهم وأعطوا إجابات عن ذلك مبينة في الجدول رقم (5)

جدول رقم: (5) يوضح توزيع أفراد عينة الدراسة حسب العمر

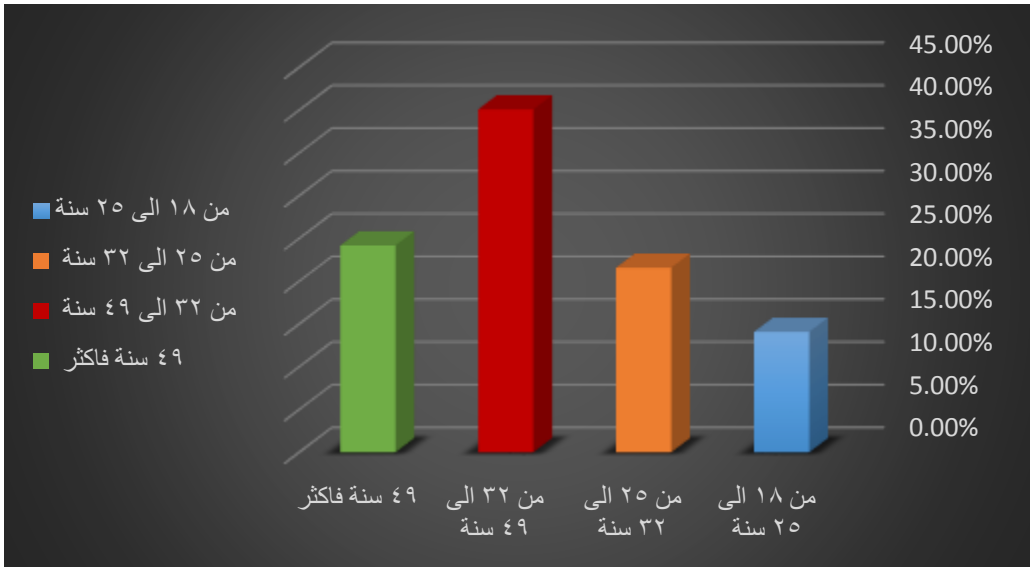
العمر	العدد	النسبة المئوية %
من 18 إلى 25 سنة	54	14.1%
من 25 إلى 32 سنة	83	21.6%
من 32 إلى 49سنة	154	40.1%
49 سنة فأكثر	93	24.2%
الإجمالي	384	100

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

ISSN: 2706-6495

من خلال الجدول رقم (5) يلاحظ أن نسبة (40.1%) من إجمالي أفراد عينة الدراسة اعمارهم بين (من 32 إلى 49 سنة) وهي أعلى فئة من الفئات العمرية المدروسة، ونسبة (24.2%) من إجمالي أفراد عينة الدراسة فئتهم العمرية (49سنة فأكثر)، اما نسبة (21.6%) من إجمالي أفراد عينة الدراسة أعمارهم (من 25 إلى 32 سنة). وكذلك نسبة (14.1%) من إجمالي أفراد عينة الدراسة اعمارهم (من 18 إلى 25 سنة)

الشكل رقم: (2) يوضح توزيع أفراد عينة الدراسة حسب العمر



المصدر: إعداد الباحثين

المستوى التعليمي:

تم سؤال المبحوثين عن مستوياتهم التعليمية وأعطوا إجابات عن ذلك مبينة في الجدول رقم (6)

جدول رقم (6): يوضح توزيع أفراد عينة الدراسة حسب المستوى التعليمي

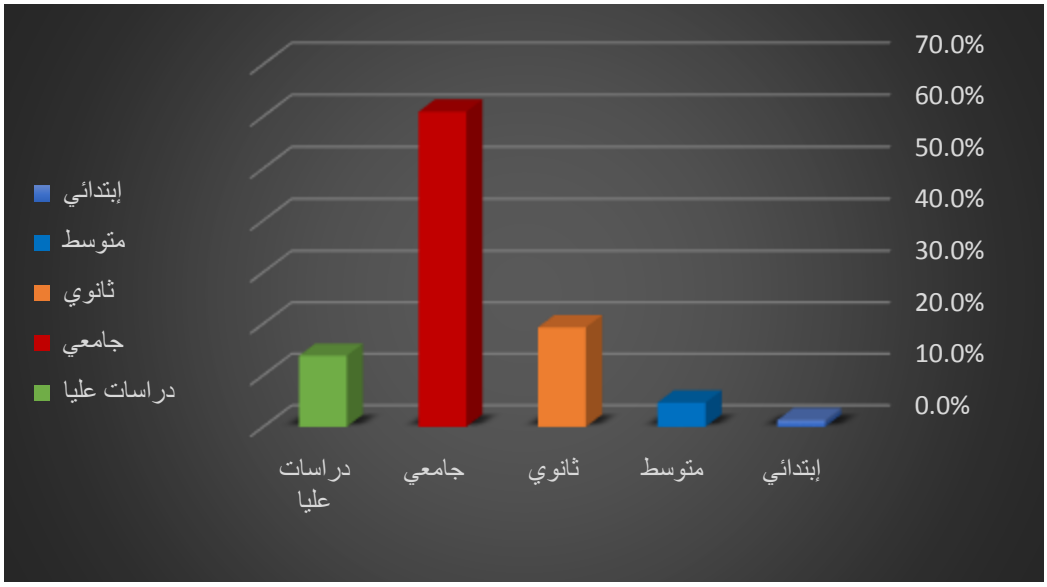
المستوى التعليمي	العدد	النسبة المئوية %
ابتدائي	5	1.3%
متوسط	18	4.7%
ثانوي	74	19.3%
جامعي	234	60.9%
دراسات عليا	53	13.8%
الإجمالي	384	100 %

