

جامعة ميد أوشن



كلية الإدارة

تخصص إدارة المخاطر

دور الأمن السيبراني في إدارة مخاطر البيانات لدى الشركات: دراسة

تطبيقية على القطاع الخاص في المملكة العربية السعودية

إعداد الطالب/عمر محمد حسن ع شماوي

243001793

إشراف/

د. الفيصل عبد الحميد

العام الدراسي:

2025

بسم الله الرحمن الرحيم

## الشكر والتقدير

نحمد الله عز وجل الذي وفقنا في إتمام هذا البحث العلمي،

والذي ألهمنا الصحة والعافية والعزيمة.

فالحمد لله حمداً كثيراً

نتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور /

د. الفيصل عبد الحميد محمد حسن

على كل ما قدمه لنا من توجيهات ومعلومات قيمة ساهمت في إثراء موضوع دراستنا في

جوانبها المختلفة.

والشكر والتقدير موصول إلى إدارة جامعة ميد أوشن ممثلة بالكادر الأكاديمي والإداري، لما

قدموه من تسهيلات وتشجيع وتوفير الخدمات المطلوبة.

كما أتقدم بالشكر الجزيل لكل من لم يسعنا الحظ بذكر أسمائهم راجياً من المولي عز

وجل أن تكون هذه الدراسة نافذة لدراسات أخرى .

## المستخلص

هدفت هذه الدراسة إلى تحليل أثر الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) على إدارة مخاطر البيانات في مؤسسات القطاع الخاص بالمملكة العربية السعودية ، و اعتمدت الدراسة على المنهج الوصفي التحليلي، وبلغت عينة الدراسة (361) مفردة تم اختيارها باستخدام العينة العشوائية الطبقية، وتم تحليل البيانات باستخدام برنامج SPSS .

أظهرت نتائج الدراسة وجود أثر ذو دلالة إحصائية للأمن السيبراني بأبعاده مجتمعة على إدارة مخاطر البيانات، حيث تبين أن جميع الأبعاد الأربعة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) تساهم بدرجات متفاوتة في تعزيز قدرة المؤسسات على حماية بياناتها وتقليل التهديدات السيبرانية المحتملة. وقد كانت مساهمة "أمن المعلومات" و "أمن الشبكات" الأعلى تأثيرًا، بينما كان أثر "حماية البنية التحتية للمعلومات" بدرجة متوسطة ولكن دالة إحصائيًا.

واختتمت الدراسة بعدد من التوصيات أبرزها ضرورة دمج الأمن السيبراني ضمن استراتيجيات إدارة المخاطر، وتكثيف برامج التوعية والتدريب، وتحسين البنية التحتية التكنولوجية، بما يعزز حماية البيانات وضمان استمرارية الأعمال في مؤسسات القطاع الخاص.

**الكلمات المفتاحية:** الأمن السيبراني، إدارة مخاطر البيانات، أمن المعلومات، أمن الشبكات، أمن

الإنترنت، حماية البنية التحتية، القطاع الخاص، المملكة العربية السعودية.

## قائمة المحتويات

|    |                                        |
|----|----------------------------------------|
| أ  | بسم الله الرحمن الرحيم.....            |
| ب  | الإهداء.....                           |
| ب  | الشكر والتقدير.....                    |
| ج  | المستخلص.....                          |
| د  | قائمة المحتويات.....                   |
| ح  | قائمة الجداول.....                     |
| ي  | قائمة الأشكال.....                     |
| 1  | الفصل الأول: الإطار العام للدراسة..... |
| 1  | المقدمة.....                           |
| 3  | 1.1 مشكلة الدراسة:.....                |
| 3  | 2.1 أهمية الدراسة:.....                |
| 4  | 1.2.1 الأهمية العلمية:.....            |
| 4  | 2.2.1 الأهمية العملية:.....            |
| 5  | 3.1 أهداف الدراسة:.....                |
| 6  | 4.1 تساؤلات الدراسة.....               |
| 6  | 5.1 فروض الدراسة:.....                 |
| 7  | 6.1 الدراسات السابقة:.....             |
| 16 | 7.1 الفجوة البحثية.....                |
| 18 | 8.1 المنطلقات النظرية للدراسة:.....    |

|                                      |    |
|--------------------------------------|----|
| 9.1 المنهجية وطرق البحث:             | 20 |
| 10.1 مصادر جمع البيانات:             | 20 |
| 11.1 أدوات الدراسة:                  | 21 |
| 12.1 الأساليب الإحصائية المستخدمة:   | 21 |
| 13.1 حدود الدراسة:                   | 22 |
| الفصل الثاني: الإطار النظري:         | 24 |
| المبحث الأول: الأمن السيبراني:       | 24 |
| التمهيد:                             | 24 |
| 1.1.2 مفهوم الأمن السيبراني:         | 24 |
| 2.2.2 أهداف الأمن السيبراني:         | 25 |
| 3.2.2 أهمية الأمن السيبراني:         | 28 |
| 4.2.2 أبعاد الأمن السيبراني:         | 28 |
| المبحث الثاني: إدارة مخاطر البيانات: | 31 |
| تمهيد:                               | 31 |
| 1.2.2 مفهوم إدارة مخاطر البيانات:    | 31 |
| 2.2.2 أهمية إدارة مخاطر البيانات:    | 32 |
| 3.2.2 أهداف إدارة مخاطر البيانات:    | 34 |
| 4.2.2 مراحل إدارة مخاطر البيانات:    | 36 |
| الفصل الثالث: الطريقة والإجراءات:    | 39 |
| 1.3 تمهيد:                           | 39 |

|    |                                                   |
|----|---------------------------------------------------|
| 39 | 2.3 منهجية الدراسة.....                           |
| 39 | 3.3 مجتمع وعينة الدراسة :.....                    |
| 40 | 4.3 مصادر جمع البيانات.....                       |
| 41 | 5.3 أداة الدراسة : .....                          |
| 42 | 6.3 صدق أداة الدراسة :.....                       |
| 44 | 7.3 ثبات أداة الدراسة:.....                       |
| 46 | 8.3 الأساليب الإحصائية.....                       |
| 48 | الفصل الرابع تحليل البيانات واختبار الفرضيات..... |
| 48 | تمهيد.....                                        |
| 48 | 1.4 نتائج البيانات الديمغرافية.....               |
| 55 | 2.4 وصف متغيرات الدراسة.....                      |
| 68 | 3.4 اختبار فرضيات الدراسة.....                    |
| 77 | الفصل الخامس: النتائج والتوصيات.....              |
| 77 | تمهيد.....                                        |
| 77 | 1.5 مناقشة النتائج.....                           |
| 80 | 2.5 التوصيات.....                                 |
| 83 | Abstract.....                                     |
| 84 | قائمة المراجع.....                                |
| 84 | أولاً: المراجع العربية.....                       |
| 86 | ثانياً: المراجع الأجنبية.....                     |

88 .....الملاحق

89 .....استمارة استبيان

## قائمة الجداول

| رقم<br>الجدول | اسم الجدول                                                                     | رقم<br>الصفحة |
|---------------|--------------------------------------------------------------------------------|---------------|
| (1)           | الجدول (1): مقياس ليكرت الخماسي                                                | 38            |
| (2)           | الجدول (2) تصنيف ليكرت                                                         | 39            |
| (3)           | الجدول (3) علاقات الارتباط بين أبعاد المتغير المستقل (الأمن السيبراني)         | 41            |
| (4)           | الجدول (4): نتائج حساب معامل "كرونيخ ألفا"                                     | 42            |
| (5)           | الجدول (5): توزيع عينة الدراسة حسب الخصائص الديموغرافية (ن=361)                | 45            |
| (6)           | الجدول (6): توزيع عينة الدراسة حسب الفئة العمرية (ن = 361)                     | 46            |
| (7)           | الجدول (7): توزيع عينة الدراسة حسب المؤهل العلمي (ن = 361)                     | 47            |
| (8)           | الجدول (8): توزيع العينة حسب سنوات الخبرة (ن = 361)                            | 48            |
| (9)           | الجدول (9): توزيع العينة حسب نوع القطاع (ن = 361)                              | 49            |
| (10)          | الجدول (10): توزيع العينة حسب الإدارة التي يعمل بها المشاركون (ن = 361)        | 50            |
| (11)          | جدول (11): المتوسطات الحسابية والانحرافات المعيارية لأبعاد الأمن السيبراني     | 52            |
| (12)          | جدول (12): المتوسطات الحسابية والانحرافات المعيارية لفقرات (أمن المعلومات)     | 53            |
| (13)          | جدول (13): المتوسطات الحسابية والانحرافات المعيارية لفقرات (البعد أمن الشبكات) | 55            |

| رقم<br>الصفحة | اسم الجدول                                                                                                        | رقم<br>الجدول |
|---------------|-------------------------------------------------------------------------------------------------------------------|---------------|
| 57            | الجدول (14): المتوسطات الحسابية والانحرافات المعيارية لفقرات<br>بُعد "أمن الإنترنت" (ن = 361)                     | (14)          |
| 58            | الجدول (15): المتوسطات الحسابية والانحرافات المعيارية لفقرات<br>بُعد "حماية البنية التحتية للمعلومات" (ن = 361)   | (15)          |
| 60            | الجدول (16): المتوسطات الحسابية والانحرافات المعيارية لفقرات<br>متغير "إدارة مخاطر البيانات" (ن = 361)            | (16)          |
| 63            | جدول (17): نتائج تحليل الانحدار المتعدد لأثر أبعاد الأمن السيبراني<br>على إدارة مخاطر البيانات                    | (17)          |
| 65            | جدول (18): تحليل الانحدار الخطي البسيط لقياس أثر أمن<br>المعلومات على إدارة مخاطر البيانات                        | (18)          |
| 66            | جدول (19): تحليل الانحدار الخطي البسيط لقياس أثر البعد أمن<br>الشبكات على إدارة مخاطر البيانات                    | (19)          |
| 67            | جدول (20): تحليل الانحدار الخطي البسيط لقياس أثر البعد أمن<br>الإنترنت على إدارة مخاطر البيانات                   | (20)          |
| 69            | جدول (21): تحليل الانحدار الخطي البسيط لقياس أثر البعد حماية<br>البنية التحتية للمعلومات على إدارة مخاطر البيانات | (21)          |

## قائمة الأشكال

| رقم<br>الصفحة | اسم الشكل                                                           | رقم<br>الشكل |
|---------------|---------------------------------------------------------------------|--------------|
| 46            | الشكل (1): توزيع عينة الدراسة حسب الخصائص الديموغرافية<br>(ن=361)   | (1)          |
| 47            | الشكل (2): توزيع عينة الدراسة حسب الفئة العمرية (ن = 361)           | (2)          |
| 48            | الشكل (3): توزيع عينة الدراسة حسب المؤهل العلمي (ن = 361)           | (3)          |
| 49            | الشكل (4): توزيع العينة حسب سنوات الخبرة (ن = 361)                  | (4)          |
| 50            | الشكل (5): توزيع العينة حسب نوع القطاع (ن = 361)                    | (5)          |
| 51            | الشكل (6): توزيع العينة حسب الإدارة التي يعمل بها المشارك (ن = 361) | (6)          |

## الفصل الأول: الإطار العام للدراسة

### المقدمة

أصبح لزاماً على منظمات الأعمال في القرن الحادي والعشرين إتخاذ خطوات استباقية لاستشراف المستقبل وتطوير خططها الإبداعية المبنية على الحقائق والأدلة للتنبؤ بالمستقبل لاستغلال الفرص المتاحة والحد من آثار المخاطر التي قد تواجهها ؛ فالقيادات المتميزة القادرة على الاستغلال الأمثل للموارد المتاحة وتسخيرها لتقديم خدمات ومنتجات تفوق خدمات المنافسين أحد متطلبات النجاح لتحقيق النتائج المؤسسية المتميزة وتعزيز رضى أصحاب العلاقة لضمان استدامة أعمال تلك المنظمات وقدراتها التنافسية (Deaver-Vazquez et al., 2024).

أصبحت إدارة الأمن السيبراني في المنظمات ذات أهمية كبيرة ومتزايدة في ظل الأزمات المتسارعة التي يمر بها العالم بدءاً من الهجمات السيبرانية على الحكومات والمنظمات وانتهاء بالأفراد، مثل الهجمات الإلكترونية التي شنتها الولايات المتحدة عام 2019 على شبكة الكهرباء الروسية كرد على الإلكترونية عام 2017 على أحد مصانع شركة أرامكو السعودية، والهجمات التي تعرض لها بنك Flagstar الأمريكي من خلال نشر معلومات عن العملاء من قبل المخربين، ويذكر بأن أكثر من 2244 هجمة إلكترونية تحدث كل يوم بالعالم بتكلفة تتجاوز 11 تريليون دولار، وأن 71% من المنظمات في جميع أنحاء العالم هم ضحايا لتلك الهجمات بحسب ما نشرته مجلة إند بدنت على موقعها بتاريخ 28/06/2022 ؛ وبناء على ما تقدم أضحت جميع المنظمات باختلاف قطاعاتها تبحث عن كيفية اكتشاف الهجمات السيبرانية وقياس مخاطرها والإبلاغ عنها وإدارتها ومجابهتها، وقد رسخت تلك المخاطر وآثارها السلبية الكبيرة ضرورة تطبيق النهج الاحترازي لإدارة الأزمات بفعالية وكفاءة للحد من تأثيرها ومواجهة عواقبها لضمان استقرار النظام الإداري والمالي للمنظمات واستدامة أعمالها وبقاءها في السوق (Silva, 2024) إن المخاطر السيبرانية المتغيرة في سياقها وخصائصها وتأثيراتها قد يكون لها عواقب وخيمة على الشركات التي لا تمتلك الآليات المناسبة لمواجهتها (Kaushik, 2024)، فيما قد تعمل الشركات الرائدة على اقتناص ما تحتويه من فرص لتحويلها إلى قيمة مضافة لتعزيز أداءها وميزتها التنافسية (Ogborigbo et al., 2024).

وتعد إدارة مخاطر البيانات عنصراً حيوياً في استراتيجيات الحوكمة والأمن السيبراني، حيث تهدف إلى تحديد، تقييم، والتخفيف من المخاطر المرتبطة بجمع البيانات، تخزينها، معالجتها، ومشاركتها داخل المؤسسات، وتزايد أهمية هذه الإدارة في ظل تصاعد التهديدات السيبرانية، حيث أصبحت الشركات أكثر عرضة للاختراقات الأمنية، هجمات الفدية، والتسريبات المعلوماتية، مما قد يؤدي إلى خسائر مالية جسيمة، تضرر السمعة، ومخاطر قانونية، وتعتمد إدارة مخاطر البيانات على إجراءات تحليلية واستباقية تشمل تطبيق أنظمة التشفير، المصادقة المتقدمة، والمراقبة المستمرة، لضمان سرية البيانات وسلامتها وتوافرها في بيئة تشغيلية آمنة (Silva, 2024).

في سياق التحول الرقمي، أصبحت المؤسسات مطالبة بالامتثال للوائح حماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) في أوروبا، ومعايير NIST و ISO 27001، لضمان حماية أصولها الرقمية وتعزيز ثقة العملاء والشركاء، ولا تزال العديد من المؤسسات تفتقر إلى نهج متكامل لإدارة المخاطر السيبرانية، مما يؤدي إلى تعرض بياناتها لمخاطر متزايدة نتيجة الإهمال أو عدم كفاية التدابير الأمنية، وتكمن أهمية إدارة مخاطر البيانات في توفير إطار تنظيمي متكامل يساعد المؤسسات على تحليل المخاطر المحتملة، تطوير خطط استجابة فعالة، وتعزيز ثقافة الأمن السيبراني بين الموظفين، مما يضمن استدامة العمليات التشغيلية وتقليل الخسائر الناجمة عن الحوادث السيبرانية (Deaver-Vazquez et al., 2024).

ونظراً لأن الشركات تتجه بشكل متزايد نحو التحول الرقمي والاعتماد على التقنيات الحديثة، فإن تطوير إطار شامل لإدارة الأمن السيبراني يعد أمراً ضرورياً لمواجهة التهديدات السيبرانية المتطورة، من خلال اعتماد استراتيجيات استباقية تشمل التحليل المستمر للمخاطر، تطبيق أحدث تقنيات الحماية، وتعزيز ثقافة الأمن السيبراني داخل المؤسسات. وقد أكدت الدراسات أن الشركات التي تستثمر في الأمن السيبراني تحقق أداءً أفضل، زيادة في حصتها السوقية، وتحقيق أرباح أعلى في بيئة الأعمال العالمية التنافسية. (Olaniyi et al., 2023).

بناءً على ذلك، تهدف هذه الدراسة إلى استكشاف دور الأمن السيبراني بأبعاده المختلفة في إدارة مخاطر البيانات لدى المؤسسات الخاصة في المملكة العربية السعودية

## 1.1 مشكلة الدراسة:

في ظل التطور المتسارع للتقنيات الرقمية، أصبحت المؤسسات الخاصة أكثر عرضة للتهديدات السيبرانية، مما يفرض الحاجة إلى تعزيز استراتيجيات الأمن السيبراني لحماية البيانات وإدارة المخاطر بفعالية، ورغم الجهود المبذولة لا تزال العديد من الشركات تعتمد على أساليب تقليدية في حماية بياناتها، مما يجعلها غير مؤهلة للتعامل مع المخاطر المتزايدة والمتطورة (Deaver-Vazquez et al., 2024).

وتشير الدراسات إلى أن الأمن السيبراني لم يعد مجرد خيار تقني، بل أصبح عنصراً حاسماً في استدامة الأعمال، حيث تؤدي الاختراقات الأمنية إلى خسائر مالية كبيرة، وتراجع ثقة العملاء، ومخاطر قانونية بسبب عدم الامتثال للوائح حماية البيانات (Silva, 2024)، ولا تزال هناك فجوة في الأبحاث التي تربط بين أبعاد الأمن السيبراني المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) وإدارة مخاطر البيانات، خاصة في بيئة الأعمال السعودية (Ogborigbo et al., 2024).

على الرغم من أن بعض الشركات بدأت في تبني تقنيات متقدمة مثل التشفير، المصادقة الثنائية، والمراقبة المستمرة، إلا أن مستوى الوعي والتنفيذ لهذه التدابير يختلف بشكل كبير بين المؤسسات، مما يعوق تحقيق أمن سيبراني شامل يحمي الأصول الرقمية بفعالية (Kaushik, 2024). كما أن غياب ثقافة أمنية قوية داخل المؤسسات يعزز من احتمالية وقوع الاختراقات، مما يستدعي دراسة أعمق حول كيفية دمج الأمن السيبراني في الهيكل التنظيمي للمؤسسات الخاصة (Olaniyi et al., 2023).