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

ISSN: 2706-6495

من خلال الجدول رقم (6) يلاحظ أن نسبة (60.9%) من إجمالي أفراد عينة الدراسة يحملون مؤهل (جامعي) وهي أعلى فئة من الفئات التعليمية المدروسة، ونسبة (19.3%) من إجمالي أفراد عينة الدراسة مؤهلهم العلمي (ثانوي)، ونسبة (13.8%) من إجمالي أفراد عينة الدراسة مؤهلهم العلمي (دراسات عليا). ونسبة (4.7%) من إجمالي أفراد عينة الدراسة مؤهلهم العلمي (متوسط). ونسبة (1.3%) من إجمالي أفراد عينة الدراسة مؤهلهم العلمي (ابتدائي).

الشكل رقم(3): يوضح توزيع أفراد عينة الدراسة حسب المستوى التعليمي



المصدر: إعداد الباحثين

المهنة:

تم سؤال المبحوثين عن المهنة وأعطوا إجابات عن ذلك مبينة في الجدول رقم (7).

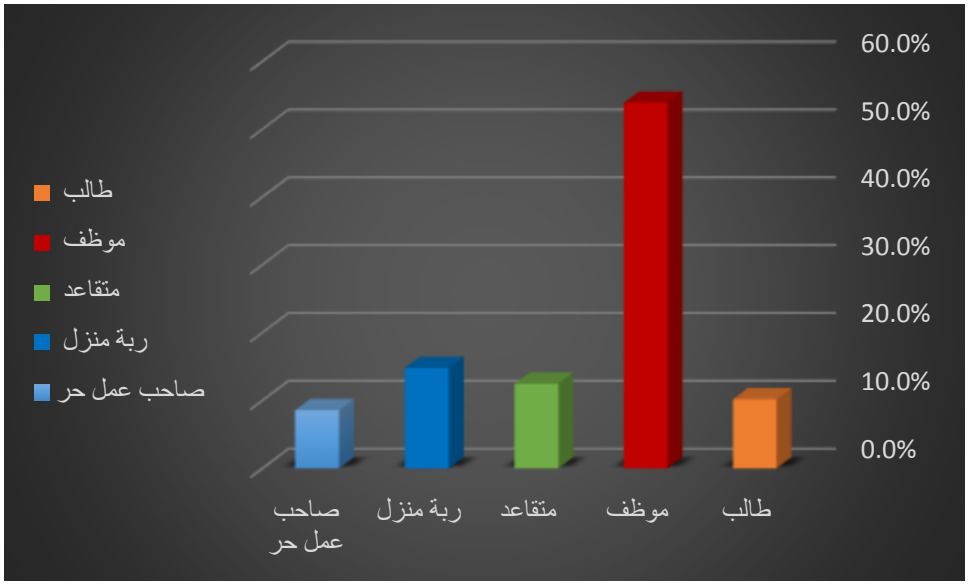
جدول رقم (7): يوضح توزيع أفراد عينة الدراسة حسب المهنة

المهنة	العدد	النسبة المئوية %
طالب	39	10.2%
موظف	207	53.9%
متقاعد	48	12.5%
ربة منزل	57	14.8%
صاحب عمل حر	33	8.6%
الإجمالي	384	100%

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

من خلال الجدول رقم (7) يلاحظ أن نسبة (53.9%) من إجمالي أفراد عينة الدراسة حسب المهنة (موظف) وهي أعلى فئة من الخبرات المهنية المدروسة، ونسبة (14.8 %) من اجمالي أفراد عينة الدراسة لديهم المهنة (ربة منزل)، بينما نسبة (12.5%) من اجمالي أفراد عينة الدراسة لديهم المهنة (متقاعد)، بينما نسبة (10.2%) من اجمالي أفراد عينة الدراسة لديهم المهنة (طالب)، ونسبة(8.6 %) من اجمالي أفراد عينة الدراسة لديهم المهنة (صاحب عمل حر).

الشكل رقم (4): يوضح توزيع أفراد عينة الدراسة حسب المهنة



المصدر: إعداد الباحثين

الحالة الاجتماعية:

تم سؤال المبحوثين عن الحالة الاجتماعية وأعطوا إجابات عن ذلك مبينة في الجدول رقم (8)

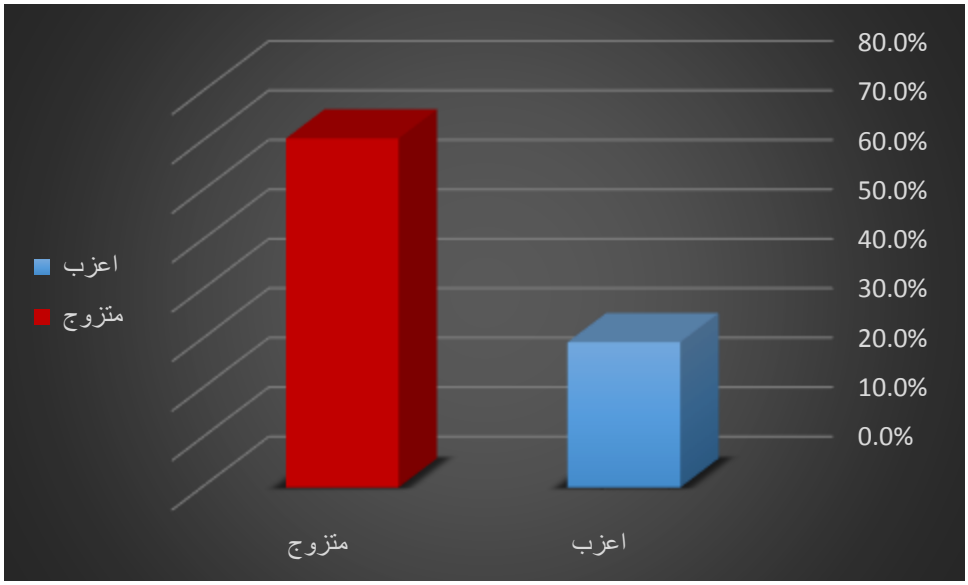
جدول رقم (8) يوضح توزيع فراد عينة الدراسة حسب الحالة الاجتماعية

الحالة الاجتماعية	العدد	النسبة المئوية %
أعزب	113	29.4%
متزوج	271	70.6%
الإجمالي	384	100 %

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS.

من خلال الجدول رقم (8) يلاحظ أن نسبة (70.6%) من إجمالي أفراد عينة الدراسة حسب الحالة الاجتماعية متزوج وهي أعلى فئة من فئات النوع المدروسة، ونسبة (29.4%) من إجمالي أفراد عينة الدراسة نوعهم (أعزب).

الشكل رقم (5) يوضح توزيع أفراد عينة الدراسة حسب النوع الحالة الاجتماعية



المصدر: إعداد الباحثين

المبحث الثالث: الدراسة الوصفية والتحليلية لإجابات أفراد عينة الدراسة

يتضمن هذا الجزء النتائج التي تم التوصل إليها من تحليل البيانات الخاصة بإجابات أفراد عينة الدراسة محل الدراسة لقيم المتغيرات في الدراسة، حيث تم قياس وتحليل معنوية الاتجاه العام لإجابات أفراد عينة الدراسة نحو قيم هذه المتغيرات.

وقد تم قياس معنوية الاتجاه العام لإجابات أفراد عينة الدراسة من خلال استخراج المتوسطات الحسابية لهذه الإجابات ومقارنتها بالمتوسط الفرضي الذي يمثل نقطة المنتصف على مقياس ليكرت المتدرج ذو الخمس نقاط، ثم تحديد مستوى الدلالة باستخدام أسلوب (T Test)، كما تم استخراج الانحراف المعياري للمجالات والمتغيرات لمعرفة مدى تركز وتشتت اراء أفراد العينة وذلك على النحو التالي:

التحليل الوصفي لإجابات أفراد العينة عن حماية خصوصية المعلومات وإدارة مخاطر خصوصية المعلومات:

تم استخراج التحليل الوصفي لأبعاد حماية خصوصية المعلومات وإدارة مخاطر خصوصية المعلومات: كلا على حدة كما يلي:

المجال الاول: التحليل الوصفي لإجابات أفراد العينة حول حماية خصوصية المعلومات

حيث كان تقسيم مكوناته كالتالي:

اولاً: التحليل الوصفي لإجابات أفراد العينة لمجال حماية خصوصية المعلومات:

كانت النتائج التي تم التوصل اليها كما يوضحها الجدول رقم (9) لمجال حماية خصوصية المعلومات، ومتوسط درجات التوافر لكل منها، ومعنوية الاتجاه العام لإجابات أفراد عينة الدراسة نحو هذا التوافر والانحرافات المعيارية لتلك الفقرات، حيث يلاحظ من بيانات الجدول رقم (9) ما يلي:

بلغ المتوسط الحسابي العام لإجابات أفراد عينة الدراسة عن مستوى مجال حماية خصوصية المعلومات (4.175)، وهذا يعنى أن درجة إدراك أفراد عينة الدراسة حول المجال خصوصية المعلومات تقع عند المستوى "متوافر بدرجة عالية" حيث تنتمي قيمة الوسط الحسابي العام إلى فئة المقياس (4.20-5.00) والذي يشير إلى توافر عالي جدا لبعد المتطلبات لمجال حماية خصوصية المعلومات للعينة محل الدراسة، كما تشير قيمة الانحراف المعياري العام إلى تقارب الآراء وتجانسها حول بعد المتطلبات لمجال حماية خصوصية المعلومات حيث بلغت قيمته (0.964).

جدول رقم (9): التحليل الوصفي ونتائج قياس معنوية الاتجاه العام لإجابات أفراد عينة الدراسة حول بعد حماية خصوصية المعلومات.