بناءً على ما سبق، تنبع مشكلة الدراسة من الحاجة إلى تقييم دور الأمن السيبراني بأبعاده المختلفة في إدارة مخاطر البيانات داخل المؤسسات الخاصة في المملكة العربية السعودية.

## 2.1 أهمية الدراسة:

تبرز أهمية هذه الدراسة من خلال تناولها لدور الأمن السيبراني في إدارة مخاطر البيانات في القطاع الخاص بالمملكة العربية السعودية، حيث تتزايد الحاجة إلى استراتيجيات قوية لحماية البيانات في ظل التهديدات السيبرانية المتصاعدة. تنقسم أهمية الدراسة إلى الجوانب التالية:

### 1.2.1 الأهمية العلمية:

- تساهم الدراسة في إثراء المعرفة العلمية حول العلاقة بين الأمن السيبراني وإدارة مخاطر البيانات، مما يساعد الباحثين والمتخصصين في تطوير فهم أعمق للموضوع.
- تسلط الضوء على أحدث الممارسات والتقنيات المستخدمة في الأمن السيبراني، مثل التشفير، والجدران النارية، وأنظمة الكشف عن الاختراقات، ودورها في الحد من المخاطر السيبرانية.
- تقدم إطارًا تحليليًا لتقييم مدى فعالية الأمن السيبراني في حماية البيانات وتقليل التهديدات في الشركات الخاصة.
- تساعد في سد الفجوة البحثية حول كيفية تأثير تطبيقات الأمن السيبراني على استدامة الأعمال في القطاع الخاص، خاصة في سياق الاقتصاد الرقمي المتنامي في المملكة العربية السعودية.
- توفر أساسًا للباحثين لإجراء دراسات مقارنة بين القطاعات المختلفة، وتحليل مدى تأثير التدابير الأمنية في تقليل المخاطر الرقمية على نطاق أوسع.

### 2.2.1 الأهمية العملية:

- توفر نتائج الدراسة إرشادات واضحة للمؤسسات الخاصة حول كيفية تعزيز استراتيجيات إدارة المخاطر السيبرانية وتحسين إجراءات الحماية.
- تساعد المؤسسات على تحديد نقاط الضعف في بنيتها التحتية الرقمية وتطوير خطط استجابة فعالة ضد التهديدات السيبرانية.

- تسهم في رفع وعي الشركات الخاصة بأهمية الامتثال للوائح التنظيمية المتعلقة بحماية البيانات، مثل معايير ISO 27001 والتشريعات الوطنية مثل نظام مكافحة الجرائم المعلوماتية في المملكة العربية السعودية.
- تدعم الشركات في تحقيق ميزة تنافسية من خلال بناء ثقة العملاء وتعزيز سمعتها في السوق عبر تطبيق سياسات أمن سيبراني قوية.

### 3.1 أهداف الدراسة:

- هدفت الدراسة إلى التعرف على دور الأمن السيبراني بأبعاده ( أمن المعلومات، وأمن الشبكات، وأمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية ، وتتفرع منها عدة أهداف فرعية منها :
  - تحليل تأثير أمن المعلومات على تحسين إدارة مخاطر البيانات وتقليل احتمالية تسرب المعلومات في المؤسسات الخاصة.
  - دراسة دور أمن الشبكات في تعزيز حماية البيانات داخل بيئات العمل الخاصة والحد من التهديدات السيبرانية التي تؤثر على إدارة المخاطر.
  - تقييم مدى تأثير أمن الإنترنت على إدارة مخاطر البيانات، من خلال تحليل دور التقنيات الدفاعية في حماية البيانات من الاختراقات والهجمات الإلكترونية.
  - استكشاف دور حماية البنية التحتية للمعلومات في تقليل المخاطر السيبرانية المرتبطة بتخزين البيانات ومعالجتها داخل القطاع الخاص.
  - قياس مدى وعي المؤسسات الخاصة في المملكة العربية السعودية حول تأثير الأمن السيبراني على إدارة مخاطر البيانات ومدى التزامها بممارسات الحماية الرقمية.
  - تحليل العلاقة بين تنفيذ استراتيجيات الأمن السيبراني ومستوى تقليل المخاطر المتعلقة بالبيانات وفقاً للمعايير والتشريعات الوطنية والدولية.

- اقتراح آليات واستراتيجيات لتحسين إدارة مخاطر البيانات من خلال تبني أحدث تقنيات الأمن السيبراني في الشركات الخاصة بالمملكة العربية السعودية.

#### 4.1 تساؤلات الدراسة

**السؤال الرئيسي:** ما هو دور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية؟ ، وتتفرع منه عدة أهداف فرعية منها :

- كيف يؤثر أمن المعلومات على تقليل مخاطر تسرب البيانات في المؤسسات الخاصة؟
- ما هو دور أمن الشبكات في الحد من التهديدات السيبرانية وتحسين إدارة مخاطر البيانات؟
- كيف يساهم أمن الإنترنت في حماية البيانات وتقليل المخاطر الناجمة عن الهجمات الإلكترونية؟
- ما مدى تأثير حماية البنية التحتية للمعلومات على إدارة مخاطر البيانات واستمرارية الأعمال؟
- ما هو مستوى وعي المؤسسات الخاصة في المملكة العربية السعودية بأهمية الأمن السيبراني في إدارة مخاطر البيانات؟
- كيف يؤثر تنفيذ استراتيجيات الأمن السيبراني على مدى تقليل مخاطر البيانات وفقًا للمعايير والتشريعات الوطنية والدولية؟
- ما هي أفضل الآليات والاستراتيجيات المقترحة لتحسين إدارة مخاطر البيانات في القطاع الخاص من خلال تطبيق تقنيات الأمن السيبراني؟

#### 5.1 فروض الدراسة:

لتحقيق أهداف الدراسة فقد أعتمد على مجموعة من الفرضيات الآتية:

**الفرضية الرئيسية الأولى:** يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لدور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية

للمعلومات) على إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية، وينبثق من هذه الفرضية مجموعة من الفرضيات الفرعية التالية:

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن المعلومات على إدارة مخاطر البيانات في المؤسسات الخاصة.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن الشبكات على تحسين إدارة مخاطر البيانات وتقليل التهديدات السيبرانية.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن الإنترنت على تقليل المخاطر السيبرانية وحماية البيانات من الهجمات الإلكترونية.
- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لحماية البنية التحتية للمعلومات على تعزيز إدارة مخاطر البيانات وضمان استمرارية الأعمال.

## 6.1 الدراسات السابقة:

✍ دراسة (Deaver-Vazquez et al., 2024)

هدف البحث إلى استكشاف دور تحديد المخاطر السيبرانية الكمية (CRQ) في تعزيز دقة وموضوعية إدارة المخاطر السيبرانية في الشركات الخاصة. يركز البحث على أهمية التقدير الرقمي لاحتمالية التهديدات وتأثيراتها المالية والتشغيلية، مما يساهم في توفير إطار عمل موحد لاتخاذ قرارات أكثر دقة في مجال الأمن السيبراني. كما يتناول البحث أبعاد المخاطر السيبرانية الأساسية، مثل احتمالية وقوع الهجمات، وحجم التأثير على الأصول الرقمية، وفعالية استراتيجيات التخفيف، مع التركيز على قدرة CRQ على تحسين كفاءة تخصيص الموارد الأمنية وتقليل التحيزات الذاتية في عملية التقييم.

تعتمد الدراسة على منهج تحليل المخاطر الكمي من خلال دراسة تطبيقية على القطاع الخاص في المملكة العربية السعودية. تم جمع البيانات من عينة مكونة من عدد من الشركات الخاصة التي تعتمد

استراتيجيات متنوعة في الأمن السيبراني، حيث تم تحليل بيانات المخاطر باستخدام نماذج كمية تعتمد على مؤشرات قابلة للقياس، مثل معدل حدوث الهجمات، التكاليف المحتملة للأضرار، وكفاءة استراتيجيات الاستجابة.

كشفت نتائج الدراسة أن استخدام النهج الكمي في تقييم المخاطر السيبرانية يعزز دقة اتخاذ القرارات، ويحسن الشفافية عند التواصل مع أصحاب المصلحة، ويقلل من عدم اليقين المرتبط بالأساليب التقليدية. كما أظهرت الدراسة أن الشركات التي تبنت CRQ تمكنت من تحسين استراتيجياتها الأمنية عبر تحديد أولويات المخاطر بناءً على التأثيرات الفعلية. بناءً على هذه النتائج، توصي الدراسة بضرورة اعتماد المؤسسات الخاصة في المملكة العربية السعودية لمنهجيات التقييم الكمي للمخاطر السيبرانية، وتعزيز ثقافة إدارة المخاطر المستندة إلى البيانات، وضمان تكامل الأمن السيبراني ضمن إطار إدارة المخاطر المؤسسية الشاملة.

#### دراسة (Silva, 2024)

هدفت الدراسة إلى تحليل التحديات القانونية والتنظيمية التي تنشأ عن الحوادث السيبرانية، مثل اختراق البيانات وهجمات الفدية وانتهاكات الأنظمة، وتأثيرها على الشركات والجهات التنظيمية، وتركز الدراسة على أبعاد متعددة، تشمل الالتزامات القانونية، المخاطر التنظيمية، الشفافية المؤسسية، وإدارة المخاطر السيبرانية، وتعتمد الدراسة على منهج تحليلي كمي ونوعي.

وأظهرت النتائج أن الأطر القانونية الحالية غير كافية لمعالجة الأضرار غير المالية، مما يزيد من مخاطر التقاضي ضد الشركات، خاصة في حال عدم الامتثال لممارسات إدارة المخاطر السيبرانية، كما كشفت الدراسة عن وجود نقص في الإفصاح عن المخاطر السيبرانية، على الرغم من المتطلبات القانونية. بناءً على هذه النتائج، توصي الدراسة بضرورة تطوير أطر قانونية جديدة تتضمن الأضرار النفسية، تعزيز الشفافية المؤسسية في الإفصاح عن المخاطر السيبرانية، وزيادة تبني استراتيجيات

استباقية لإدارة المخاطر، مثل معايير NIST وAICPA، لتعزيز القدرة المؤسسية على مواجهة التهديدات السيبرانية بفاعلية.

#### دراسة (Ogborigbo et al., 2024)

هدفت الدراسة إلى تحديد استراتيجيات تعزيز الأمن السيبراني في أنظمة التحليل الذكي للأعمال (BI)، من خلال استكشاف الأساليب والتقنيات التي يمكن استخدامها لحماية البيانات وتقليل المخاطر السيبرانية، وتشمل الأبعاد التي تركز عليها الدراسة: تقنيات التشفير المتقدمة، المصادقة الثنائية، أنظمة المراقبة، وأثر ثقافة الأمن السيبراني داخل المؤسسات على الحماية الفعالة للبيانات، وتعتمد الدراسة على نهج بحثي مختلط.

أظهرت النتائج أن تطبيق الأمن السيبراني بشكل استراتيجي يؤدي إلى تحسين حماية البيانات، وتقليل مخاطر الاختراقات، وتعزيز ثقة العملاء، وضمان الامتثال للوائح. كما كشفت الدراسة أن المؤسسات التي تستثمر في تدابير مثل تقنيات التشفير الحديثة، المصادقة المتقدمة، والمراقبة المستمرة تتمتع بمستويات أمان أعلى، مما يقلل من الخسائر الناتجة عن الهجمات السيبرانية.

بناءً على هذه النتائج، توصي الدراسة بتطوير سياسات أمنية قوية، تدريب الموظفين على أساليب الأمن السيبراني، وتحديث الأنظمة بشكل دوري وفقاً لأحدث معايير الأمان مثل NIST وISO 27001 لضمان استمرارية الأعمال وتعزيز مكانة المؤسسات في السوق.

#### دراسة (Kaushik, 2024)

هدفت الدراسة إلى تقديم منهجية شاملة مبتكرة لإعادة تعريف نهج المؤسسات في حماية أصولها المعلوماتية الحيوية، من خلال تنفيذ وتقييم استراتيجية متكاملة للأمن السيبراني، وتعتمد الدراسة على منهج تحليلي تطبيقي، حيث يتم دمج التحليلات المتقدمة، تقنية البلوك تشين، وخوارزميات التعلم الآلي لإنشاء نموذج أكثر دقة وقدرة على التنبؤ بالتهديدات السيبرانية والتعامل معها بفعالية، وتشمل العينة

مجموعة متنوعة من المؤسسات التي تواجه تحديات أمنية مختلفة، حيث تم اختبار المنهجية المقترحة عبر تجارب ميدانية وتحليل بيانات الأمن السيبراني، لتقييم مدى فعاليتها في تعزيز قدرات الدفاع الرقمي. تم تحليل البيانات من خلال نماذج محاكاة المخاطر السيبرانية وأنظمة إدارة المعلومات الأمنية لتقييم كفاءة التدابير الوقائية وتحديد سبل تحسينها.

أظهرت النتائج أن تطبيق هذه المنهجية الشاملة يعزز وضع الأمن السيبراني للمؤسسات بشكل جذري، من خلال تحسين القدرات التعاونية، وزيادة المرونة الأمنية، وبناء بيئة سيبرانية متماسكة ومتطورة. كما بينت الدراسة أن التكامل بين التحليلات المتقدمة والذكاء الاصطناعي والتقنيات الحديثة يساهم في خفض احتمالات الاختراقات الأمنية، وتحسين الاستجابة للحوادث، وتعزيز استدامة استراتيجيات الأمن السيبراني.

بناءً على هذه النتائج، توصي الدراسة باعتماد نهج أمني متكامل، يشمل تقنيات الذكاء الاصطناعي والبلوك تشين، وتعزيز ثقافة الأمن السيبراني داخل المؤسسات، وتطوير استراتيجيات استباقية لمواجهة التهديدات المستقبلية، لضمان حماية المعلومات وتحقيق مستويات أمان أعلى تتماشى مع تطورات العصر الرقمي.

#### دراسة (Olaniyi et al., 2023)

هدفت الدراسة إلى تحليل أهمية بناء ثقافة مخاطر قوية داخل المؤسسات لضمان نجاح استراتيجيات إدارة المخاطر المؤسسية (ERM) واستدامتها، وتعتمد الدراسة على نهج تحليلي تطبيقي يركز على تقييم تأثير العوامل التنظيمية والثقافية على نجاح إدارة المخاطر المؤسسية. تشمل العينة مجموعة من الشركات التي تعتمد ERM، حيث تم تحليل استراتيجياتها التنظيمية، ومستويات الشفافية، وتفاعل الموظفين مع سياسات المخاطر. كما تم قياس مدى تكامل إدارة المخاطر مع عناصر الحوكمة المؤسسية، التخطيط الاستراتيجي، تقييم الأداء، وتدفق المعلومات داخل المؤسسات.

كشفت النتائج أن بناء ثقافة مخاطر قوية داخل المؤسسات يساعد على تحقيق استدامة إدارة المخاطر المؤسسية (ERM)، ويؤدي إلى تحسين الحوكمة، وتعزيز عمليات اتخاذ القرار، وزيادة القدرة التنافسية. كما أظهرت الدراسة أن وضوح الأدوار، التواصل الشفاف، وإشراك الموظفين في عمليات إدارة المخاطر يساهم في التغلب على الحواجز التنظيمية وتحقيق نجاح طويل الأمد في ERM. بناءً على هذه النتائج، توصي الدراسة بدمج التقنيات الحديثة في إدارة المخاطر، تعزيز برامج التدريب والتوعية، وإنشاء قنوات اتصال فعالة بين جميع المستويات الإدارية لضمان استمرارية الأداء الفعال لأنظمة إدارة المخاطر المؤسسية.

#### ✍ دراسة ( العبدالات والشورة، 2023)

هدفت الدراسة للتعرف الى أثر الأمن السيبراني بأبعاده تحديد (الأدوار والمسؤوليات ، أمن وسلامة المعلومات ، البنية التحتية الإلكترونية، تدريب العاملين ) والتسويق الإلكتروني بأبعاده خدمات البنك الإلكتروني ، الترويج الإلكتروني ، التوزيع الإلكتروني ، إدارة علاقات العملاء الإلكترونية في البنوك التجارية الأردنية ، استخدمت الدراسة المنهج الوصفي التحليلي لتفسير الأثر بين متغيرات الدراسة و تم استخدام مجموعة من الأساليب الإحصائية التي تشتمل عليها الحزمة الإحصائية للعلوم الاجتماعية (SPSS) وذلك لغايات تحليل البيانات ، تم تطوير الاستبانة كأداة لجمع بيانات الدراسة استخدمت الدراسة على عينة العشوائية الطبقية التناسبية حيث بلغ حجم العينة (299) موظف وموظفة وجاءت ممثلة لجميع العاملين في أقسام التسويق وتكنولوجيا المعلومات في البنوك التجارية الأردنية في العاصمة عمان .

أظهرت النتائج وجود أثر للأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية ، وفق متغيرات المستقل تحديد الأدوار والمسؤوليات ، امن وسلامة المعلومات والبيانات، البنية التحتية الإلكترونية ، تدريب العاملين وكانت النتائج الدراسة أن الأمن السيبراني يساهم في حماية الأنظمة الإلكترونية من الوصول أو الاستخدام أو الكشف غير المصرح ، ويعد الأمن السيبراني مهما في التسويق الرقمي في البنوك لأنه يساعد في حماية موقع الويب الخاص فيها عبر الأنترنت من التعرض للاختراق ، ضمان

تحديد أدوار ومسؤوليات واضحة لجميع الأطراف المشاركة في تطبيقات وضوابط الأمن السيبراني يؤثر إيجاباً على التسويق الإلكتروني.

ولقد أوصت الدراسة العمل على مواكبة العمل لتزويد العاملين في البنوك التجارية الأردنية بالتقنيات الحديثة بأمن المعلومات والفضاء السيبراني ، وتشجيع البنوك على التقييم المستمر للثغرات ونقاط الضعف في نظم المعلومات ثم إعداد كوادر بشرية مؤهلة ومتخصصة في الأمن السيبراني والاستفادة من التجارب الدولية في هذا المجال.

#### ✍ دراسة (الفلاح وآخرون، 2023)

هدفت الدراسة إلى التعرف على تطبيق معايير الأمان السيبراني وأثرها على أداء شركات الاتصالات في الأردن. بناءً على مراجعة الدراسات السابقة وتحليلها، ذلك من خلال استخدام المنهج الوصفي التحليلي وتوزيع استبانة على عينة من الموظفين والمديرين حيث تم تطوير نموذج يعتبر معايير إدارة الأمان السيبراني (أمن المعلومات، وأمن الشبكات، وأمن الإنترنت، وحماية البنية التحتية للمعلومات) كمتغيرات مستقلة، وأداء شركات الاتصالات الأردنية الفاعلية، الكفاءة الإنتاجية، الإبداع كمتغير تابع.

توصلت النتائج إلى أن تطبيق معايير الأمان السيبراني بشكل سليم يؤدي إلى أداء متميز للشركات الاتصالات، حيث يُسهم تحسين الإنتاجية، وزيادة الفاعلية، وتعزيز الكفاءة والتشجيع على الابتكار، وأظهرت نتائج الدراسة أن تطبيق معايير الأمان السيبراني يسهم في تحسين الإنتاجية، وزيادة الفاعلية، وتعزيز الكفاءة، وتشجيع على الابتكار في شركات الاتصالات في الأردن. توصل البحث إلى استنتاجاته بناءً على تحليل البيانات وفحص فرضيات الدراسة، وقدم توصيات عملية لتعزيز استخدام معايير الأمان السيبراني كأداة استراتيجية لتحسين أداء شركات الاتصالات في المستقبل.

#### ✍ دراسة (الحجاية والحباشة، 2023)

هدفت الدراسة إلى التعرف على أثر الثقافة التنظيمية على الأمن السيبراني في الحكومة الإلكترونية وزارة العدل أنموذجاً"، حيث تم استخدام المنهج الوصفي التحليلي وتم استخدام استبيان مكون من (28) فقره واعتماد تحليل الانحدار البسيط ( Simple Linear Regression)، وتم التأكد من صدق الأداة وثباتها واستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) لتحليل البيانات. ويتكون مجتمع الدراسة من الموظفين العاملين في وزارة العدل، وتم أيضاً اختيار عينة من مجتمع الدراسة باستخدام الطريقة الطبقية التناسبية العشوائية، وتكونت العينة من (97) موظفاً عاملاً في وزارة العدل. وخلصت الدراسة إلى النتائج التالية:

تؤكد الدراسة أن تطبيق الثقافة التنظيمية بأبعادها وتطبيق الأمن السيبراني بأبعاده في الحكومة الإلكترونية في وزارة العدل - الأردن كان بدرجة موافقة عالية.

وتوصي الدراسة بتعزيز الشفافية والمساءلة والاحترام والمصادقية لدى موظفي الدوائر الحكومية الأردنية، وتوصي الدراسة بالإشارة إلى أهمية دور القادة في تشجيع ودعم الثقافة التنظيمية التي تركز على الأمن السيبراني، من خلال تحديد دور الأولويات وتوفير الموارد وتعزيز التوعية والتدريب.

✍ دراسة ( على وآخرون، 2023)

هدف البحث إلى تحليل أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني. ولتحقيق هذا الهدف تم تقسيم البحث إلى شقين، الشق النظري لتأصيل موضوع البحث واستطلاع الجهود السابقة في هذا المجال، والشق الميداني لاختبار فروض البحث، وذلك من خلال قائمة استبيان كأحد الأساليب المقترحة لتجميع البيانات الأولية من عينة البحث، ولقد تم تصميمها بشكل مبسط ومختصر بقدر المستطاع والتي تتعلق بأثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني.

وقد توصلت نتائج البحث إلى وجود علاقة ذات دلالة إحصائية بين دعم دور المراجعة الداخلية وتعزيز أنظمة الأمن السيبراني.

هدف البحث إلى التعرف على "أثر وعى العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني في البنوك الحكومية بمحافظة بورسعيد مع اختبار العلاقة ميدانيا بين المتغيرين، ومعرفة مدى العلاقة بين أبعاد وعى العملاء بالقرصنة الإلكترونية، الأمن السيبراني من وجهة نظر عملاء البنوك. ، وقد اعتمدت الباحثة على أسلوب العينة العشوائية من البنوك الحكومية بمحافظة بورسعيد وذلك نظرا لكبر حجم مجتمع البحث فإن أسلوب الحصر الشامل في جميع البيانات الخاصة بالبحث سيكون أمر صعب جدا لاعتبارات الوقت والجهد والتكلفة، وقد استخدمه أداة دراسة متمثلة في "استبانة"، واستند البحث على "المنهج الوصفي"، وتكون مجتمع البحث من العملاء بالبنوك الحكومية بمحافظة بورسعيد وتم توزيع (450) واستخدام برنامج التحليل الإحصائي (SPSS) للإجابة عن أسئلة البحث، وخلصت لمجموعة من النتائج كان أبرزها بأن مستوى ودور إدارة الحماية البنكية كان مرتفعا، وكذلك بينت البحث وجود دور الأمن السيبراني بدلالة أبعاده (الجهود التنظيمية، المتطلبات الفنية، التنسيق مع المؤسسات الأخرى، رصد وتقييم التهديدات) في التوعية والحد من الجرائم المالية، أظهرت نتائج التحليل الإحصائي بأن فاعلية إجراء الرقابة الداخلية في توفير الأمن السيبراني في التصدي للجرائم (القرصنة الإلكترونية) وذلك من خلال توفير آليات مناسبة لتطوير معارف ومهارات للعملاء الحاليين والمستقبليين ورفع مستوى الوعي والإرشاد وتمكينهم من فهم المخاطر الأساسية للمعاملات التي يجرونها مع البنوك والتصدي من عمليات الاحتيال التي يعرض لها العملاء وكيفية توفير وتوضيح الطرق التي من خلالها يقوم المحتالون بخداع ضحاياهم .

أوصت الدراسة بضرورة تضافر الجهود بين القطاعات الحكومية ومن ضمنها البنوك في التعاون والتنسيق فيما بينها لأجل تطوير وتحسين إدارة الأمن السيبراني والقدرة علي توفير الثقافة البنكية ودورها في تحقيق التوعية المصرفية والتصدي للقرصنة الإلكترونية بالإضافة إلي زيادة الأبحاث المرتبطة بالأمن السيبراني إذ تبين قلة في هذه الدراسات وخصوصا العربية منها.

هدفت الدراسة إلى التعرف على دور الأمن السيبراني في تحقيق الميزة التنافسية من خلال بحث وتحليل البرامج التي يقوم باستخدامها الموظفين والمستفيدين وتحديد دور الأمن السيبراني فيها وتغطية الفجوة العلمية في هذا المجال، وتم استخدام المنهج الوصفي التحليلي، حيث تم استخدام الاستبانة لاستطلاع عينة البحث بهدف جمع البيانات، وتكون مجتمع البحث من الموظفين الإداريين بمطار الملك عبد العزيز الدولي بجدة حيث تم اختيار عينة عشوائية بسيطة مقدارها (340) موظف .

وتوصلت نتائج الدراسة إلى وجود دور إيجابي وبدرجة كبيرة في تحقيق الميزة التنافسية بمطار الملك عبد العزيز الدولي، ووجود علاقة عكسية ذات أثر سلبي بين توفر الخصوصية في مطار الملك عبد العزيز وتحقيق الميزة التنافسية، ووجود علاقة طردية ذات أثر موجب وأن التعزيز كمتغير مستقل يؤثر في تحقيق الميزة التنافسية، وكشفت نتائج الدراسة أن الميزة التنافسية تتحقق بدرجة كبيرة في مطار الملك عبد العزيز الدولي، وأوصت الباحثة بضرورة الاستمرار في تحقيق درجة عالية في مستوى الأمن السيبراني في مطار الملك عبد العزيز بجدة من خلال أبعاده (السرية، الخصوصية، والتعزيز)، حيث إن ذلك يعتبر جزء من الأمن الوطني للمملكة العربية السعودية، وذلك لأن أمن المعلومات الآن أصبح جزءاً أصيلاً في مجال علوم الأمن، ومراجعة أوجه الخلل في عناصر الخصوصية.

## 7.1 الفجوة البحثية

على الرغم من الاهتمام المتزايد بالأمن السيبراني ودوره في إدارة مخاطر البيانات، إلا أن الدراسات السابقة لا تزال تفتقر إلى تحليل متكامل يجمع بين جوانب الأمن السيبراني المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) وتأثيرها على إدارة مخاطر البيانات في القطاع الخاص في المملكة العربية السعودية. ركزت الأبحاث السابقة على أحد هذه الأبعاد بشكل منفصل أو في سياقات محددة، مثل البنوك، شركات الاتصالات، أو المؤسسات الحكومية، دون تقديم نموذج شامل يوضح الترابط بين هذه العناصر داخل البيئة التجارية الخاصة في المملكة.

كما أظهرت الدراسات السابقة اهتمامًا بالمعايير القانونية والتنظيمية، مثل دراسة Silva (2024) التي تناولت الأطر القانونية والتحديات التنظيمية للحوادث السيبرانية، لكنها لم تستكشف بشكل كافٍ كيف يمكن للقطاع الخاص في المملكة العربية السعودية مواءمة استراتيجيات الأمن السيبراني مع هذه اللوائح لضمان الامتثال والحد من المخاطر القانونية. بالإضافة إلى ذلك، لم تتعمق الأبحاث في كيفية تأثير البيئة القانونية على تطبيق الأمن السيبراني بشكل عملي داخل المؤسسات الخاصة، وما إذا كان هناك التزام حقيقي من الشركات بتلك القوانين أو مجرد امتثال شكلي.

على صعيد آخر، ركزت دراسات مثل Deaver-Vazquez et al (2024) على النهج الكمي لتحديد المخاطر السيبرانية (CRQ)، وأكدت أن هذا الأسلوب يعزز دقة اتخاذ القرار وتقليل التحيزات الذاتية. ومع ذلك، فإن هذه الدراسة لم تتناول بشكل كافٍ كيفية دمج CRQ مع استراتيجيات الأمن السيبراني التقليدية، مما يترك فجوة بحثية حول مدى توافق التحليل الكمي مع الحلول الأمنية الفعلية المستخدمة في المؤسسات الخاصة، وخاصة في المملكة العربية السعودية حيث تختلف التحديات السيبرانية بناءً على طبيعة السوق المحلي والبنية التحتية الرقمية.

كما أن الدراسات مثل Ogborigbo et al (2024) التي تناولت الأمن السيبراني في أنظمة التحليل الذكي للأعمال (BI) تركزت على التكنولوجيا الحديثة مثل التشفير المتقدم، المصادقة الثنائية، والمراقبة

المستمرة، لكنها لم توضح كيف يمكن لهذه التقنيات أن تندمج في نموذج متكامل للأمن السيبراني وإدارة المخاطر في بيئات الأعمال المختلفة. من هنا، تبرز الحاجة إلى دراسة تربط بين الحلول التقنية الحديثة والاحتياجات الأمنية الواقعية في المؤسسات الخاصة بالمملكة.

ومن منظور أكثر شمولية، تناولت دراسة Kaushik (2024) منهجية جديدة في الأمن السيبراني من خلال تقنيات البلوك تشين والذكاء الاصطناعي، لكنها لم تتطرق إلى مدى قابلية تطبيق هذه المنهجية في الشركات الخاصة السعودية، خاصة مع التحديات الفعلية التي قد تواجهها تلك الشركات عند تبني هذه التقنيات، سواء من ناحية التكاليف أو من ناحية التوافق مع البنية التحتية المتاحة. لذا، فإن البحث في كيفية دمج الحلول التقنية الحديثة مع واقع الأمن السيبراني في القطاع الخاص السعودي يمثل فجوة بحثية تستحق الدراسة.

أخيراً، ركزت بعض الأبحاث مثل Olaniyi et al (2023) على ثقافة المخاطر في المؤسسات ودورها في استدامة إدارة المخاطر، لكن لم يتم ربط هذا المفهوم مع عوامل الأمن السيبراني، مما يجعل هناك حاجة لدراسة توضح كيف يمكن تعزيز ثقافة الأمن السيبراني في القطاع الخاص وتأثيرها على إدارة المخاطر السيبرانية بشكل فعال. في ظل بيئة الأعمال السعودية التي تشهد تطورات رقمية سريعة، لا يزال من غير الواضح مدى إدراك الشركات لأهمية ثقافة الأمن السيبراني، وكيفية دمجها في عملياتها اليومية للحماية من التهديدات السيبرانية.

تكشف الفجوة البحثية عن غياب دراسة متكاملة تستكشف العلاقة بين جميع أبعاد الأمن السيبراني وإدارة مخاطر البيانات في القطاع الخاص السعودي، مع التركيز على الجوانب القانونية، التكامل بين التقنيات الحديثة والممارسات التقليدية، والتحديات الفعلية التي تواجه المؤسسات في تطبيق استراتيجيات الأمن السيبراني. من هنا، تأتي أهمية هذه الدراسة لسد هذه الفجوة وتقديم نموذج شامل يعالج هذه القضايا بعمق.

## 8.1 المنطلقات النظرية للدراسة:

### ➤ الأمن السيبراني (Cybersecurity):

يشير الأمن السيبراني إلى مجموعة من التقنيات، العمليات، والممارسات المصممة لحماية الشبكات، الأجهزة، البرامج، والبيانات من الهجمات السيبرانية أو الوصول غير المصرح به. يهدف إلى ضمان سرية، سلامة، وتوافر المعلومات، ويتضمن عدة أبعاد رئيسية تشمل أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات (Deaver-Vazquez et al., 2024).

إجرائيا : يتم قياسه من خلال درجة تطبيق المؤسسات الخاصة في المملكة العربية السعودية للإجراءات الأمنية المتعلقة بحماية المعلومات، الشبكات، الإنترنت، والبنية التحتية الرقمية. يتم جمع البيانات باستخدام استبيانات ومقاييس كمية تقيس مدى تبني هذه المؤسسات لتقنيات الأمان السيبراني والاستراتيجيات الوقائية.

### ➤ أمن المعلومات (Information Security):

هو مجموعة من السياسات والإجراءات التي تركز على حماية البيانات من الوصول غير المصرح به، التلاعب، أو الضياع، مع الحفاظ على سريتها وسلامتها وتوافرها. يشمل أمن المعلومات تقنيات مثل التشفير، أنظمة التحكم في الوصول، وبرامج الحماية من الفيروسات (Ogborigbo et al., 2024).

إجرائيا : يتم قياسه من خلال عدد الإجراءات الأمنية المتبعة لحماية البيانات داخل المؤسسات، مثل استخدام التشفير، سياسات التحكم في الوصول، وآليات حماية البيانات الحساسة.

### ➤ أمن الشبكات (Network Security):

يشير إلى التدابير المستخدمة لحماية الشبكات الداخلية والخارجية من الاختراقات والتسلل غير المصرح به، وذلك من خلال أنظمة الجدران النارية، بروتوكولات التشفير، وأنظمة كشف التسلل. يهدف أمن الشبكات إلى تأمين الاتصال بين الأنظمة المختلفة ومنع الهجمات الضارة (Kaushik, 2024).

إجراء: يتم قياسه من خلال مدى تبني المؤسسات لأنظمة الحماية الشبكية مثل الجدران النارية، أنظمة كشف التسلل، وتأمين نقاط الاتصال الداخلية والخارجية

#### ➤ أمن الإنترنت (Internet Security):

يُعرف بأنه حماية الأنظمة المتصلة بالإنترنت من التهديدات الإلكترونية مثل الفيروسات، التصيد الاحتيالي، وهجمات البرمجيات الخبيثة. يتضمن هذا البعد استخدام تقنيات الأمان المتقدمة مثل تصفية المحتوى، برامج مكافحة الفيروسات، وأنظمة إدارة الهوية والمصادقة (Olaniyi et al., 2023).

إجراء: يتم قياسه من خلال عدد التدابير المتبعة لحماية العمليات الرقمية عبر الإنترنت، مثل برامج مكافحة الفيروسات، الحماية من التصيد الاحتيالي، والمصادقة الثنائية.

#### ➤ حماية البنية التحتية للمعلومات (Information Infrastructure Protection):

يشير إلى التدابير الأمنية المتخذة لحماية الأنظمة والموارد التقنية الأساسية التي تدعم العمليات الرقمية للمؤسسات، مثل مراكز البيانات، الخوادم، وأنظمة التخزين السحابية. يهدف هذا البعد إلى تقليل تأثير الهجمات السيبرانية على استمرارية الأعمال (الحجاية والحباشة، 2023).

إجراء: يتم قياسها من خلال مدى قدرة المؤسسات على تأمين أصولها الرقمية الأساسية مثل الخوادم، أنظمة النسخ الاحتياطي، ومراكز البيانات، باستخدام تقنيات التشفير، أنظمة التحكم في الوصول، وخطط استمرارية الأعمال.

#### ➤ إدارة مخاطر البيانات (Data Risk Management):

تُعرف إدارة مخاطر البيانات بأنها مجموعة من العمليات والسياسات التي تهدف إلى تحديد، تقييم، والتخفيف من المخاطر المرتبطة بجمع البيانات، تخزينها، نقلها، ومعالجتها. تهدف هذه العملية إلى تقليل احتمالية حدوث تسريبات أو اختراقات وضمان الامتثال للمعايير القانونية والتنظيمية (Silva, 2024).

إجراءات : يتم تقييمها بناءً على مدى قدرة الشركات على تحديد المخاطر المرتبطة بالبيانات، تصنيفها وفق درجة الخطورة، وتطبيق خطط استجابة فعالة في حال وقوع اختراقات. يشمل القياس مدى الامتثال لمعايير الأمان، إجراءات الحماية المطبقة، وعدد الحوادث الأمنية المسجلة خلال فترة الدراسة.

## 9.1 المنهجية وطرق البحث:

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، وهو منهج يستخدم لجمع وتحليل البيانات بطريقة منظمة لتفسير الظواهر ودراستها بشكل دقيق. يتميز هذا المنهج بالتركيز على وصف خصائص الظاهرة المدروسة، وتحليل العلاقات بينها وبين المتغيرات الأخرى، ومن ثم تفسير النتائج بناءً على البيانات التي تم جمعها، ويتيح هذا المنهج فهم الظواهر كما هي موجودة في الواقع دون التدخل فيها، مما يجعله مثاليًا لدراسة تأثير الأمن السيبراني على إدارة مخاطر البيانات في القطاع الخاص.

## 10.1 مصادر جمع البيانات

تعتمد هذه الدراسة على المصادر الأولية كمصدر رئيسي لجمع البيانات، حيث سيتم استخدام الاستبيان كأداة وحيدة لجمع المعلومات مباشرة من المشاركين في الدراسة. سيتم تصميم الاستبيان بطريقة منهجية تغطي جميع المتغيرات الرئيسية للدراسة، مثل أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات، وذلك بهدف قياس تأثير الأمن السيبراني على إدارة مخاطر البيانات في المؤسسات الخاصة بالمملكة العربية السعودية، وسيتم توزيع الاستبيان على عينة من العاملين في أقسام

تقنية المعلومات والأمن السيبراني داخل الشركات الخاصة، لضمان الحصول على بيانات دقيقة تعكس واقع الممارسات الأمنية في تلك المؤسسات.