م	الفقرات	المتوسط	الانحراف المعياري	الترتيب	مستوى التوافر
1	ما مدى اعتقادك ان سياسة حماية الخصوصية المعلوماتية يتم مراعاتها وتطبيقها في الموقع الإلكتروني في وزارة المالية في المملكة العربية السعودية	4.25	.958	1	عال جدا
2	ما مدى اعتقادك ان الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية تفي بسياسات حماية خصوصية المعلومات التي تزودهم بها	4.17	0.934	2	عال
3	إلى اي مدى تشارك معلوماتك الصحيحة عند استخدامك الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية	4.15	1.01	3	عال
4	ما مدى تطبيق سياسة حماية خصوصية المعلومات بالمواقع الإلكترونية للمؤسسات الحكومية بالسعودية من وجهة نظرك	4.13	0.957	4	عال
	المتوسط الحسابي العام	4.175	0.964		عال

المصدر: إعداد الباحثين بالاعتماد على برنامج SPSS

من خلال الجدول رقم (9) يتضح ان تحليل الفقرات قد اوضح النتائج الاتية، حيث تم ترتيب فقرات المحور تنازليا وفقا لترتيبها بالنسبة للوسط الحسابي:

الفقرة رقم (1) بالجدول، حصلت هذه الفقرة على المرتبة الأولى في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.25)، كما بلغ الانحراف المعياري (958.) مما يشير إلى تركيز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان هناك اعتقاد جازم بان سياسة حماية الخصوصية المعلوماتية يتم مراعاتها وتطبيقها في الموقع الإلكتروني لوزارة المالية في المملكة العربية السعودية.

الفقرة رقم (2) بالجدول، حصلت هذه الفقرة على المرتبة الثانية في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.17)، كما بلغ الانحراف المعياري (934.) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان هناك اعتقاد عالي بان الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية تفي بسياسات حماية خصوصية المعلومات التي تزودهم بها.

الفقرة رقم (3) بالجدول، حصلت هذه الفقرة على المرتبة الثالثة في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.15)، كما بلغ الانحراف المعياري (1.01) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان هناك مشاركة للمعلومات الصحيحة عند استخدام الفرد الخدمات الإلكترونية لوزارة المالية في المملكة العربية السعودية.

الفقرة رقم (4) بالجدول، حصلت هذه الفقرة على المرتبة الرابعة في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.13)، كما بلغ الانحراف المعياري.(957) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان هناك تطبيق لسياسة حماية خصوصية المعلومات بالمواقع الإلكترونية للمؤسسات الحكومية بالسعودية من وجهة نظر المبحوثين.

المجال الثاني: التحليل الوصفي لإجابات أفراد العينة المجال إدارة مخاطر خصوصية المعلومات

ويتضمن هذا المجال (5) فقرات تقيس مستوى إدارة مخاطر خصوصية المعلومات كالتالي:

كانت النتائج التي تم التوصل اليها كما يوضحها الجدول رقم (10) لبعد إدارة مخاطر خصوصية المعلومات، ومتوسط درجات التوافر لكل منها، ومعنوية الاتجاه العام لإجابات أفراد عينة الدراسة نحو هذا التوافر والانحرافات المعيارية لتلك الفقرات، حيث يلاحظ من بيانات الجدول رقم (10) ما يلي:

بلغ المتوسط الحسابي العام لإجابات أفراد عينة الدراسة عن مستوى إدارة مخاطر خصوصية المعلومات (4.07)، وهذا يعنى أن درجة إدراك أفراد عينة الدراسة عن إدارة مخاطر خصوصية المعلومات، تقع عند المستوى "متوافر بدرجة عالية جدا" حيث تنتمي قيمة الوسط الحسابي العام إلى فئة المقياس (4.20-5.00) والذي يشير إلى توافر عالي جدا لمستوى إدارة مخاطر خصوصية المعلومات، للعينة محل الدراسة، كما تشير قيمة الانحراف المعياري العام إلى تقارب الآراء وتجانسها حول مستوى إدارة مخاطر خصوصية المعلومات، حيث بلغت قيمته (0.991).

جدول (10): التحليل الوصفي ونتائج قياس معنوية الاتجاه العام لإجابات أفراد عينة الدراسة حول إدارة مخاطر خصوصية المعلومات.

	الفقرات	المتوسط	الانحراف المعياري	الترتيب	مستوى التوافر
1	هل من الممكن ان الجهات الرقابية تسعى لتقييم المخاطر المحتملة لخصوصية معلوماتك عند استخدام الخدمات الإلكترونية لوزارة المالية	4.12	.94	1	عال
2	ما مدى اعتقادك بأن لا يتم الكشف عن المعلومات الشخصية التي تم جمعها او استخدامها لخدمات الإلكترونية لوزارة المالية لأي شخص	4.10	1.046	2	عال

3	موظفي وزارة المالية متدربين على متطلبات حماية المعلومات الشخصية وعلى دراية بالسياسات ذات الصلة بالخدمات الإلكترونية	4.09	0.962	3	عال
4	عند مشاركتك بمعلوماتك الشخصية عند استخدام الخدمات الإلكترونية لوزارة المالية يتم النظر في الأدوات التكنولوجية	4.02	0.988	4	عال
5	إذا تم تحديد المخاطر المحتملة لخصوصية المعلومات هل تعتقد ان الجهات الرقابية تتجنبها او تخفف منها	4.02	1.023	4	عال
المتوسط الحسابي العام		4.07	0.991	عال	

المصدر: إعداد الباحث بالاعتماد على برنامج SPSS

* مستوى الدلالة عند 0.05 (P=0.05)

من خلال الجدول رقم (10) يتضح أن تحليل الفقرات قد اوضح النتائج الاتية، حيث تم ترتيب فقرات المحور تنازليا وفقا لترتيبها بالنسبة للوسط الحسابي:

الفقرة رقم (1) بالجدول، حصلت هذه الفقرة على المرتبة الأولى في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.12)، كما بلغ الانحراف المعياري (.94) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان من الممكن من الجهات الرقابية ان تسعى لتقييم المخاطر المحتملة لخصوصية معلوماتك عند استخدام الخدمات الإلكترونية لوزارة المالية.