أما المصادر الثانوية، فسيتم الاعتماد عليها لدعم تحليل النتائج وإثراء الإطار النظري للدراسة، حيث سيتم الرجوع إلى الدراسات السابقة، الكتب العلمية، التقارير المتخصصة، والمقالات الأكاديمية التي تتناول موضوع الأمن السيبراني وإدارة مخاطر البيانات، وستساعد هذه المصادر في توفير خلفية نظرية متينة، وتوضيح مدى توافق نتائج الدراسة الحالية مع نتائج الأبحاث السابقة، مما يساهم في تفسير النتائج المستخلصة من الاستبيان بشكل أكثر دقة وعمق.

## 11.1 أدوات الدراسة:

ستعتمد هذه الدراسة على أداة الاستبيان كأداة رئيسية لجمع البيانات الأولية من المشاركين. تم تصميم الاستبيان بطريقة علمية ومنهجية لضمان قياس دقيق لمتغيرات الدراسة، حيث يشمل مجموعة من الأسئلة التي تغطي أبعاد الأمن السيبراني الأربعة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات)، ومدى تأثيرها على إدارة مخاطر البيانات في المؤسسات الخاصة بالمملكة العربية السعودية.

وسيتم تطوير الاستبيان وفقًا لمقاييس علمية مستخدمة في الدراسات السابقة، مع مراعاة وضوح الأسئلة وسهولة الإجابة عليها لضمان جمع بيانات دقيقة وموضوعية. سيتم استخدام مقياس ليكرت الخماسي لقياس استجابات المشاركين، مما يسمح بتحليل اتجاهاتهم نحو تطبيق ممارسات الأمن السيبراني وتأثيرها على تقليل المخاطر السيبرانية.

## 12.1 الأساليب الإحصائية المستخدمة

تعتمد هذه الدراسة على مجموعة من الأساليب الإحصائية الكمية لتحليل البيانات المستخلصة من الاستبيان، وذلك باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) لضمان دقة النتائج واستخلاص استنتاجات علمية موثوقة. تشمل الأساليب الإحصائية المستخدمة ما يلي:

### الإحصاء الوصفي (Descriptive Statistics):

يتم استخدام المتوسطات الحسابية، الانحراف المعياري، والنسب المئوية لوصف خصائص العينة، وتحليل استجابات المشاركين حول دور الأمن السيبراني في إدارة مخاطر البيانات.

#### ○ اختبار الصدق والثبات (Reliability and Validity Tests):

- يتم اختبار الصدق (Validity) للتأكد من أن الاستبيان يقيس المفاهيم المستهدفة بدقة.
- يتم اختبار الثبات (Reliability) باستخدام معامل كرونباخ ألفا (Cronbach's Alpha) لقياس مدى اتساق إجابات المشاركين والتأكد من موثوقية الأداة البحثية.

#### ○ تحليل الارتباط (Correlation Analysis): يستخدم معامل ارتباط بيرسون (Pearson Correlation)

لقياس العلاقة بين أبعاد الأمن السيبراني (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) ومستوى إدارة مخاطر البيانات.

#### ○ تحليل الانحدار البسيط والمتعدد (Simple and Multiple Regression Analysis): يتم تطبيق

تحليل الانحدار البسيط لدراسة تأثير كل بعد من أبعاد الأمن السيبراني على إدارة مخاطر البيانات بشكل منفرد، ويتم استخدام تحليل الانحدار المتعدد لتحديد الأثر المجمع لجميع الأبعاد على المتغير التابع (إدارة مخاطر البيانات)، مما يساعد في فهم العوامل الأكثر تأثيراً.

### 13.1 حدود الدراسة:

← حدود موضوعية: ستركز الدراسة على دور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) في إدارة مخاطر البيانات في القطاع الخاص.

← حدود زمنية: سيتم إجراء الدراسة خلال الفترة 2024 إلى 2025 م.

← حدود مكانية: تقتصر الدراسة على المؤسسات الخاصة في المملكة العربية السعودية.

← الحدود البشرية: ستركز الدراسة على العاملين في أقسام تقنية المعلومات والأمن السيبراني داخل المؤسسات الخاصة في المملكة العربية السعودية، بما في ذلك مديرو أمن المعلومات، مسؤولو الشبكات، محللو البيانات، ومديرو المخاطر والامتثال، حيث يمتلكون الخبرة في تطبيق استراتيجيات الأمن السيبراني وإدارة مخاطر البيانات.

## الفصل الثاني: الإطار النظري

### المبحث الأول: الأمن السيبراني

#### التمهيد

يشهد العالم تطورًا رقميًا متسارعًا، حيث باتت التكنولوجيا الرقمية والبنى التحتية المعلوماتية تشكل ركيزة أساسية في أعمال المؤسسات سواء الحكومية أو الخاصة. وفي ظل هذا التحول الرقمي، أصبحت المؤسسات معرضة لمجموعة من التهديدات السيبرانية التي تستهدف بياناتها وأنظمتها التشغيلية. هذه التهديدات لم تعد محصورة في اختراقات فردية، بل تطورت لتصبح هجمات ممنهجة تستهدف زعزعة الأمن الرقمي للمؤسسات وسرقة أو إتلاف بياناتها الحيوية.

من هذا المنطلق، برز مفهوم الأمن السيبراني كعنصر حاسم في حماية الأصول المعلوماتية ومواجهة مخاطر الهجمات الإلكترونية، خاصة في القطاعات الحساسة مثل القطاع الخاص، الذي يعتمد على التكنولوجيا لتقديم الخدمات وتحقيق التنافسية.

#### 1.1.2 مفهوم الأمن السيبراني

تناول العديد من الباحثين مفهوم الأمن السيبراني من زوايا متعددة، باعتباره مجالًا مركبًا يجمع بين التقنيات الحديثة والممارسات الإدارية لحماية البيانات والأنظمة من التهديدات الإلكترونية، وقد تنوعت التعريفات بحسب الخلفية البحثية والأطر المؤسسية التي اعتمدها كل باحث، ويمكن عرض أبرزها على النحو الآتي:

عرّف المري (2023) الأمن السيبراني بأنه "مجموعة من التدابير والسياسات الفنية والتنظيمية التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات والمعلومات الحساسة من التهديدات والاختراقات التي تحدث عبر الفضاء السيبراني"، مما يعكس البعد الوقائي والردعي في ذات الوقت.

بينما قدّم الحيمودي (2023) تعريفًا يركّز على البعد التكنولوجي، حيث وصف الأمن السيبراني بأنه "نظام متكامل من البرمجيات والتقنيات والسياسات التي تهدف إلى التصدي للهجمات الإلكترونية وضمان أمن الأنظمة المعلوماتية في بيئة رقمية متغيرة".

أما الهاجري (2024) فقد تناول الأمن السيبراني من منظور الأمن الإلكتروني العام، معتبرًا إياه "جزءًا أساسيًا من المنظومة الأمنية للدولة، يهدف إلى حماية مكوناتها الرقمية من أي تهديد يمسّ سيادتها الرقمية أو البنية التحتية الحرجة".

أشار Deaver-Vazquez et al. (2024) إلى أن الأمن السيبراني هو "مجموعة من الأدوات والسياسات والإجراءات التي تُستخدم لمنع الدخول غير المصرح به إلى البيانات الرقمية، وضمان استمرارية الأعمال وسرية المعلومات وسلامتها".

و يرى Silva (2024) أن الأمن السيبراني لا يقتصر على الإجراءات التقنية فحسب، بل يشمل أيضًا "الإستراتيجيات القانونية والتنظيمية التي تضمن التزام المؤسسات بضوابط حماية البيانات والتصدي للتهديدات الرقمية وفق أطر حوكمة فعالة".

كما قدّم Kaushik (2024) تعريفًا مركبًا يدمج الجوانب التقنية والتنظيمية، حيث اعتبر الأمن السيبراني بأنه "عملية استراتيجية تهدف إلى بناء بيئة رقمية محمية وأمنة، من خلال نشر ثقافة التوعية، واعتماد الحلول التقنية، وتطبيق سياسات الوصول الآمن".

ويرى الباحث أن الأمن السيبراني يُمثل منظومة شاملة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية الأنظمة الإلكترونية والمعلومات الحيوية من التهديدات السيبرانية المتزايدة، سواء كانت داخلية أو خارجية، عشوائية أو موجهة.

## 2.2.2 أهداف الأمن السيبراني

يسعى الأمن السيبراني إلى تحقيق مجموعة من الأهداف الجوهرية التي تهدف إلى تعزيز الحماية الرقمية للمؤسسات والأفراد على حد سواء، وتُعد هذه الأهداف الركائز الأساسية التي يقوم عليها أي نظام فعال للأمن السيبراني، حيث تتكامل فيما بينها لضمان سلامة البنية التحتية المعلوماتية، وسرية البيانات، واستمرارية الأعمال. ومن أبرز هذه الأهداف:

#### 1. ضمان سرية المعلومات (Confidentiality)

يُعد الحفاظ على سرية البيانات من أبرز الأهداف التي يسعى الأمن السيبراني إلى تحقيقها، حيث يُقصد بها التأكد من أن المعلومات لا تكون متاحة أو مكشوفة إلا للأشخاص المصرح لهم بالوصول إليها، وتحقق هذه السرية من خلال استخدام تقنيات التشفير، وتحديد صلاحيات الوصول، وتطبيق نظم المصادقة. (Silva, 2024) إن اختراق سرية البيانات يمكن أن يؤدي إلى خسائر فادحة على المستويين المالي والسمعة المؤسسية، لا سيما في المؤسسات التي تتعامل مع بيانات حساسة مثل المصارف وشركات التأمين.

#### 2. ضمان سلامة البيانات (Integrity)

يعني هذا الهدف التأكد من أن البيانات محفوظة دون تعديل أو تلاعب أثناء التخزين أو النقل أو المعالجة، سواء عن قصد أو بغير قصد، ويعد الحفاظ على سلامة البيانات أمراً ضرورياً لاستقرار النظم واتخاذ قرارات دقيقة داخل المؤسسات. (Kaushik, 2024) كما يشمل ذلك توفير أدوات كشف التلاعب والتغيرات غير المصرح بها في الملفات أو قواعد البيانات.

#### 3. ضمان التوافر (Availability)

يتطلب الأمن السيبراني أيضاً ضمان توافر الأنظمة والبيانات في الوقت المناسب للمستخدمين المصرح لهم، دون انقطاع أو تأخير، ويشمل هذا البُعد الحماية من الهجمات التي تستهدف حرمان المستخدم من الخدمة) مثل هجمات حجب الخدمة (DDoS) - ، كما يستلزم بنية تحتية مرنة تسمح بالتعافي السريع من الأعطال. (Temitope & Kareem, 2023)

#### 4. التحقق من الهوية والتحكم في الوصول (Authentication & Access Control)

يهدف الأمن السيبراني إلى التأكد من هوية المستخدمين أو الأنظمة التي تحاول الدخول إلى الموارد الرقمية، من خلال آليات مثل كلمات المرور، والتوثيق متعدد العوامل، وبطاقات التعريف الرقمية (الفلاح وآخرون، 2023)، كما يشمل التحكم في الصلاحيات الممنوحة لكل مستخدم بناءً على مهامه الوظيفية.

#### 5. الاستجابة للحوادث والتعافي منها (Incident Response & Recovery)

يُعنى الأمن السيبراني بوضع خطط واضحة للتعامل مع الحوادث الأمنية عند وقوعها، بما يشمل الكشف المبكر عنها، واحتوائها، ومعالجة آثارها، واستعادة الأنظمة إلى وضعها الطبيعي، ويتطلب ذلك وجود فرق متخصصة ومُدرّبة على الاستجابة للطوارئ السيبرانية. (Neeli, 2023)

#### 6. تعزيز الوعي والتدريب الأمني

من الأهداف المستدامة للأمن السيبراني رفع مستوى وعي العاملين بالمخاطر السيبرانية، وتدريبهم على سلوكيات رقمية آمنة، مثل التعامل مع الرسائل الاحتيالية، وتحديث البرمجيات، وتخزين كلمات المرور بشكل آمن (التيماي، 2021)، فالثغرات البشرية تظل من أخطر نقاط الضعف في أي منظومة معلوماتية.

#### 7. الامتثال للمعايير والتشريعات

تهدف المنظومات السيبرانية إلى ضمان التزام المؤسسات بالقوانين المحلية والدولية الخاصة بحماية البيانات والخصوصية، مثل قوانين حماية البيانات العامة (GDPR)، ومعايير أمن المعلومات ISO/IEC 27001. ويُعد هذا الامتثال شرطاً أساسياً للعمل في الأسواق العالمية، وتفادي العقوبات. (Ogborigbo et al., 2024).

ويرى الباحث أن أهداف الأمن السيبراني لم تعد تقتصر على حماية الأنظمة من الهجمات فحسب، بل توسّعت لتشمل بناء مناعة تنظيمية ضد التهديدات الرقمية، وخلق بيئة رقمية مستدامة تُمكن من الابتكار والتوسع الرقمي الآمن.

### 3.2.2 أهمية الأمن السيبراني

تتزايد أهمية الأمن السيبراني بشكل ملحوظ في ظل الاعتماد المتنامي على التكنولوجيا الرقمية في مختلف القطاعات، حيث أصبحت البيانات والمعلومات الأصول الأهم في المنظمات الحديثة، وباتت حماية هذه الأصول أولوية قصوى تفرضها التهديدات الإلكترونية المتسارعة.

ومع ازدياد الهجمات السيبرانية تطورًا وتنظيمًا، لم يعد الأمن السيبراني خيارًا تقنيًا، بل ضرورة استراتيجية لضمان استمرارية الأعمال، وحماية الخصوصية، والامتثال للتشريعات، وتعزيز الثقة في البيئة الرقمية.

ويشير (Silva (2024 إلى أن أهمية الأمن السيبراني تنبع من كونه الركيزة الأساسية التي تضمن:

1. الحفاظ على سرية المعلومات وحمايتها من التسريب أو الوصول غير المصرح به.
  2. ضمان سلامة البيانات ومنع تعديلها أو التلاعب بها دون إذن.
  3. تحقيق استمرارية الأنظمة الرقمية، وتفادي تعطل الخدمات نتيجة الهجمات الإلكترونية.
- ويرى المري (2023) أن أهمية الأمن السيبراني لا تقتصر على حماية الأفراد والمؤسسات، بل تمتد لتشمل دعم الأمن الوطني للدول، ومواجهة التحديات المتزايدة في الفضاء الرقمي، خاصة في ظل التقدم الكبير في أدوات الهجوم السيبراني واستهداف البنى التحتية الحيوية.

ومن جهة أخرى، يؤكد (Kaushik (2024 أن الأمن السيبراني يمثل عنصرًا محوريًا في تمكين المؤسسات من التحول الرقمي الآمن، وتحقيق الميزة التنافسية، من خلال بناء بيئة تكنولوجية موثوقة تحفز على الابتكار، وتُعزز من ولاء العملاء، وتُمكّن من التوسع في الأسواق بثقة أكبر.

### 4.2.2 أبعاد الأمن السيبراني

يمثل الأمن السيبراني منظومة متكاملة تتكون من عدة أبعاد رئيسية، تتكامل فيما بينها لتوفير الحماية الشاملة للبيئة الرقمية. وقد حددت هذه الدراسة أربعة أبعاد رئيسية تشكل جوهر الأمن

السيبراني، وهي: أمن المعلومات، أمن الشبكات، أمن الإنترنت، حماية البنية التحتية للمعلومات. لكل بُعد منها وظيفة محددة تسهم في بناء استراتيجية أمنية فعّالة للمؤسسات، لا سيما في القطاع الخاص.

#### ■ أمن المعلومات

يشير أمن المعلومات إلى مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى حماية البيانات من الوصول أو الاستخدام أو الكشف أو التعديل أو الإتلاف غير المصرّح به. ويُعتبر هذا البعد هو الأساس الذي تنطلق منه جميع مكونات الأمن السيبراني. (Ogborigbo et al., 2024) ويؤكد علي وآخرون (2023) أن أمن المعلومات يعتمد على المبادئ الثلاثة الشهيرة: السرية (Confidentiality)، السلامة (Integrity)، والتوافر (Availability)، وهي ما يُعرف اختصارًا بـ CIA Triad، والتي تُعد الإطار المرجعي الأساسي في تصميم نظم حماية المعلومات.

كما يرى العبدلات والشورة (2023) أن وجود سياسات واضحة للتحكم في الوصول، ونظم تشفير فعالة، وإجراءات نسخ احتياطي دورية، يشكل أساسًا صلبًا لأمن المعلومات في المؤسسات المالية، ويسهم في التقليل من مخاطر التسرب أو الفقد.

#### ■ أمن الشبكات

يتعلق أمن الشبكات بحماية البنية التحتية للاتصالات الرقمية، بما في ذلك الخوادم، وأجهزة التوجيه (Routers)، والجدر النارية (Firewalls)، وأنظمة كشف التسلل (IDS). ويهدف هذا البعد إلى منع الدخول غير المصرّح به، والكشف المبكر عن الأنشطة الخبيثة، وتأمين نقل البيانات بين الأجهزة والمواقع المختلفة. (Kaushik, 2024)

تشير دراسة الفلاح وآخرون (2023) إلى أن أمن الشبكات يُعد من أبرز الخطوط الدفاعية ضد الهجمات الخارجية، إذ أن معظم محاولات الاختراق تبدأ من نقاط الاتصال الشبكية، مما يجعل من الضروري تحديث البنية التحتية باستمرار واستخدام أساليب متقدمة كالعزل الشبكي وتقنيات VPN.

## ■ أمن الإنترنت

يركّز هذا البُعد على حماية المستخدمين أثناء التصفح عبر الإنترنت، وضمان سلامة الاتصال بالويب، من خلال تقنيات مثل تصفية المواقع الضارة، ومنع التصيد الاحتيالي، وفحص الروابط والمرفقات قبل الوصول إليها. ويُعد أمن الإنترنت أمرًا بالغ الأهمية في ظل تزايد الهجمات التي تعتمد على الهندسة الاجتماعية لخداع المستخدمين وسرقة بياناتهم. (Silva, 2024)

كما أشار الهاجري (2024) إلى أن المؤسسات في بيئة العمل الرقمي لا بد أن تستثمر في أدوات حماية التصفح الآمن، وبرامج مكافحة البرمجيات الخبيثة، خاصة في ظل تنامي استخدام الحوسبة السحابية والعمل عن بُعد.

## ■ حماية البنية التحتية للمعلومات

يشير هذا البعد إلى حماية الأنظمة التشغيلية والخوادم ومراكز البيانات والتطبيقات الحيوية من الهجمات السيبرانية التي تستهدف البنية التحتية الرقمية ذاتها، بما في ذلك أنظمة الطاقة، والنقل، والخدمات الصحية، والمالية. وتُعد هذه الحماية ضرورية لتأمين استمرارية الأعمال ومنع الانهيار المؤسسي في حال التعرض لهجوم واسع النطاق. (Dhamani, 2023)

يرى قلاع الضروس (2022) أن حماية البنية التحتية للمعلومات تمثل اليوم أحد الأبعاد السيادية للدول، حيث إن أي اختراق لتلك البنية لا يهدد فقط المؤسسات، بل يُعرض الأمن القومي والمجتمعي للخطر، خاصة في القطاعات الاستراتيجية مثل المصارف والطيران.

## المبحث الثاني: إدارة مخاطر البيانات

### تمهيد

في ظل التحولات الرقمية الكبرى التي يشهدها القطاع الخاص، أضحت البيانات تمثل قلب العمليات التشغيلية والاستراتيجية، ومع التوسع في استخدام الحوسبة السحابية، وإنترنت الأشياء، والذكاء الاصطناعي، ازداد حجم البيانات المتداولة، وتعاظمت معها التهديدات التي قد تتعرض لها هذه البيانات من اختراق، أو فقد، أو تعديل غير مصرح به.

وهنا تبرز إدارة مخاطر البيانات كوظيفة حيوية تهدف إلى تحديد مصادر الخطر المرتبطة بالبيانات، وتحليل آثارها، ووضع السياسات والإجراءات التي تضمن الوقاية منها والتعامل معها في حال وقوعها.

وتزداد الحاجة إلى هذه الإدارة بالتوازي مع تعقيد البنية التحتية الرقمية، ما يفرض على المؤسسات تطوير منظومة متكاملة من الأدوات والإجراءات التي تُمكنها من الحفاظ على استقرار عملياتها وثقة عملائها، وضمان امتثالها للمعايير القانونية والتنظيمية.

### 1.2.2 مفهوم إدارة مخاطر البيانات

يمثل مفهوم إدارة مخاطر البيانات أحد المحاور الجوهرية في بيئة الأعمال الرقمية المعاصرة، إذ يهدف إلى حماية البيانات من المخاطر التي قد تتسبب في فقدانها، أو اختراقها، أو استخدامها بشكل غير مصرح به، سواء بفعل الأخطاء البشرية أو الأعطال التقنية أو الهجمات السيبرانية، وقد تناول الباحثون هذا المفهوم من زوايا متعددة، تؤكد جميعها على الطبيعة الاستراتيجية والتكاملية لهذه الوظيفة.

يشير Olaniyi et al. (2023) إلى أن إدارة مخاطر البيانات هي "منهجية تحليلية واستباقية تُعنى بتحديد التهديدات المرتبطة بالبيانات، وتقييم احتمالية وقوعها، وقياس أثرها على الأعمال، مع تطوير

خطط للتخفيف من تلك الآثار إلى أدنى حد ممكن، ويؤكدون على أن البيانات لم تعد مجرد مورد داعم، بل أصل مؤسسي يجب حمايته وإدارته كجزء من استراتيجية المخاطر الشاملة.

و يرى Silva (2024) أن إدارة مخاطر البيانات تُعرّف بأنها "مجموعة من العمليات التنظيمية والتقنية التي تهدف إلى تقليل احتمالية التعرض لأحداث تؤثر سلبًا على أصول البيانات الرقمية، وضمان استمرارية الأداء التشغيلي والامتثال القانوني.

كما عرّفها Mızrak (2023) بأنها "نظام متكامل لتحديد وتقييم والتحكم في المخاطر المتعلقة بالبيانات، في إطار استراتيجية إدارية أوسع تدمج بين الحوكمة التكنولوجية والرقابة التشغيلية، ويُشير إلى أن المؤسسات التي تُدرك قيمة البيانات كأصل حرج تكون أكثر التزامًا بإدارة مخاطرها بشكل مهني ومستدام. فقد قدّم زغني وحمول (2022) تعريفًا يعتمد على الممارسة الواقعية، حيث اعتبروا إدارة مخاطر البيانات "وظيفة تنظيمية تسعى إلى تعزيز الجاهزية المؤسسية ضد الأخطار التي تهدد استقرار المعلومات وجودتها وشرعيتها القانونية، من خلال أدوات التحليل الوقائي والتخطيط الاستباقي."

وتُضيف تناح (2023) أن إدارة المخاطر المرتبطة بالمعلومات تمثل في جوهرها "عملية ديناميكية تقوم على تحليل احتمالات الضرر، ووضع سيناريوهات متعددة للمواجهة، تضمن التكيف السريع في بيئة غير يقينية."

و يرى الباحث أن إدارة مخاطر البيانات تمثل إطارًا شموليًا يتجاوز التعامل التقني مع التهديدات، ليشمل أبعادًا تنظيمية، واستراتيجية، وسلوكية، تهدف إلى حماية الأصول المعلوماتية وضمان استخدامها الآمن والمشروع.

## 2.2.2 أهمية إدارة مخاطر البيانات

أصبحت إدارة مخاطر البيانات في العصر الرقمي المعاصر ضرورة ملحة للمؤسسات التي تعتمد على التكنولوجيا في إدارة عملياتها، وتخزين معلوماتها، وتقديم خدماتها، ومع تنامي حجم البيانات وتنوع مصادرها وتعقيد بنيتها، تزايدت التهديدات التي قد تؤثر على سريتها وسلامتها وتوافرها.

ومن هنا، تبرز إدارة مخاطر البيانات كأداة استراتيجية للحفاظ على استقرار المؤسسة ومرونتها التشغيلية، وضمان التزامها بالمتطلبات القانونية والتنظيمية.

يشير Olaniyi et al. (2023) إلى أن إدارة مخاطر البيانات تُعد أحد الأعمدة الرئيسية للحوكمة الرقمية، إذ تتيح للمؤسسات تقليل احتمالية التعرض للحوادث الأمنية، وتعزز من قدرتها على الاستجابة الفورية للأزمات، كما أن وجود إدارة فعالة للمخاطر يرفع من نضج البنية الرقمية للمؤسسة ويسهم في بناء بيئة بيانات آمنة تدعم اتخاذ القرار.

وفي ذات السياق، يرى Silva (2024) أن أهمية إدارة مخاطر البيانات لا تقتصر على حماية الأصول المعلوماتية فقط، بل تمتد لتشمل حماية السمعة المؤسسية، وتعزيز الثقة مع العملاء والمستفيدين، لا سيما في المؤسسات التي تتعامل مع بيانات حساسة مثل المؤسسات المالية والطبية والتجارية.

وتُضيف Zgheni & Hamoul (2022) أن الإدارة الجيدة للمخاطر تساعد على تقليل الخسائر الناتجة عن الحوادث التقنية أو الاختراقات، وتُجنب المؤسسة التعرض للغرامات والعقوبات التي قد تُفرض نتيجة لخرق التشريعات الخاصة بحماية البيانات مثل اللائحة العامة لحماية البيانات (GDPR) أو أنظمة أمن المعلومات ISO/IEC 27001.

كما يشير Mızrak (2023) إلى أن أهمية إدارة مخاطر البيانات تزايدت في ظل الاعتماد المتنامي على الحوسبة السحابية والذكاء الاصطناعي، حيث تصبح البيانات أكثر عرضة للمخاطر العابرة للحدود، مما يتطلب إطارًا تنظيميًا قادرًا على التعامل مع تهديدات معقدة ومتغيرة باستمرار.

يرى الباحث أن إدارة مخاطر البيانات لم تعد وظيفة تقنية منعزلة ضمن أقسام تكنولوجيا المعلومات، بل أصبحت محورًا استراتيجيًا تتقاطع معه وظائف الامتثال، والتخطيط، وحوكمة البيانات، والاتصال المؤسسي، وتكمن أهميتها في كونها تُبني المؤسسة لتبني التحول الرقمي الآمن، وتُعزز من مرونتها في مواجهة الأزمات، وتمنحها ميزة تنافسية مستدامة في سوق يتسم بالتقلبات والاضطرابات. كما أن اعتماد نهج استباقي ومتكامل في إدارة مخاطر البيانات هو ما يميز المؤسسات الناجحة رقميًا عن غيرها.

### 3.2.2 أهداف إدارة مخاطر البيانات

تهدف إدارة مخاطر البيانات إلى بناء إطار تنظيمي واستراتيجي يُمكن المؤسسات من التنبؤ بالمخاطر التي تهدد أصولها المعلوماتية، والاستعداد لها، والتعامل معها بفعالية عند وقوعها، وتتمثل هذه الأهداف في ضمان سلامة البيانات واستمراريتها، وتكامل العمليات، وحماية المؤسسة من التبعات القانونية والمالية المترتبة على أي خرق أمني أو سوء استخدام للمعلومات.

ومن أبرز أهداف إدارة مخاطر البيانات ما يلي:

#### ❖ حماية سرية البيانات وسلامتها وتوافرها

تسعى المؤسسات من خلال إدارة المخاطر إلى حماية البيانات من التلاعب، أو الضياع، أو الوصول غير المصرح به، بما يحفظ خصوصية المستخدمين، ويعزز الثقة بالخدمات الرقمية، وتُعد هذه الأهداف الثلاثة (السرية – السلامة – التوافر) من المبادئ الجوهرية التي تنبثق عنها معظم الممارسات الأمنية (Silva, 2024).

#### ❖ تحقيق الامتثال للمتطلبات القانونية والتنظيمية

تهدف إدارة مخاطر البيانات إلى ضمان التزام المؤسسة بالقوانين الوطنية والدولية مثل اللائحة العامة لحماية البيانات (GDPR)، وقوانين خصوصية البيانات المحلية، والمعايير الدولية مثل ISO/IEC

27005 الخاصة بإدارة مخاطر أمن المعلومات. (Mizrak, 2023) ويساعد ذلك في تجنب الغرامات والعقوبات المحتملة الناتجة عن أي اختراق أو تقصير تنظيمي.

#### ❖ تحسين اتخاذ القرار المبني على بيانات آمنة وموثوقة

عندما تكون البيانات محمية وآمنة، فإنها تُشكّل أساسًا قويًا لاتخاذ قرارات سليمة واستراتيجية في الوقت المناسب، فالإدارة الفعالة للمخاطر تُسهم في توفير بيانات عالية الجودة، خالية من التزوير أو الفقد أو الغموض، مما يدعم مسارات النمو والتطوير داخل المؤسسة. (Olaniyi et al., 2023)

#### ❖ تقليل التكاليف الناتجة عن الحوادث السيبرانية

من خلال استباق التهديدات وتحليلها ووضع خطط التعامل معها، يمكن تقليل الخسائر المالية الناجمة عن الحوادث، بما يشمل توقف الأنظمة، وسرقة البيانات، والتقاضى، والتعويضات (Zgheni & Hamoul, 2022) وتُعد الوقاية دائمًا أقل كلفة من المعالجة بعد وقوع الضرر.

#### ❖ رفع الجاهزية المؤسسية في مواجهة الأزمات الرقمية

تهدف إدارة مخاطر البيانات إلى تعزيز قدرة المؤسسة على الصمود أمام الأزمات الطارئة، من خلال إعداد خطط للطوارئ، وتمارين استجابة، وتحديثات دورية للسياسات الأمنية، مما يمنحها مرونة استراتيجية واستعدادًا دائمًا للتفاعل مع التغيرات التكنولوجية والتهديدات الجديدة. (Neeli, 2023)

ويرى الباحث أن أهداف إدارة مخاطر البيانات لا تقتصر على تقليل احتمالات التعرض للمخاطر، بل تتجاوز ذلك نحو بناء ثقافة مؤسسية قائمة على الوقاية، والمسؤولية، والاستباقية في التعامل مع البيانات، كما أن هذه الأهداف ترتبط بشكل مباشر برؤية المؤسسة الرقمية الشاملة، فكلما كانت أهداف إدارة المخاطر واضحة ومفعلة، زادت قدرة المؤسسة على الاستفادة من إمكانيات التكنولوجيا دون التعرّض للضرر.

## 4.2.2 مراحل إدارة مخاطر البيانات

تُعد إدارة مخاطر البيانات عملية منهجية تتكون من مراحل مترابطة تُنفذ بشكل متسلسل أو دوري، وتهدف إلى ضمان التقييم الشامل والتعامل الفعال مع المخاطر التي قد تهدد أصول البيانات داخل المؤسسة، وتعتمد هذه المراحل على المعايير الدولية مثل ISO/IEC 27005، وتتمحور حول خمس خطوات رئيسية: التحديد، التقييم، التحليل، المعالجة، والمتابعة.

### ✓ تحديد المخاطر (Risk Identification)

تبدأ إدارة المخاطر بتحديد مصادر الخطر المحتملة التي قد تؤثر على البيانات، سواء أكانت داخلية (كأخطاء بشرية أو ضعف في السياسات) أو خارجية (كالهجمات السيبرانية أو الكوارث الطبيعية)، ويشمل ذلك تحديد أنواع البيانات الحساسة، وتحديد الأماكن التي تُخزّن أو تمر من خلالها، وتحديد الأطراف المتعاملة معها. (Mizrak, 2023)

يشير Silva (2024) إلى أن مرحلة التحديد تمثل الأساس لبناء خطة فعّالة، إذ أن الإخفاق في تحديد جميع المخاطر المحتملة قد يؤدي إلى ضعف شامل في نظام الحماية.

### ✓ تقييم المخاطر (Risk Assessment)

بعد تحديد المخاطر، يتم تقييمها من حيث احتمالية حدوثها وشدة أثرها. يُستخدم في ذلك مصفوفات التقييم الكمي أو النوعي، لتحديد درجة الخطورة وترتيب أولويات المعالجة، ويساعد هذا التقييم في تخصيص الموارد بشكل عقلاني وتوجيه الجهود إلى التهديدات الأكثر إلحاحًا. (Olaniyi et al., 2023).

### ✓ تحليل المخاطر (Risk Analysis)

تُركز هذه المرحلة على فهم الأسباب الجذرية للمخاطر، والعلاقات المحتملة بينها، وكيفية تطورها أو تفاقمها عبر الزمن، كما تشمل تحليل نقاط الضعف في النظم التقنية والبشرية، وتحديد مدى تأثير

العمليات الحيوية بها، ويهدف التحليل إلى توفير معلومات عميقة تساعد في اختيار أنسب الاستراتيجيات للتعامل مع الخطر. (Zgheni & Hamoul, 2022)

### ✓ معالجة المخاطر (Risk Treatment)

تشمل هذه المرحلة اتخاذ القرار المناسب بشأن كل خطر محدد، من خلال واحدة أو أكثر من الخيارات التالية: القبول، أو التخفيف، أو التحويل (مثل التأمين)، أو الإزالة الكاملة للخطر، ويتم تصميم وتنفيذ الضوابط الأمنية المناسبة مثل التشفير، ومراقبة الوصول، والتدريب، والتحديثات الدورية للأنظمة. (Temitope & Kareem, 2023)

## ✓ مراقبة ومراجعة المخاطر (Monitoring & Review)

تُعتبر هذه المرحلة مستمرة، وتتمثل في متابعة فعالية الإجراءات المطبقة، ومراقبة ظهور مخاطر جديدة، وتقييم الأداء الأمني بشكل دوري، كما تتضمن مراجعة السياسات وتحديثها بما يتوافق مع تغير البيئة الرقمية والتشريعات والمهددات التقنية. (Neeli, 2023)

يؤكد Kaushik (2024) أن المؤسسات الرائدة لا تكتفي بالتحكم في المخاطر، بل تطور آليات للرصد الاستباقي، وتستفيد من الذكاء الاصطناعي في كشف المؤشرات المبكرة للهجمات أو الاختراقات.

ويرى الباحث أن اتباع هذه المراحل الخمس يُمثل المنهجية العلمية المثلى لإدارة مخاطر البيانات، إذ يوفر إطارًا متكاملًا يُمكن المؤسسات من التعامل مع المخاطر بكفاءة ومرونة، كما أن هذه المراحل ليست منفصلة، بل يُعاد تفعيلها باستمرار ضمن دورة حياة إدارة المخاطر، ما يضمن استجابة ديناميكية للمهددات المتغيرة..

## الفصل الثالث: الطريقة والإجراءات

### 1.3 تمهيد

يعرض الفصل الحالي الأساليب العلمية التي تستند عليها الدراسة الحالية لتحقيق أهدافها والإجابة على تساؤلات مشكلة الدراسة، حيث يتناول هذا الفصل منهجية الدراسة، مجتمع وعينة الدراسة، ومن ثم الأساليب العلمية لجمع البيانات وأداة الدراسة، وصدق أداة الدراسة بالإضافة إلى الأساليب المعالجة الإحصائية التي تعتمد عليها الدراسة.

### 2.3 منهجية الدراسة

اعتمدت هذه الدراسة على المنهج الوصفي التحليلي، بوصفه المنهج الأنسب لتحليل العلاقة بين متغيرين أساسيين: الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، حماية البنية التحتية للمعلومات) كمتغير مستقل، وإدارة مخاطر البيانات كمتغير تابع. يركز المنهج الوصفي التحليلي على دراسة الظاهرة كما هي موجودة في الواقع، ومن ثم تحليل بياناتها كما تظهر في الميدان بهدف تفسير طبيعة العلاقة بين المتغيرات، وفهم الاتجاهات والأنماط التي تفسّر تفاعلها، واستخلاص النتائج بناءً على أدلة كمية أو كيفية.

### 3.3 مجتمع وعينة الدراسة :

يتكوّن مجتمع الدراسة من جميع العاملين في إدارات الأمن السيبراني، وتقنية المعلومات، وإدارة المخاطر في مؤسسات القطاع الخاص بالمملكة العربية السعودية، وذلك نظراً لارتباط هذه الفئة بشكل مباشر بطبيعة موضوع الدراسة، إذ تمثل نقطة الالتقاء بين الإجراءات التقنية والقرارات الإدارية المتعلقة بحماية البيانات وتحليل أخطارها، كما تُعد هذه الإدارات من الجهات الأكثر تفاعلاً مع أنظمة الأمن السيبراني وتطبيقاته اليومية، وهي المسؤولة عن تنفيذ سياسات حماية المعلومات واستراتيجيات تقليل المخاطر الرقمية.

وبالاستناد إلى البيانات المنشورة من وزارة الموارد البشرية وتقارير التحول الرقمي والحوكمة السيبرانية لعام 2023، يُقدّر عدد العاملين في هذه الإدارات لدى مؤسسات القطاع الخاص في المملكة بأكثر من 7000 موظف، موزعين على قطاعات متعددة مثل: البنوك، والاتصالات، والرعاية الصحية، وشركات التقنية، والخدمات اللوجستية.

ونظرًا لكبر حجم المجتمع وتوزعه على قطاعات مختلفة، فقد تم استخدام أسلوب العينة العشوائية الطبقية، وذلك لضمان تمثيل نسبي لكافة القطاعات المستهدفة، وتم تقسيم المجتمع إلى طبقات وفقًا للقطاع (مالي - صحي - تقني - خدمي)، وكذلك وفقًا للإدارة (أمن سيبراني - تقنية معلومات - إدارة مخاطر).