الفقرة رقم (2) بالجدول، حصلت هذه الفقرة على المرتبة الثانية في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.10)، كما بلغ الانحراف المعياري (1.046) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان هناك اعتقادك بأن لا يتم الكشف عن المعلومات الشخصية التي تم جمعها او استخدامها لخدمات الإلكترونية لوزارة المالية لأي شخص.

الفقرة رقم (3) بالجدول، حصلت هذه الفقرة على المرتبة الثالثة في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة، إذ بلغ متوسط إجابات المبحوثين (4.09)، كما بلغ الانحراف المعياري (0.962) مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة، ويشير ذلك إلى ان موظفي وزارة المالية متدربين يقومون بالمحافظة على متطلبات حماية المعلومات الشخصية وعلى دراية بالسياسات ذات الصلة بالخدمات الإلكترونية.

الفقرة رقم (4،5) بالجدول، حصلت هذه الفقرات على المرتبة الرابعة في التركيز والموافقة من قبل عينة الدراسة، حيث تشير نتائج إجابات المبحوثين إلى قناعتهم بمضمون الفقرة ، إذ بلغ متوسط إجابات المبحوثين (4.02) ، كما بلغ الانحراف المعياري (,988,1.023) على التوالي، مما يشير إلى تركز آراء عينة الدراسة حول هذه الفقرة ويشير ذلك إلى عند مشاركتك بمعلوماتك الشخصية عند استخدام الخدمات الإلكترونية لوزارة المالية يتم النظر في الأدوات التكنولوجية، وأيضا، يتم تحديد المخاطر المحتملة لخصوصية المعلومات وتعمل الجهات الرقابية على تتجنبها و تخفف منها.

التحليل الوصفي لأبعاد حماية خصوصية المعلومات وإدارة المخاطر خصوصية المعلومات

كانت النتائج التي تم التوصل إليها عن ابعاد حماية خصوصية المعلومات وإدارة المخاطر خصوصية المعلومات موضحة في الجدول(11) والذي يبين ابعاد حماية خصوصية المعلومات على إدارة المخاطر خصوصية المعلومات، ومتوسط درجات التوافر لكل منها، ومعنوية الاتجاه العام لإجابات أفراد عينة الدراسة والانحرافات المعيارية لتلك الابعاد، حيث يلاحظ من بيانات الجدول رقم(11) ما يلي:

بلغ المتوسط الحسابي العام لإجابات أفراد عينة الدراسة عن توافر استخدام حماية خصوصية المعلومات على إدارة مخاطر خصوصية المعلومات (4.175، 4.07) على التوالي، وهذا يعنى أن درجة إدراك أفراد عينة الدراسة عن توافر ابعاد حماية خصوصية المعلومات و إدارة المخاطر لخصوصية المعلومات, مجتمعة معاً تقع عند المستوى "متوافر بدرجة عالية " حيث تنتمي قيمة الوسط الحسابي العام إلى فئة المقياس(4.20-5.00) والذي يشير إلى توافر عال جدا لـ حماية الخصوصية المعلوماتية و إدارة خطر خصوصية المعلومات، كما تشير قيمة الانحراف المعياري العام إلى تقارب الآراء وتجانسها حول أثر حماية خصوصية المعلومات و إدارة المخاطر لخصوصية المعلومات حيث بلغت قيمته (964.،991.) على التوالي.

جدول رقم (11) التحليل الوصفي ونتائج قياس معنوية الاتجاه العام لإجابات أفراد عينة الدراسة حول حماية خصوصية المعلومات وإدارة المخاطر خصوصية المعلومات

المحاور	المتوسط الحسابي	الانحراف المعياري	الترتيب
المتغير المستقل			
(1) المحور الكلي: إدارة المخاطر خصوصية المعلومات	4.07	0.991	عال
المتغير التابع			
(2) المحور الكلي: حماية خصوصية المعلومات	4.175	0.964	عال
جميع الفقرات	4.12	0.977	

المصدر: التحليل الإحصائي لبيانات الدراسة الميدانية

المبحث الرابع: اختبار الفرضيات:

قام الباحثون بإجراء الاختبارات الاحصائية الخاصة بمعرفة مدى صحة الفرضيات التي تم وضعها للبحث لمعرفة أثر إدارة مخاطر خصوصية المعلومات على حماية خصوصية المعلومات حيث استخدم الباحثون المتوسط الحسابي والانحراف المعياري اضافة إلى اختبار معامل الارتباط والانحدار المتعدد لمعرفة نوع وقوة العلاقة عند مستوى دلالة (0.05) والتالي عرض لنتائج اختبار الفرضيات كالاتي:

الفرضية الرئيسية :(يوجد أثر ذو دلالة إحصائية بين إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات)، ويتفرع منها:

يوجد أثر ذو دلالة إحصائية ان الفرد يواجه مخاطر عند استخدامه للبوابة الإلكترونية لوزارة المالية بالمملكة العربية السعودية.