ولتحديد الحجم المناسب للعينة، تم اعتماد معادلة كرجسي ومورغان (Krejcie & Morgan, 1970)، بناءً على مستوى ثقة قدره 95%، وهامش خطأ لا يتجاوز  $\pm 5\%$ ، وتم توزيع 400 استبانة على العاملين في الإدارات المستهدفة، في عدد من المدن الرئيسية التي تمثل التوزيع الجغرافي للمؤسسات الخاصة في المملكة، وهي: الرياض، جدة، الدمام، المدينة المنورة، وأبها، وبعد جمع البيانات وفرزها، تم استبعاد الاستبانات غير المكتملة أو التي احتوت على أخطاء منطقية، وبلغ عدد الاستبانات الصالحة للتحليل النهائي 361 استبانة، تمثل العينة المعتمدة للدراسة.

### 4.3 مصادر جمع البيانات

اعتمدت هذه الدراسة على مصدرين رئيسيين لجمع البيانات اللازمة لتحقيق أهدافها المتمثلة في تحليل أثر الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، حماية البنية التحتية للمعلومات) على إدارة مخاطر البيانات في مؤسسات القطاع الخاص بالمملكة العربية السعودية.

- المصدر الأول تمثل في المصادر الثانوية، والتي اشتملت على مراجعة شاملة للأدبيات النظرية ذات العلاقة بمحوري الدراسة، بما في ذلك مفاهيم الأمن السيبراني، استراتيجيات حماية المعلومات، أسس إدارة مخاطر البيانات، ونماذج الحوكمة الرقمية. كما تم الرجوع إلى عدد من الدراسات

الأكاديمية المنشورة في المجالات المحكمة، إضافة إلى تقارير رسمية صادرة عن مؤسسات وطنية ودولية، مثل الهيئة الوطنية للأمن السيبراني، ومؤسسة النقد العربي السعودي (ساما)، وتقارير المخاطر الصادرة عن قطاعات حيوية في القطاع الخاص.

■ أما المصدر الثاني فتمثل في المصادر الأولية، من خلال تطوير استبانة ميدانية صُممت لقياس درجة تطبيق ممارسات الأمن السيبراني، وفعالية إدارة مخاطر البيانات، من وجهة نظر العاملين في الإدارات المعنية بالأمن الرقمي والمخاطر في مؤسسات القطاع الخاص. وقد تم بناء هذه الاستبانة بالاستناد إلى عدد من الدراسات التطبيقية السابقة مثل دراسة Isenberg et al (2022)، وجعفر وبدرني (2022)، والعمرى وكتبونة (2022)، مع إجراء التعديلات اللازمة لتكييفها مع السياق السعودي.

### 5.3 أداة الدراسة :

تم اعتماد الاستبانة كأداة رئيسية لجمع البيانات الميدانية في هذه الدراسة، نظرًا لما توفره من قدرة على قياس متغيرات متعددة بصورة كمية ومنظمة، وقد صُممت الاستبانة بهدف قياس أبعاد المتغير المستقل (الأمن السيبراني بأبعاده الأربعة: أمن المعلومات، أمن الشبكات، أمن الإنترنت، حماية البنية التحتية للمعلومات)، والمتغير التابع (إدارة مخاطر البيانات)، وذلك بالاعتماد على مقياس ليكرت الخماسي، الذي يمنح للمبحوثين إمكانية التعبير عن درجة موافقتهم على العبارات ضمن خمس مستويات، تبدأ من: (1) لا أوافق بشدة، حتى (5) أوافق بشدة.

وقد اشتملت الاستبانة على 30 فقرة، موزعة على النحو التالي:

الجدول (1): مقياس ليكرت الخماسي

| نوع المتغير     | البعد / المحور | عدد الفقرات | أرقام الفقرات |
|-----------------|----------------|-------------|---------------|
| المتغير المستقل | أمن المعلومات  | 5           | 1 – 5         |
|                 | أمن الشبكات    | 5           | 6 – 10        |

| نوع المتغير    | البُعد / المحور                | عدد الفقرات | أرقام الفقرات |
|----------------|--------------------------------|-------------|---------------|
| المتغير التابع | أمن الإنترنت                   | 5           | 11 – 15       |
|                | حماية البنية التحتية للمعلومات | 5           | 16 – 20       |
|                | إدارة مخاطر البيانات           | 10          | 21 – 30       |
| الإجمالي       |                                | 30فقرة      |               |

ولتحليل استجابات المشاركين، تم تصنيف درجات ليكرت إلى خمس فئات لقياس مستوى الموافقة، بحيث يكون المتوسط الحسابي المرجعي كالتالي:

#### الجدول (2) تصنيف ليكرت

| المتوسط الحسابي         | درجة الموافقة |
|-------------------------|---------------|
| من 1.00 إلى أقل من 1.80 | لا أوافق بشدة |
| من 1.80 إلى أقل من 2.60 | لا أوافق      |
| من 2.60 إلى أقل من 3.40 | محايد         |
| من 3.40 إلى أقل من 4.20 | أوافق         |
| من 4.20 إلى 5.00        | أوافق بشدة    |

#### 6.3 صدق أداة الدراسة :

يُقصد بصدق أداة الدراسة مدى قدرة الأداة المستخدمة (الاستبانة) على قياس متغيرات الدراسة بدقة وموضوعية، وانسجام فقراتها مع الأبعاد النظرية التي تنتمي إليها، وللتحقق من صدق الاستبانة، تم الاعتماد في هذه الدراسة على أسلوبين رئيسيين هما: الصدق الظاهري والصدق الداخلي البنائي.

## أولاً: الصدق الظاهري (Face Validity)

تم التأكد من الصدق الظاهري للاستبانة من خلال عرضها على لجنة من المحكمين المتخصصين في مجالات الإدارة المصرفية، والأمن السيبراني، وإدارة المخاطر، والإحصاء التربوي، والبحث العلمي. وقد تألفت اللجنة من ثلاثة محكمين أكاديميين من جامعات سعودية، إلى جانب خبيرين مهنيين من القطاع المصرفي السعودي.

تم تزويد المحكمين بنسخة من الاستبانة مرفقة بشرح مفصل عن أهداف الدراسة، ومحاورها، ومتغيراتها، وتم الطلب منهم تقييم مدى:

- وضوح الفقرات وسلامة صياغتها،
  - مدى ملاءمتها لقياس الأبعاد المعنية بالدراسة،
  - شمولية الأداة وترابط محاورها.
- وبناءً على ملاحظاتهم التخصصية، أُجريت عدة تعديلات نوعية، تمثلت في:
- تحسين صياغة عدد من الفقرات لتكون أكثر وضوحاً وسهولة في الفهم،
  - إعادة ترتيب بعض المحاور وفق تسلسل منسجم مع السياق الإجرائي داخل المؤسسات،
  - حذف بعض العبارات المتكررة دون الإخلال بالمحتوى النظري.

وقد أجمعت اللجنة على أن الاستبانة تحقق درجة مقبولة من الصدق الظاهري، وتُعد ملائمة لقياس المتغيرات المستهدفة بدقة ووضوح.

## ثانياً: الصدق الداخلي (Internal Validity)

للتحقق من الصدق الداخلي البنائي للاستبانة، تم احتساب معاملات الارتباط البسيط لبيرسون (Pearson Correlation Coefficient) بين كل فقرة من فقرات الاستبانة والمحور الذي تنتهي إليه،

باستخدام برنامج SPSS الإصدار (26)، ويُعبّر هذا الأسلوب عن مدى اتساق الفقرات الداخلية لكل محور، ومدى تعبير كل فقرة عن البعد الذي تقيسه.

وقد أظهرت النتائج وجود معاملات ارتباط موجبة ودالة إحصائيًا عند مستوى (0.01) بين جميع الفقرات والمحاور النظرية التي تنتمي إليها، مما يعكس قوة الترابط البنائي والاتساق الداخلي داخل الأداة. ويُبيّن الجدول التالي علاقات الارتباط بين أبعاد المتغير المستقل (الأمن السيبراني):

**الجدول (3) علاقات الارتباط بين أبعاد المتغير المستقل (الأمن السيبراني)**

| الأبعاد                        | أمن المعلومات | أمن الشبكات | أمن الإنترنت | حماية البنية التحتية |
|--------------------------------|---------------|-------------|--------------|----------------------|
| أمن المعلومات                  | 1.000         |             |              |                      |
| أمن الشبكات                    | 0.712**       | 1.000       |              |                      |
| أمن الإنترنت                   | 0.689**       | 0.703**     | 1.000        |                      |
| حماية البنية التحتية للمعلومات | 0.653**       | 0.691**     | 0.698**      | 1.000                |

جميع القيم دالة إحصائيًا عند مستوى (0.01).

يتّضح من الجدول أعلاه وجود علاقات ارتباط طردية قوية بين مختلف أبعاد الأمن السيبراني، مما يُعزز من الصديق البنائي لأداة الدراسة، وقد كانت أعلى العلاقات بين أمن المعلومات وأمن الشبكات (0.712)، تليها العلاقة بين أمن الإنترنت وأمن الشبكات (0.703)، بينما جاءت أضعف علاقة نسبيًا بين أمن المعلومات وحماية البنية التحتية (0.653)، وهي رغم انخفاضها النسبي إلا أنها لا تزال ضمن مستوى دلالة مرتفع، ما يدل على التكامل البنوي لأبعاد الأداة.

### 7.3 ثبات أداة الدراسة:

يُعد التحقق من ثبات أداة الدراسة أحد الشروط الأساسية لضمان موثوقية نتائج القياس، إذ يُعبّر عن مدى اتساق فقرات الاستبانة واستقرارها في قياس المفاهيم المستهدفة عند إعادة استخدامها في بيانات مشابهة، ويُعد الثبات مؤشراً جوهرياً يُساعد في الحكم على جودة الأداء الداخلي للأداة، وقدرتها على إعطاء نتائج موثوقة.

وفي هذه الدراسة، تم الاعتماد على معامل الاتساق الداخلي "كرونباخ ألفا (Cronbach's Alpha)" بوصفه من أكثر الأساليب استخداماً لقياس الثبات في الدراسات الكمية، حيث يوفر تقديرًا لدرجة تجانس الفقرات ضمن كل محور من محاور الاستبانة.

وبحسب ما أشار إليه (Sekaran & Bougie (2020)، فإن القيم المقبولة لمعامل "ألفا" يجب ألا تقل عن (0.70)، وتُعد القيم بين (0.80 – 0.90) مؤشراً على ثبات جيد جداً، بينما القيم التي تتجاوز (0.90) تدل على موثوقية مرتفعة للغاية.

وقد جاءت نتائج حساب معامل "كرونباخ ألفا" في هذه الدراسة كما يلي:

الجدول (4): نتائج حساب معامل "كرونباخ ألفا"

| المحور                                | عدد الفقرات | معامل كرونباخ ألفا |
|---------------------------------------|-------------|--------------------|
| أمن المعلومات                         | 4           | 0.762              |
| أمن الشبكات                           | 4           | 0.785              |
| أمن الإنترنت                          | 4           | 0.741              |
| حماية البنية التحتية للمعلومات        | 4           | 0.773              |
| إدارة مخاطر البيانات (المتغير التابع) | 10          | 0.868              |
| الدرجة الكلية للاستبانة               | 26          | 0.917              |

تشير النتائج الموضحة في الجدول إلى أن جميع أبعاد الاستبانة تجاوزت الحد الأدنى المقبول لمعامل الثبات (0.70)، حيث تراوحت القيم بين (0.741) و(0.868)، مما يعكس اتساقاً داخلياً جيداً في كل محور،

ويُلاحظ أن أعلى ثبات تحقق في بُعد "إدارة مخاطر البيانات" (0.868)، وهو ما يدل على قدرة الفقرات على تمثيل هذا البُعد بدقة وموضوعية.

أما بالنسبة إلى المعامل الكلي للاستبانة، فقد بلغ (0.917)، وهو ما يُعد مؤشرًا قويًا على الثبات العام للأداة وموثوقيتها العالية، ويُعزز من إمكانية الاعتماد على الاستبانة في اختبار فرضيات الدراسة وتحليل نتائجها بثقة علمية عالية.

### 8.3 الأساليب الإحصائية

بعد الانتهاء من جمع البيانات الميدانية، تم إدخالها إلى برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) الإصدار 26، وتحليلها باستخدام مجموعة من الأساليب الإحصائية الوصفية والاستدلالية المناسبة لطبيعة أهداف الدراسة وفرضياتها.

#### أولاً: الأساليب الإحصائية الوصفية

تم استخدام مجموعة من المؤشرات الوصفية لتحليل استجابات أفراد العينة، وبيان اتجاهاتهم نحو كل بُعد من أبعاد الدراسة، وقد شملت ما يلي:

- التكرارات والنسب المئوية: لوصف الخصائص الديموغرافية لعينة الدراسة.
- المتوسطات الحسابية: لقياس درجة الموافقة على كل فقرة من فقرات الاستبانة.
- الانحرافات المعيارية: لقياس مدى تباين استجابات أفراد العينة عن المتوسط العام.
- ترتيب الأبعاد: وفقاً للمتوسطات الحسابية لمعرفة أكثر الأبعاد تأثيراً من وجهة نظر المبحوثين.

#### ثانياً: الأساليب الإحصائية الاستدلالية

تم استخدام مجموعة من الأساليب الإحصائية الاستدلالية لاختبار فرضيات الدراسة وتحليل العلاقة بين المتغيرات، على النحو الآتي:

- معامل ارتباط بيرسون (Pearson Correlation) لدراسة قوة واتجاه العلاقة بين المتغيرات المستقلة والتابعة.
- تحليل الانحدار الخطي المتعدد (Multiple Linear Regression) لقياس مدى تأثير أبعاد الأمن السيبراني مجتمعة على إدارة مخاطر البيانات.
- اختبارات الصدق والثبات: والتي شملت معامل كرونباخ ألفا للثبات، ومعاملات الارتباط للتحقق من الصدق الداخلي.

## الفصل الرابع تحليل البيانات واختبار الفرضيات

### تمهيد

يتناول هذا الفصل تحليل بيانات الدراسة الميدانية، حيث يهدف إلى عرض نتائج التحليلات الإحصائية التي تم تطبيقها باستخدام برنامج SPSS، وذلك للإجابة على تساؤلات الدراسة واختبار فرضياتها. وقد تم تقسيم التحليل إلى قسمين: الأول يعرض التحليل الوصفي للبيانات، من خلال المتوسطات والانحرافات المعيارية والتكرارات والنسب المئوية لوصف خصائص العينة، ومستوى استجاباتهم على أبعاد الدراسة، أما القسم الثاني، فيتناول الاختبارات التحليلية المناسبة لاختبار الفرضيات، مثل الانحدار الخطي البسيط والمتعدد، وتحليل معاملات الارتباط، وغيرها.

### 1.4 نتائج البيانات الديمغرافية

#### أولاً: وصف عينة الدراسة:

هدف هذه الفقرة إلى عرض الخصائص الديموغرافية لأفراد العينة الذين شاركوا في الدراسة وعددهم (ن=361)، وذلك لفهم تركيبة العينة من حيث النوع الاجتماعي، بما يساهم في تفسير أنماط الاستجابة، وتقييم مدى توازن التمثيل بين الفئات المختلفة. وقد تم تقسيم المشاركين بحسب الجنس إلى فئتين: (ذكور – إناث)، كما هو موضح في الجدول: (4)

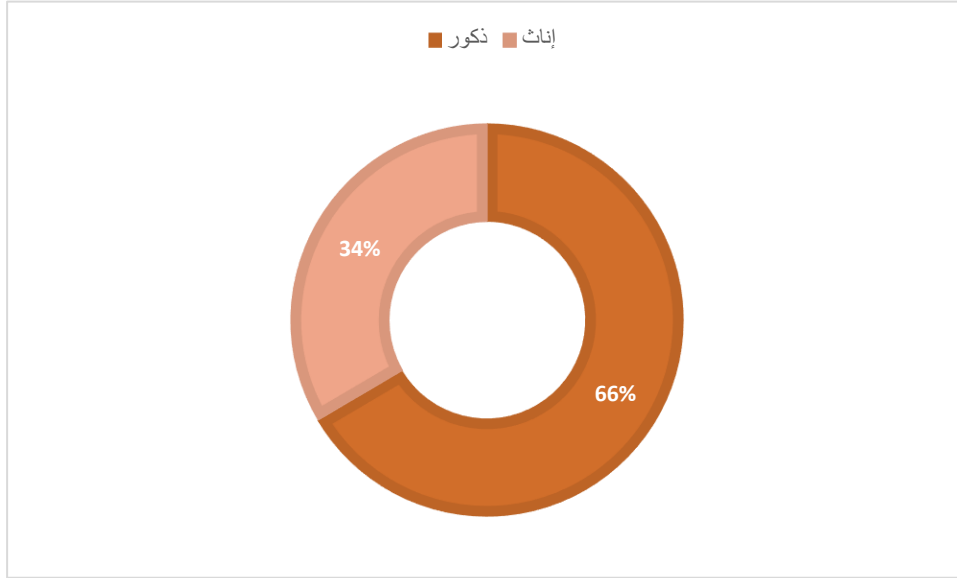
#### ➤ الجنس

الجدول (5): توزيع عينة الدراسة حسب الخصائص الديموغرافية (ن=361)

| المتغير الديموغرافي | الفئة | الذكور | الإناث | الإجمالي | (%) النسبة |
|---------------------|-------|--------|--------|----------|------------|
| الجنس               | ذكور  | 240    | —      | 240      | 66.5%      |
|                     | إناث  | —      | 121    | 121      | 33.5%      |

| المتغير الديموغرافي | الفئة | الذكور | الإناث | الإجمالي | (%) النسبة |
|---------------------|-------|--------|--------|----------|------------|
| الإجمالي            |       | 240    | 121    | 361      | 100%       |

الشكل (1): توزيع عينة الدراسة حسب الخصائص الديموغرافية (ن=361)



يعرض الجدول (5) توزيع المشاركين في الدراسة بناءً على متغير الجنس، وقد تبين أن عدد الذكور بلغ (240) مشاركاً (بنسبة 66.5% من إجمالي العينة، في حين بلغ عدد الإناث 121) مشاركة (بنسبة 33.5% وتشير هذه النتائج إلى أن الذكور يشكلون النسبة الأكبر من أفراد العينة، وهو ما قد يُعزى إلى طبيعة الوظائف الفنية والإدارية في مجالات الأمن السيبراني وتقنية المعلومات وإدارة المخاطر، حيث لا تزال نسبة تمثيل الذكور أعلى في معظم مؤسسات القطاع الخاص السعودي، لا سيما في المناصب المتعلقة بالأمن الرقمي والتحليل السيبراني..