يوجد أثر ذو دلالة إحصائية ان الفرد يواجه خطر انتهاك خصوصية المعلومات بشكل أكبر جراء استخدامه للخدمة الإلكترونية

من الوزارة المالية بالسعودية.

يوجد أثر ذو دلالة إحصائية ان ممارسات وضوابط إدارة المخاطر التي تتبعها وزارة المالية قادرة على تذليل خطر خصوصية المعلومات.

لإتمام هدف الدراسة في معرفة مدى وجود علاقة ارتباط بين المتغيرات فقد تم اختبار العلاقات بين الفقرات ومحاورها باستخدام البيانات المستخرجة من اختبار معامل ارتباط بيرسون والانحدار الخطي المتعدد وكما هو مبين في الجدول رقم(11) وذلك لاختبار الفرضية التي تنص على (يوجد أثر ذو دلالة إحصائية بين إدارة مخاطر خصوصية المعلومات وحماية خصوصية المعلومات).

ولغرض التحقق من نوع وطبيعة العلاقة بين ابعاد إدارة مخاطر خصوصية المعلومات بوصفها متغير مستقل وبين حماية خصوصية المعلومات بوصفه متغيرا تابعاً، تم تطبيق أسلوب معامل الارتباط والانحدار المتعدد وذلك لمعرفة نوع وقوة العلاقة بين إدارة مخاطر خصوصية المعلومات وحماية خصوصية المعلومات وذلك على النحو التالي:

جدول رقم (12) يوضح قيم معامل الارتباط بين عناصر إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات

			المتغيرات المستقلة			
المتغير التابع	Q1	Q2	Q3	Q4	Q5	**بصورة الكلية**
	0.594	0.219	0.126	0.589	0.615	0.660
مستوى الدلالة sig	0.00	0.00	0.007	0.00	0.00	0.000

المصدر: إعداد الباحثين بواسطة SPSS

** ذات دلالة احصائية عند مستوى (0.01) * ذات دلالة احصائية عند مستوى (0.05)

اذ تشير نتائج الجدول المعروض بجدول رقم (11) إلى وجود علاقات ارتباط بين إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات، حيث بلغت قيمة هذه العلاقة (0.660) وهي قيمة ارتباط مرتفعة بين المحورين وتؤكد قبول الفرضية التي تنص على وجود علاقة ارتباط بين إدارة المخاطر خصوصية المعلومات وحماية الخصوصية المعلوماتية

حيث يأتي أقوى الارتباطات بين إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات بالسؤال (Q5) "ما مدى تطبيق سياسة حماية خصوصية المعلومات بالمواقع الإلكترونية للمؤسسات الحكومية بالسعودية من وجهة نظرك" بمعامل (0.615) يليها الارتباط بالسؤال Q1 يليها الارتباط بالسؤال Q4 ويأتي بعدها الارتباط بالسؤال Q2

ولاختبار الفرض القائم على العلاقة بين أثر إدارة المخاطر خصوصية المعلومات بمتغيراته المختلفة على حماية خصوصية المعلومات قام الباحثون باستخدام تحليل الانحدار الخطي المتعدد لمعرفة نوع وقوة العلاقة بين أثر عناصر إدارة المخاطر خصوصية المعلومات في تحقيق حماية خصوصية المعلومات وذلك على النحو التالي: وفق النموذج $y=a+bx$ حيث إن:

y المتغير التابع وهو حماية خصوصية المعلومات

x المتغير المستقل وهو إدارة المخاطر خصوصية المعلومات

a وهو عبارة عن ثابت الانحدار

b وهو عبارة عن مقدار التأثير في المتغير التابع نتيجة تغير المتغير المستقل، و كانت أهم النتائج اللازمة لاختبار هذه الفرضية موضحة في الجدول رقم (13):

جدول رقم (13) أهم نتائج الانحدار الخطي المتعدد لمعرفة دور إدارة المخاطر خصوصية المعلومات في تحقيق حماية

نموذج الانحدار الخطي المتعدد	معامل الارتباط R	معامل التحديد R^2	درجة الحرية	قيمة (f)	مستوى الدلالةsig
النموذج الكلي	0.66	0.436	1/384	295.1	0.00

المتغير التابع	المتغير المستقل
	ثابت الانحدار
قيمة المعامل	0.970
قيمة T	5.30
المعنوية	0.000
	0.775
	17.17
	0.000

المصدر: اعداد الباحث من بيانات الدراسة الميدانية.

خصوصية المعلومات

من خلال الجدول رقم (13) نجد ان مستوى المعنوية للمحور المستقل إدارة مخاطر خصوصية المعلومات بصورة الكلية كانت كالتالي:

للمتغير المستقل إدارة المخاطر خصوصية المعلومات كان ذو تأثير معنوي في نموذج الانحدار عند مستوى معنوية (0.005).