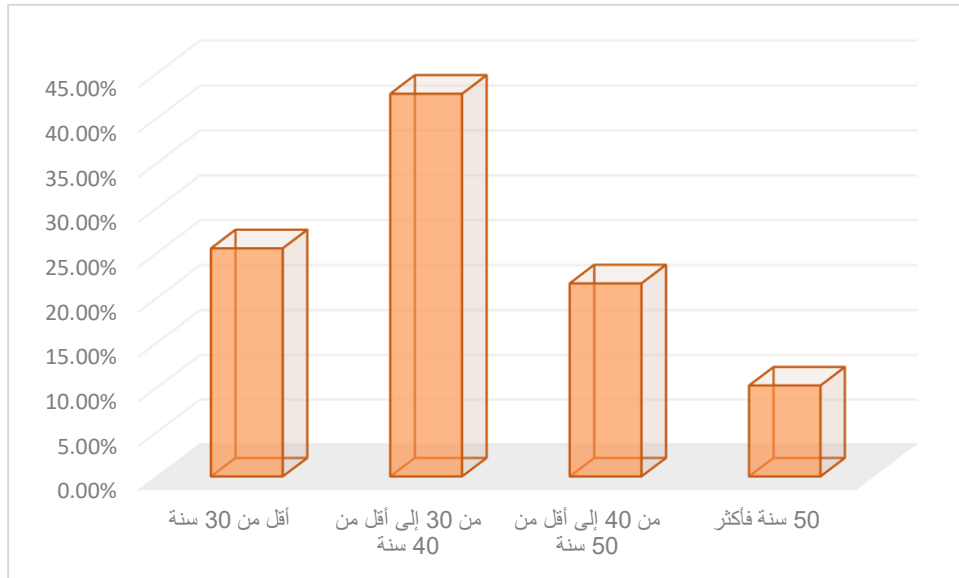
### ➤ الفئة العمرية

الجدول (6): توزيع عينة الدراسة حسب الفئة العمرية (ن = 361)

| الفئة العمرية           | عدد المشاركين | النسبة (%) |
|-------------------------|---------------|------------|
| أقل من 30 سنة           | 92            | 25.5%      |
| من 30 إلى أقل من 40 سنة | 154           | 42.7%      |

|       |     |                         |
|-------|-----|-------------------------|
| 21.6% | 78  | من 40 إلى أقل من 50 سنة |
| 10.2% | 37  | 50 سنة فأكثر            |
| 100%  | 361 | الإجمالي                |

الشكل (2): توزيع عينة الدراسة حسب الفئة العمرية (ن = 361)



يتضح من الجدول أن غالبية المشاركين يتركزون في الفئة العمرية (من 30 إلى أقل من 40 سنة) بنسبة 42.7%، يليها فئة أقل من 30 سنة (25.5%)، ثم فئة من 40 إلى أقل من 50 سنة (21.6%)، وأخيراً فئة 50 سنة فأكثر (10.2%)، ويُشير هذا التوزيع إلى أن أكثر من ثلثي العينة هم من الفئات العمرية النشطة مهنيًا، والتي تجمع بين الخبرة المتراكمة والكفاءة التشغيلية العالية

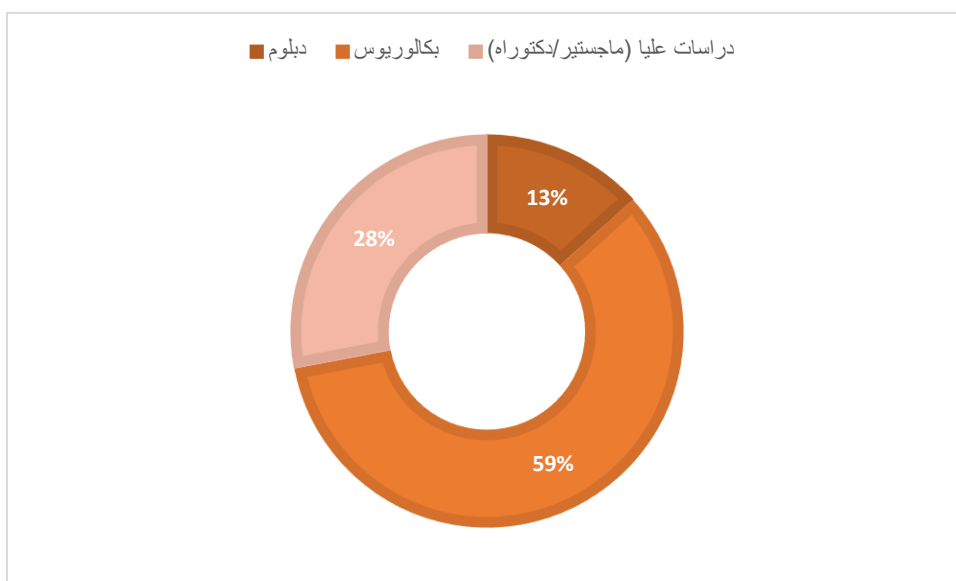
## ➤ المؤهل العلمي

الجدول (7): توزيع عينة الدراسة حسب المؤهل العلمي (ن = 361)

| المؤهل العلمي                 | عدد المشاركين | النسبة (%) |
|-------------------------------|---------------|------------|
| دبلوم                         | 48            | 13.3%      |
| بكالوريوس                     | 212           | 58.7%      |
| دراسات عليا (ماجستير/دكتوراه) | 101           | 28.0%      |

|      |     |          |
|------|-----|----------|
| 100% | 361 | الإجمالي |
|------|-----|----------|

الشكل (3): توزيع عينة الدراسة حسب المؤهل العلمي (ن = 361)



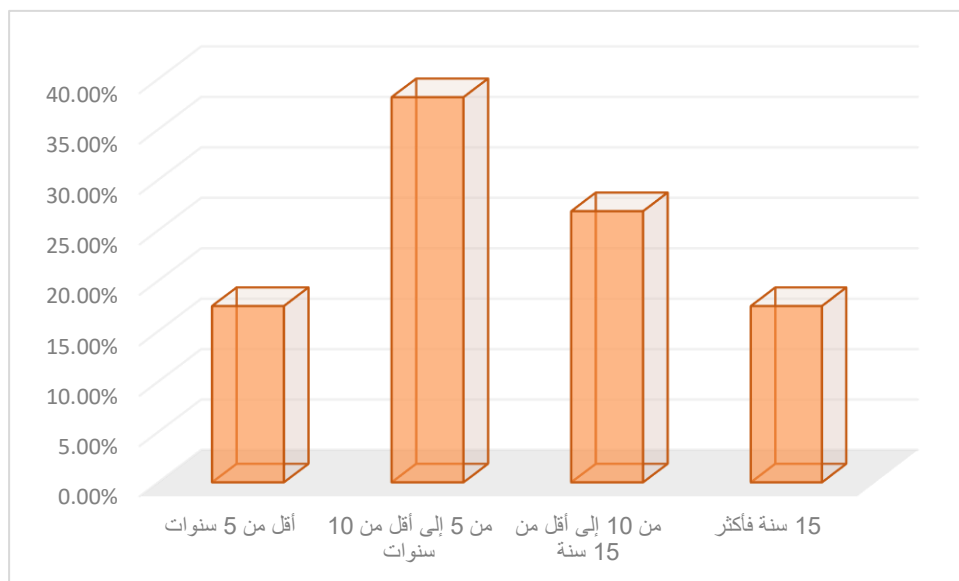
أظهر الجدول أن النسبة الأكبر من المشاركين يحملون درجة البكالوريوس (58.7%) ، تليها فئة حملة الدراسات العليا (28%) ، ثم حملة الدبلوم (13.3%) ، ويمثل هذا التوزيع مؤشراً على أن أغلب العينة تتمتع بمستوى علمي مناسب لموضوع الدراسة، خصوصاً أن موضوعات مثل الأمن السيبراني وإدارة البيانات تتطلب معرفة تقنية ومهارية متقدمة .

#### ➤ سنوات الخبرة

الجدول (8): توزيع العينة حسب سنوات الخبرة (ن = 361)

| سنوات الخبرة             | عدد المشاركين | (%) النسبة |
|--------------------------|---------------|------------|
| أقل من 5 سنوات           | 63            | 17.5%      |
| من 5 إلى أقل من 10 سنوات | 138           | 38.2%      |
| من 10 إلى أقل من 15 سنة  | 97            | 26.9%      |
| سنة فأكثر 15             | 63            | 17.5%      |
| الإجمالي                 | 361           | 100%       |

الشكل (4): توزيع العينة حسب سنوات الخبرة (ن = 361)



تُظهر النتائج أن الفئة الأكبر من المشاركين تقع ضمن نطاق من 5 إلى أقل من 10 سنوات خبرة (38.2%)، تليها فئة من 10 إلى أقل من 15 سنة (26.9%)، ثم فئة أقل من 5 سنوات و 15 سنة فأكثر بنسبة متساوية (17.5%).

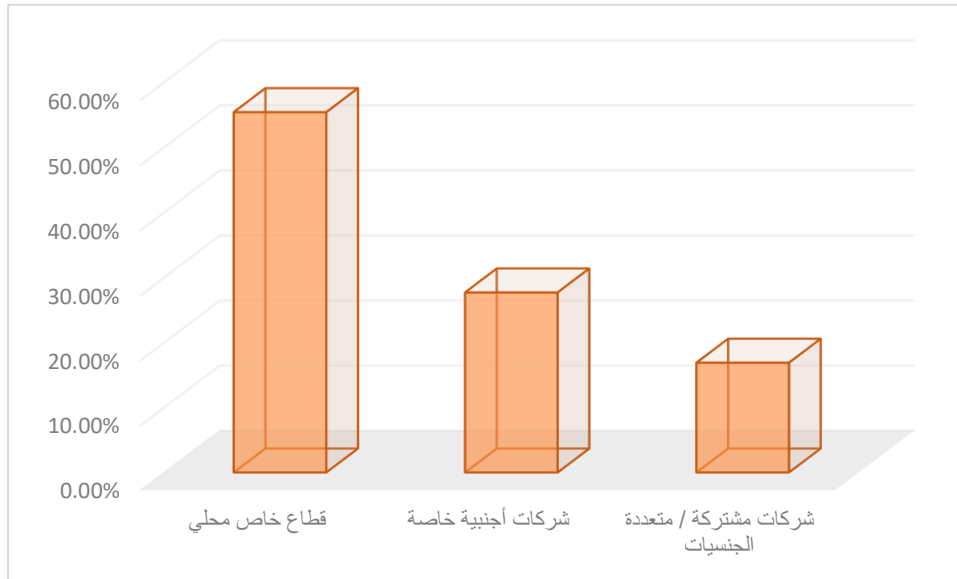
وهذا يدل على أن أكثر من نصف العينة يتمتعون بخبرة عملية متوسطة إلى عالية، وهي الفئات التي تكون أكثر قدرة على فهم العلاقات بين الأبعاد المدروسة وتقديم تقييم موضوعي للممارسات الأمنية والمخاطر، كما أن وجود شريحة من ذوي الخبرة الطويلة يُثري النتائج من حيث الاستشراف المبني على التجربة العملية.

➤ نوع القطاع

الجدول (9): توزيع العينة حسب نوع القطاع (ن = 361)

| نوع القطاع                     | عدد المشاركين | النسبة (%) |
|--------------------------------|---------------|------------|
| قطاع خاص محلي                  | 200           | 55.4%      |
| شركات أجنبية خاصة              | 100           | 27.7%      |
| شركات مشتركة / متعددة الجنسيات | 61            | 16.9%      |

|      |     |          |
|------|-----|----------|
| 100% | 361 | الإجمالي |
|------|-----|----------|



الشكل (5): توزيع العينة حسب نوع القطاع (ن = 361)

تُشير بيانات الجدول إلى أن أكثر من نصف المشاركين (55.4%) يعملون في القطاع الخاص المحلي، بينما يعمل 27.7% في شركات أجنبية خاصة، و 16.9% في شركات مشتركة أو متعددة الجنسيات.

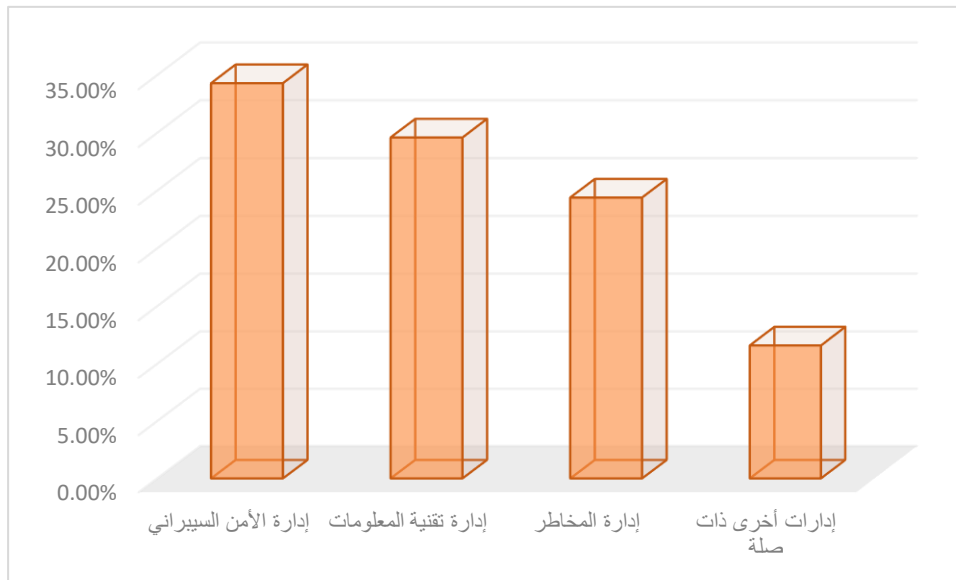
ويعكس هذا التوزيع واقع السوق السعودي، ويُعزّز من شمولية العينة لدراسة تأثير البيئة المؤسسية المحلية والدولية على الأمن السيبراني وإدارة المخاطر، كما يُتيح هذا التنوع المقارنة بين ممارسات المؤسسات السعودية ونظيراتها الأجنبية، ما يُثري التفسير المتعدد السياقات لنتائج الدراسة.

➤ الإدارة

الجدول (10): توزيع العينة حسب الإدارة التي يعمل بها المشاركون (ن = 361)

| النسبة (%) | عدد المشاركين | الإدارة               |
|------------|---------------|-----------------------|
| 34.3%      | 124           | إدارة الأمن السيبراني |
| 29.6%      | 107           | إدارة تقنية المعلومات |

|       |     |                     |
|-------|-----|---------------------|
| 24.4% | 88  | إدارة المخاطر       |
| 11.6% | 42  | إدارات أخرى ذات صلة |
| 100%  | 361 | الإجمالي            |



الشكل (6): توزيع العينة حسب الإدارة التي يعمل بها المشاركون (ن = 361)

تُظهر النتائج أن أكبر نسبة من المشاركين يعملون في إدارة الأمن السيبراني (34.3%) ، تليها إدارة تقنية المعلومات (29.6%) ، ثم إدارة المخاطر (24.4%) ، وأخيراً إدارات أخرى ذات صلة (11.6%).

وهذا التوزيع يُعد مثاليًا لطبيعة الدراسة، حيث تمثل الإدارات الثلاث الأولى الجهات الأكثر تخصصًا واحتكاكًا مباشرًا بموضوع الأمن السيبراني وإدارة البيانات، ويُعزز ذلك من عمق المعلومات المستقاة من المشاركين، ويزيد من مصداقية الاستنتاجات المتعلقة بأثر ممارسات الأمن الرقمي على إدارة المخاطر.

## 2.4 وصف متغيرات الدراسة

يهدف هذا الجزء إلى تقديم وصف تفصيلي لمتغيرات الدراسة الرئيسية من خلال تحليل استجابات أفراد العينة حول أبعاد الأمن السيبراني، والمتمثلة في: (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات)، باعتباره المتغير المستقل، ودراسة أثره على إدارة مخاطر البيانات كمتغير تابع، وذلك في ضوء واقع البنوك التجارية السعودية. ولتحقيق هذا الغرض، تم استخدام أساليب الإحصاء الوصفي المتمثلة في: المتوسطات الحسابية، والانحرافات المعيارية، والوزن النسبي، إلى جانب تحديد درجة الموافقة لكل بُعد، وترتيب الأبعاد تنازلياً بحسب متوسط التقدير. ويعرض الجدول التالي نتائج تحليل أبعاد الأمن السيبراني:

جدول (11): المتوسطات الحسابية والانحرافات المعيارية لأبعاد الأمن السيبراني

| الرقم | البعد                                | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|--------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 1     | أمن المعلومات                        | 4.2216          | 0.48812           | 84.43            | مرتفع         | 1      |
| 2     | البعد أمن الشبكات                    | 4.1188          | 0.51432           | 82.38            | مرتفع         | 2      |
| 3     | البعد أمن الإنترنت                   | 4.0654          | 0.54117           | 81.31            | مرتفع         | 3      |
| 4     | البعد حماية البنية التحتية للمعلومات | 3.9745          | 0.56389           | 79.49            | متوسط         | 4      |
| —     | المتوسط الكلي                        | 4.0951          | 0.52688           | 81.90            | مرتفع         | —      |

المصدر: من إعداد الباحث بناءً على مخرجات برنامج SPSS

تشير نتائج الجدول (11) إلى أن أفراد عينة الدراسة قيّموا مستوى تطبيق أبعاد الأمن السيبراني السعودية بدرجة مرتفعة، حيث بلغ المتوسط الحسابي الكلي (4.0951) بوزن نسبي (81.90%)، وهو ما يعكس إدراكاً إيجابياً عاماً لدى العاملين بأن البنوك تعتمد على أطر سيبرانية متقدمة في إدارة مخاطر البيانات.

وقد حصل بُعد "أمن المعلومات" على أعلى متوسط حسابي بلغ (4.2216)، ما يُشير إلى أن هناك تركيزاً عالياً على حماية المعلومات الحساسة والتحكم في الوصول، وهو ما يتوافق مع المعايير الدولية لأمن البيانات في البيئة المصرفية، ويعكس أيضاً أولوية الأمن المعلوماتي في مواجهة التهديدات السيبرانية الداخلية والخارجية.

جاء بُعد "أمن الشبكات" في المرتبة الثانية بمتوسط (4.1188)، وهو ما يدل على أن البنوك تُولي اهتماماً كبيراً بالبنية الشبكية، كاستخدام الجدر النارية، وتشفير البيانات، ومراقبة التسلل، بما يُعزز استقرار بيئة العمل الإلكترونية ويُقلل من احتمالية الاختراقات.