ويتضح من النتائج الإحصائية لقيمة النموذج الكلي وجود علاقة تأثير ذات دلالة معنوية للمتغير المستقل المتمثل إدارة مخاطر خصوصية المعلومات في المتغير التابع و المتمثل في حماية خصوصية المعلومات، حيث بلغت قيمة معامل الانحدار (0.970) اي انه كلما زاد إدارة مخاطر خصوصية المعلومات بمقدار وحدة قياس واحدة تؤدي إلى زيادة التأثير في حماية خصوصية المعلومات بمقدار0.970 من الوحدة، في حين بلغت قيمة معامل الارتباط (0.66) وهو معامل ارتباط طردي معنوي قوي اي انه كلما زاد إدارة مخاطر خصوصية المعلومات تؤدي إلى زيادة في حماية خصوصية المعلومات والعكس صحيح، اما القابلية التفسيرية لنموذج الانحدار اعلاه في الجدول (13) والمتمثلة في معامل التحديد فقد بلغت قيمته 0.436مما يشير إلى إن 43% من التغيرات في إدارة مخاطر خصوصية المعلومات تعود إلى خصوصية المعلومات وحدها (مع ثبات بقية العوامل الاخرى) بينما نسبة 57% من التغيرات في إدارة مخاطر خصوصية المعلومات تعود إلى عوامل اخرى، وبلغت مستوى دلالة sig (0.00) وهي اقل من مستوى الدلالة المعتمد في هذه الدراسة وهي 0.05 وبهذه النتائج نتوصل إلى ان إدارة مخاطر خصوصية المعلومات له تأثير قوي وذو دلالة معنوية على حماية خصوصية المعلومات وبالتالي نقبل الفرض الذي ينص على **(يوجد أثر ذو دلالة إحصائية بين إدارة مخاطر خصوصية المعلومات و حماية خصوصية المعلومات)**.

4. النتائج والتوصيات

المحور الأول: النتائج

من خلال تحليل النتائج وتفسيرها في ضوء فرضيات المتغيرات إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات توصلنا إلى ما يلي:

1- ممارسات وضوابط إدارة المخاطر المطبقة في البوابة الإلكترونية لوزارة المالية بالسعودية ذات فائدة لحماية خصوصية المعلومات للمستخدم الفرد.
2- يوجد وعي وتثقيف لدى المستخدم الفرد عند مشاركة معلوماته الشخصية في المواقع الإلكترونية
3- الجهات الرقابية الرسمية في السعودية مثل هيئة الحكومة الرقمية ووزارة الاتصالات وتقنية المعلومات تعمل بشكل دؤوب لحماية المعلومات في المواقع الإلكترونية لكيانات الدولة.
4- البوابة الإلكترونية لوزارة المالية بالسعودية بما فيها الخدمات الإلكترونية المقدمة للمستخدم الفرد مستوفية بسياسات حماية خصوصية المعلومات.
5- إن موظفي وزارة المالية لديهم درجة إدراك عالية لفهم متطلبات الوزارة فيما يخص خصوصية المعلومات وحمايتها والحفاظ على سريتها.
6- الجهات الرقابية لديها حس أمني عالي لمنع انتهاك المخاطر الخصوصية المحتملة او التخفيف منها.

المحور الثاني: التوصيات والمقترحات

في ظل النتائج المتوصل إليها في دراستنا والمتمثلة في علاقة استخدام إدارة المخاطر خصوصية المعلومات وحماية خصوصية المعلومات تمكننا من تقديم مجموعة التوصيات التالية:

1- تعيين فريق خبراء مختص بإدارة مخاطر خصوصية المعلومات وتحديد مسؤولياتهم في الوزارة المالية في المملكة العربية السعودية
2- سن سياسات واجراءات أكثر صرامة للمحافظة على حماية خصوصية المعلومات بما في ذلك تشفير البيانات الحساسة.
3- تكثيف الجهود التدريبية لموظفي وزارة المالية فيما يخص آلية التعامل مع المعلومات الحساسة والاجراءات الأمنية لضمان المحافظة على خصوصيتها.
4- الاستمرار في تطوير آلية التقييم الدوري لمخاطر خصوصية المعلومات والثغرات الأمنية في نظام المعلومات لوزارة المالية بالتعاون مع الجهات الرقابية ذات العلاقة.
5- استمرار هيئة الحكومة الرقمية في تحديث سياسات واجراءات إدارة المخاطر بشكل دوري لتغطية التهديدات الجديدة.
6- تعزيز التعاون بين الجهات الرقابية الحكومية والكيانات العامة والخاصة لتبادل المعلومات والخبرات وتحديد أفضل الممارسات لحماية المعلومات.
7- ديمومية تحسين الإجراءات بحيث تكون أكثر صرامة لإدارة الوصول إلى المعلومات الخاصة بالتزامن مع التطورات الحديثة في التقنية.
8- مراجعة التقارير الدورية عن حالة إدارة المخاطر وخصوصية المعلومات في وزارة المالية بشكل أكثر تفصيلاً واكمالها.

المراجع:

المراجع العربية:

1- الهادي. محمد. (2022). الذكاء الاصطناعي معالمة وتطبيقاته وتأثيراته التنموية والمجتمعية ط 1. الدار المصرية اللبنانية. مصر

2- سلايمي. جميلة، واخرون، (2019)."التحول بين الضرورة والمخاطر". (مجلة العلوم القانونية والسياسية). المجلد 10.العدد 2. الصفحات 944-967

3- هيئة الاتصالات وتقنية المعلومات السعودية. (2023)."مفهوم الخصوصية" https://www.cst.gov.sa/ar/Pages/default.aspx

4- محمود. هناء. (2022)."العلاقة بين التحول الرقمي والخدمات المالية" (المجلة العلمية للبحوث التجارية جامعة المنوفية) 2022/12/4

5- ريان. إيمان. (2021)." الحماية التشريعية للحق في خصوصية البيانات في العصر الرقمي"(مجلة كلية الشريعة والقانون بطنطا). المجلد 36. العدد 3. الصفحات 177-188

6- النحاس. أحمد. واخرون. (2022)."إدارة مخاطر التحول الرقمي" (المجلة العلمية للدراسات والبحوث المالية والإدارية). المجلد 13. العدد 6. الصفحات 1501-1513

7- عرب. يونس. (1972). (المخاطر التي تهدد خصوصية المعلومات في العصر الرقمي). https://kenanaonline.com/users/ahmedkordy/posts/323471

8- العتيبي. محمد. (2020)."تقييم مخاطر خصوصية المعلومات بوزارة العدل بالمملكة العربية السعودية".(جامعة الأمير نايف للعلوم الأمنية). https://repository.nauss.edu.sa/handle/123456789/50737/browse?rpp=20&offset=2642&etal=-1&sort_by=1&type=title&starts_with=P&order=ASC

9- موقع وزارة المالية بالمملكة العربية السعودية. (2023)."التحول الرقمي بالوزارة" https://www.mof.gov.sa/about/Pages/Enable.aspx

10-خنفر. الصديق. وكريم. حمزة. (2022)."أثر إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات". المجلد 1. العدد 4. الصفحات 502-522

- حاج. وعلي. قاسم. (2020)." إسهامات الاتحاد الإفريقي في عملية التحول الرقمي في إفريقيا قراءة في مشروع استراتيجية التحول الرقمي لإفريقيا". https://dspace.zu.edu.ly/handle/1/913
- صيفي. وحسنية. (2020). "الإدارة الإلكترونية الصحية وتحديات التحول الرقمي في الدول العربية-دراسة حالة مملكة البحرين" https://dspace.zu.edu.ly/handle/1/914

11-البار. والمرحبي. (2028)."التحول الرقمي كيف ولماذا" https://www.awforum.org/index.php/ar/مقالات-وبحوث-2018-/191-item/التحول-

12- هيئة الحكومة الرقمية. (2021)."التحول الرقمي" http://dga.gov.sa/digital-transformation#.ZBmGlz62onM.mailto

13- شديد. مصطفى. (2021). "تأثير التحول الرقمي على مستوى أداء الخدمة المقدمة بالتطبيق على موظفي الإدارة العامة للمرور بمحافظة القاهرة". المجلد 22. العدد 4. الصفحات 193-226 10.21608/JPSA.2021.200080

14- أجيال. (2023)."التحول الرقمي باستخدام المنهجية المرنة" https://dga.gov.sa/node/594

15- رشوان. وقاسم. (2020)."دور التحول الرقمي في رفع كفاءة أداء البنوك وجذب الاستثمارات" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3683715

16- الربيعة. صالح. (2013)."الأمن الرقمي وحماية المستخدم من مخاطر الانترانت" https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs/مركز%20التحميل/تقنية%20المعلومات/الملتقى%20الأول%20لتقنية%20المعلومات%201439هـ/أوراق%20العمل/Digital%20Security.pdf.

17- الموسوي. منى. (2013). "الخصوصية المعلوماتية واهميتها والتقنيات الحديثة عليها". (مجلة كلية بغداد للعلوم الاقتصادية الجامعية). المجلد 2013. العدد 4. الصفحات 303-355 https://www.iasj.net/iasj/download/51b569f8c8bd04b7

18- الدليل الاسترشادي لوزارة المالية. (2021)."الدليل الاسترشادي لإدارة المخاطر المبادئ الأساسية والممارسات التوجيهية" https://mof.gov.sa/Documents/risk-management-guide.pdf

المراجع الأجنبية:

21- IBM Security.(2021). Cost of data breach report –Risk Quanificatio https://www.ibm.com/downloads/cas/OJDVQGRY

22-Brysch. A.(2027).”Digital Transformation in Tourism Sector Challenges andOpportunities”

https://www.researchgate.net/publication/323557395_Digital_Transformation_in_the_Tourism_Sector_-_Challenges_and_Opportunities

23-Chen.D.and Zhao.H.(2012).” Data security and privacy protection issues in cloud computing”

10.4236/blr.2012.34020

24- KellyD.and others.(2020).” Date Privacy in Retail” https://www.sciencedirect.com/science/article/pii/S0022435920300531?via%3Dihub

جميع الحقوق محفوظة © 2023، الباحثة/ أمل محمد الوادعي، الباحثة/ هتون إبراهيم الوابل، الباحث/ مرتضى صابر الشبعان، المجلة الأكاديمية للأبحاث والنشر العلمي (CC BY NC)

Doi: https://doi.org/10.52132/Ajrsp/v5.49.7