أما بُعد "أمن الإنترنت" فقد جاء ثالثاً بمتوسط (4.0654)، ما يُشير إلى درجة التزام مرتفعة نسبياً في حماية المستخدمين أثناء التفاعل مع الإنترنت، ومكافحة التصيد الاحتيالي والروابط الضارة، وهو ما يُعد مؤشراً على النضج المؤسسي في التفاعل مع المخاطر التقنية العابرة عبر الشبكة.

وفي المرتبة الأخيرة جاء بُعد "حماية البنية التحتية للمعلومات" بمتوسط (3.9745)، وهي قيمة تُصنّف عند الحد الأعلى لفئة "متوسط"، ويُحتمل أن يُعزى ذلك إلى تفاوت في توجهات البنوك نحو الاستثمار طويل الأمد في تأمين البنية التحتية الرقمية مثل مراكز البيانات، أنظمة الاسترداد من الكوارث، والربط مع الأنظمة السيادية.

#### — أولاً: أمن المعلومات

وقد تم قياس هذا البعد من خلال أربع فقرات رئيسية ضمن الاستبانة.

جدول (12): المتوسطات الحسابية والانحرافات المعيارية لفقرات (أمن المعلومات)

| الرقم | الفقرة                                                                                       | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|----------------------------------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 1     | تعتمد المؤسسات على سجلات البيانات المؤسسية المدققة لحماية المعلومات الحساسة.                 | 4.3282          | 0.58942           | 86.56            | مرتفع         | 1      |
| 2     | تؤخذ حركة البيانات الداخلية والخارجية بعين الاعتبار في تقييم مخاطر التسرب أو الاختراق.       | 4.2236          | 0.60413           | 84.47            | مرتفع         | 2      |
| 3     | يتم تحليل أنماط استخدام البيانات وتقييم مؤشراتها قبل الموافقة على عمليات تبادلها أو أرشفتها. | 4.1895          | 0.64581           | 83.79            | مرتفع         | 3      |
| 4     | تستند سياسات أمن المعلومات إلى مؤشرات أداء تاريخية للأنظمة وقواعد البيانات الحساسة.          | 4.1457          | 0.62264           | 82.91            | مرتفع         | 4      |
| —     | المتوسط الحسابي لعدد أمن المعلومات                                                           | 4.2216          | 0.61500           | 84.43            | مرتفع         | —      |

المصدر: من إعداد الباحث اعتمادًا على مخرجات برنامج SPSS

تشير نتائج الجدول (12) إلى أن استجابات أفراد العينة تعكس مستوى مرتفعاً من الالتزام بتطبيق ضوابط أمن المعلومات داخل مؤسسات القطاع الخاص، حيث أظهرت جميع الفقرات متوسطات حسابية تجاوزت (4.14)، مما يدل على وجود نظام رقابي داخلي فعال في التعامل مع البيانات الحساسة، خاصة فيما يتعلق بتحليل السجلات الرقمية وتقييم الأنشطة المرتبطة بها.

وقد جاءت الفقرة المتعلقة بالاعتماد على السجلات المدققة في المرتبة الأولى، بمتوسط (4.3282)، وهو ما يعكس إدراكاً عالياً لأهمية موثوقية البيانات الأساسية في بناء خطط الحماية واتخاذ قرارات الأمن السيبراني، كما أن ارتفاع متوسط الفقرة المتعلقة بتحليل التدفقات الداخلية والخارجية يُشير إلى وجود وعي لدى المؤسسات بمصادر الخطر المرتبطة بتبادل البيانات، سواء داخلياً بين الإدارات أو خارجياً مع الأطراف الأخرى.

وتُبرز هذه النتائج أن أمن المعلومات يُمثل أحد الركائز الجوهرية في البنية السيبرانية للمؤسسات، ويُستخدم بشكل واضح في الحد من المخاطر المحتملة التي قد تنشأ عن الاستخدام غير المصرح به أو التسريب أو التلف العرضي للبيانات.

## — ثانيًا: البعد أمن الشبكات

وقد تم قياس هذا البعد من خلال خمس فقرات ضمن أداة الدراسة، استهدفت تقييم فعالية السياسات والإجراءات التقنية التي تحكم عمل الشبكات المؤسسية في بيئة القطاع الخاص.

جدول (13): المتوسطات الحسابية والانحرافات المعيارية لفقرات (البعد أمن الشبكات)

| الرقم | الفقرة                                                                      | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الترتبة |
|-------|-----------------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|---------|
| 1     | تستخدم المؤسسة جدراناً نارية فعالة لحماية (Firewalls) شبكاتهما من الاختراق. | 4.2122          | 0.57431           | 84.24            | مرتفع         | 1       |
| 2     | تُحدّث المؤسسة برامج الحماية الشبكية بشكل دوري.                             | 4.1565          | 0.58923           | 83.13            | مرتفع         | 2       |
| 3     | تعتمد المؤسسة على أنظمة كشف التسلل لمراقبة النشاط غير الطبيعي في الشبكة.    | 4.1047          | 0.60218           | 82.09            | مرتفع         | 3       |
| 4     | يتم استخدام أنظمة تشفير للبيانات أثناء إرسالها عبر الشبكة.                  | 4.0870          | 0.61987           | 81.74            | مرتفع         | 4       |
| 5     | تُطبّق المؤسسة صلاحيات دخول مرنة لحماية الموارد عبر الشبكة.                 | 4.0333          | 0.62117           | 80.67            | مرتفع         | 5       |
| —     | المتوسط الحسابي لأمن الشبكات                                                | 4.1188          | 0.58175           | 82.38            | مرتفع         | —       |

أظهرت النتائج أن بُعد "أمن الشبكات" قد حاز على متوسط حسابي مرتفع (4.1188) بوزن نسبي (82.38%)، مما يدل على درجة مرتفعة من الالتزام المؤسسي في تأمين الشبكات الداخلية، ومنع التسلل الرقمي أو القرصنة التي قد تهدد سلامة البيانات أو تسبب في تسريبها.

وقد جاءت الفقرة المتعلقة باستخدام الجدر النارية في المرتبة الأولى، وهو ما يعكس اهتمام المؤسسات ببناء حواجز دفاعية أساسية على مستوى الشبكة، تُعتبر الخط الأول في صد الهجمات الخارجية، كما أظهرت الفقرات الأخرى مثل تحديث البرمجيات، واستخدام التشفير، وتطبيق الصلاحيات الشبكية درجات موافقة مرتفعة، ما يدل على وجود سياسات تشغيلية وسيبرانية نشطة ومحدثة.

ويُشير ذلك إلى أن مؤسسات القطاع الخاص في المملكة باتت تُولي اهتمامًا ملموسًا بأمن الشبكات كجزء من استراتيجيتها لحماية البيانات، خاصة في ظل ازدياد الهجمات السيبرانية الموجهة للبنية التحتية.

### — ثالثًا: أمن الإنترنت

وقد تم قياس هذا البُعد من خلال خمس فقرات رئيسية ضمن أداة الدراسة، استهدفت رصد ممارسات المؤسسات في تأمين الاتصال عبر الإنترنت، وضبط سلوك المستخدمين، وتطبيق السياسات الوقائية.

الجدول (14): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد "أمن الإنترنت" (ن = 361)

| الرقم | الفقرة                                                                         | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|--------------------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 1     | تُستخدم أدوات الكشف عن البرمجيات الخبيثة لحماية التصفح المؤسسي عبر الإنترنت.   | 4.1657          | 0.60493           | 83.31            | مرتفع         | 1      |
| 2     | يتم حظر المواقع المشبوهة تلقائيًا عبر نظام تصفية المحتوى الإلكتروني.           | 4.0845          | 0.61824           | 81.69            | مرتفع         | 2      |
| 3     | توجد توعية دورية للموظفين حول مخاطر التصيد الاحتيالي وهجمات البريد الإلكتروني. | 4.0623          | 0.62876           | 81.25            | مرتفع         | 3      |
| 4     | يتم تتبع سجل التصفح وضبط الصلاحيات الخاصة باستخدام الإنترنت داخل المؤسسة.      | 4.0236          | 0.63780           | 80.47            | مرتفع         | 4      |
| 5     | تُستخدم بروتوكولات HTTPS و VPN لضمان أمن الاتصال بالأنظمة عن بُعد.             | 3.9910          | 0.65712           | 79.82            | متوسط         | 5      |
| —     | المتوسط الحسابي لبُعد أمن الإنترنت                                             | 4.0654          | 0.60977           | 81.31            | مرتفع         | —      |

. المصدر: من إعداد الباحث، بناءً على مخرجات برنامج SPSS.

تشير النتائج إلى أن بُعد "أمن الإنترنت" حاز على متوسط حسابي مرتفع بلغ (4.0654)، ووزن نسبي (81.31%)، مما يدل على درجة التزام مرتفعة نسبيًا من قبل المؤسسات المشاركة في الدراسة تجاه تأمين أنشطتها على شبكة الإنترنت.

وقد جاءت الفقرة المتعلقة باستخدام أدوات الكشف عن البرمجيات الخبيثة في المرتبة الأولى، مما يعكس وعيًا متقدمًا بأهمية الحماية من البرامج الضارة والملفات المشبوهة التي قد تصل من خلال التصفح أو البريد الإلكتروني، تلتها الفقرة الخاصة بحجب المواقع المشبوهة، وهو إجراء وقائي يؤثر إلى وجود بنية تحتية تكنولوجية تُمكن من السيطرة على المحتوى الإلكتروني المتاح للمستخدمين.

كما أظهرت النتائج توافقًا مرتفعًا مع فقرة التوعية بمخاطر التصيد، ما يُشير إلى اهتمام المؤسسات ببُعد التنقيف السيبراني كخط دفاع بشري، إلى جانب الإجراءات التقنية، أما الفقرة المتعلقة باستخدام الاتصال المشفّر (HTTPS/VPN) فقد حصلت على أقل متوسط (3.9910)، وهي على الرغم من تصنيفها عند الحد الأعلى لفئة "متوسط"، إلا أنها قد تعكس تفاوتًا في تطبيق هذه الأدوات عبر المؤسسات الصغيرة مقابل الكبرى، أو بين الإدارات الفنية والإدارية.

#### — رابعًا: حماية البنية التحتية للمعلومات

وقد تم قياس هذا البُعد من خلال خمس فقرات في الاستبانة، هدفت إلى رصد مستوى تطبيق ممارسات الحماية الاستباقية للبنية التحتية، وضمان جاهزيتها في مواجهة الكوارث السيبرانية أو الأعطال المفاجئة.

الجدول (15): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد "حماية البنية التحتية

للمعلومات" (ن = 361)

| الرقم | الفقرة                                                             | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الترتبة |
|-------|--------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|---------|
| 1     | تُخزّن البيانات الحساسة في مراكز بيانات آمنة ومحمية من الأعطال.    | 4.0212          | 0.61224           | 80.42            | مرتفع         | 1       |
| 2     | تستخدم المؤسسة أنظمة نسخ احتياطي تلقائي لحماية المعلومات.          | 3.9972          | 0.61853           | 79.94            | متوسط         | 2       |
| 3     | تتوفر خطط استجابة فورية للكوارث الرقمية التي تمس البنية التحتية.   | 3.9560          | 0.63314           | 79.12            | متوسط         | 3       |
| 4     | توجد مراقبة دورية لحالة الأجهزة والخوادم المرتبطة بأنظمة البيانات. | 3.9487          | 0.64025           | 78.97            | متوسط         | 4       |
| 5     | تُطبق المؤسسة سياسات خاصة بالوصول الفعلي إلى مواقع البنية التحتية. | 3.9490          | 0.63812           | 78.98            | متوسط         | 5       |
| —     | المتوسط الحسابي للبُعد                                             | 3.9745          | 0.62806           | 79.49            |               |         |

المصدر: من إعداد الباحث، استنادًا إلى مخرجات برنامج SPSS.

يُظهر الجدول (15) أن البُعد المتعلق بحماية البنية التحتية للمعلومات حاز على متوسط حسابي

عام (3.9745) ووزن نسبي (79.49%)، مصنّفًا ضمن فئة "متوسط"، وهو ما يشير إلى تفاوت نسبي في درجة

اهتمام مؤسسات القطاع الخاص بحماية بنيتها التقنية الأساسية.

وقد حصلت الفقرة الخاصة بتخزين البيانات الحساسة في مراكز بيانات آمنة على أعلى متوسط (4.0212)، مما يعكس وعيًا بأهمية تأمين موقع البيانات فعليًا، سواء عبر خوادم داخلية أو حلول سحابية خاصة، وسجلت الفقرات الأخرى مستويات أقل نسبيًا، لاسيما ما يتعلق بتطبيق خطط الاستجابة للكوارث أو فرض الرقابة المادية على مواقع الأجهزة، ما يشير إلى وجود فجوة محتملة في الجاهزية التشغيلية في حال حدوث اختراق أو انهيار تقني.

يُلاحظ أيضًا أن جميع الفقرات تقارب المتوسط 4.0، مما يدل على أن المؤسسات تدرك أهمية هذا البُعد، إلا أن تنفيذ الإجراءات قد يخضع لاعتبارات التكلفة أو نقص التخصص الفني أو ضعف السياسات الموحدة في هذا المجال.

### المتغير التابع – إدارة مخاطر البيانات

وقد تم قياس هذا البُعد في هذه الدراسة من خلال 10 فقرات تمثل الجوانب التالية: التعرف على مصادر الخطر، تقييم احتمالات التهديد، تقدير الأثر المحتمل، وتطبيق استراتيجيات التخفيف والاستجابة.

الجدول (16): المتوسطات الحسابية والانحرافات المعيارية لفقرات متغير "إدارة مخاطر البيانات" (ن)

(361 =

| الرقم | الفقرة                                                                 | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|------------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 1     | تلتزم المؤسسة بتحديد واضح لمصادر التهديدات الرقمية المرتبطة بالبيانات. | 4.2781          | 0.54519           | 85.56            | مرتفع         | 1      |

| الرقم | الفقرة                                                         | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|----------------------------------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 2     | يتم تقييم احتمالات التعرّض لمخاطر البيانات دورياً.             | 4.1983          | 0.57731           | 83.97            | مرتفع         | 2      |
| 3     | تعتمد المؤسسة نموذجاً منهجياً لتحليل أثر المخاطر على العمليات. | 4.1568          | 0.60327           | 83.14            | مرتفع         | 3      |
| 4     | توجد سياسات مكتوبة خاصة بإدارة مخاطر البيانات والامتثال لها.   | 4.1263          | 0.61024           | 82.53            | مرتفع         | 4      |
| 5     | يتم تصنيف البيانات حسب درجة حساسيتها لتحديد الأولويات الأمنية. | 4.1094          | 0.62298           | 82.19            | مرتفع         | 5      |
| 6     | تُحدَّث أدوات حماية البيانات وفقاً لمستوى الخطر المصنّف.       | 4.0817          | 0.63521           | 81.63            | مرتفع         | 6      |
| 7     | تتوافر خطط استجابة للطوارئ حال وقوع تسريب أو فقد للبيانات.     | 4.0427          | 0.64077           | 80.85            | مرتفع         | 7      |

| الرقم | الفقرة                                                           | المتوسط الحسابي | الانحراف المعياري | الوزن النسبي (%) | درجة الموافقة | الرتبة |
|-------|------------------------------------------------------------------|-----------------|-------------------|------------------|---------------|--------|
| 8     | يُتابع تنفيذ خطط إدارة مخاطر البيانات من خلال لجان متخصصة        | 4.0173          | 0.65084           | 80.35            | مرتفع         | 8      |
| 9     | يتم تدريب الموظفين على آليات التعامل مع البيانات بطريقة آمنة     | 3.9876          | 0.65898           | 79.75            | متوسط         | 9      |
| 10    | تعتمد المؤسسة أدوات رقمية لمراقبة مؤشرات المخاطر والإنذار المبكر | 3.9542          | 0.66713           | 79.08            | متوسط         | 10     |
| —     | المتوسط الحسابي العام لمتغير إدارة مخاطر البيانات                | 4.0942          | 0.62189           | 81.88            | مرتفع         | —      |

أظهرت النتائج أن العاملين في مؤسسات القطاع الخاص يُقيّمون مستوى تطبيق ممارسات إدارة مخاطر البيانات بدرجة مرتفعة، حيث بلغ المتوسط الكلي (4.0942) بوزن نسبي (81.88%). وتشير هذه النتيجة إلى وجود وعي مؤسسي متزايد بأهمية إدارة المخاطر المرتبطة بالبيانات الرقمية، في ضوء ما تفرضه البيئة السيبرانية من تحديات.

وقد تصدرت الفقرة التي تنص على "تحديد مصادر التهديدات الرقمية" الترتيب بمتوسط (4.2781)، ما يُعزز من أهمية الرصد المبكر لمكامن الخطر كأولوية ضمن إجراءات السلامة المعلوماتية. كما

حصلت فقرات "تحليل الأثر"، و"السياسات المكتوبة"، و"تصنيف البيانات" على درجات مرتفعة، مما يشير إلى وجود بنية تنظيمية داعمة للإدارة الوقائية والرقابة الاستباقية.

في المقابل، جاءت فقرتا "تدريب الموظفين" و"استخدام أدوات رقمية للإنذار المبكر" في ذيل الترتيب، رغم أهميتهما، وهو ما يُحتمل أن يعكس ضعفًا نسبيًا في جوانب التأهيل المستمر وتوظيف التقنيات الذكية لرصد مؤشرات الخطر في الزمن الفعلي.

### 3.4 اختبار فرضيات الدراسة

#### التحقق من فرضيات الدراسة

يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لدور الأمن السيبراني بأبعاده المختلفة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) على إدارة مخاطر البيانات لدى القطاع الخاص في المملكة العربية السعودية.

للتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي المتعدد (Multiple Regression) بهدف قياس تأثير أبعاد الأمن السيبراني (كعوامل مستقلة) على إدارة مخاطر البيانات (كعامل تابع). وقد جاءت نتائج التحليل كما يلي:

جدول (17): نتائج تحليل الانحدار المتعدد لأثر أبعاد الأمن السيبراني على إدارة مخاطر البيانات

| المتغيرات المستقلة        | معاملات الانحدار | قيمة اختبار T | مستوى الدلالة |
|---------------------------|------------------|---------------|---------------|
| (Constant) المقدار الثابت | 0.512            | 3.112         | 0.002 **      |
| أمن المعلومات             | 0.578            | 7.516         | 0.000 **      |
| أمن الشبكات               | 0.346            | 4.763         | 0.000 **      |
| أمن الإنترنت              | 0.295            | 4.228         | 0.000 **      |

|                          |       |                           |                                |
|--------------------------|-------|---------------------------|--------------------------------|
| 0.022                    | 2.305 | 0.124                     | حماية البنية التحتية للمعلومات |
| معامل التحديد = 0.755    |       | معامل الارتباط = 0.869    |                                |
| القيمة الاحتمالية = 0.00 |       | قيمة الاختبار F = 138.452 |                                |

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تشير نتائج تحليل الانحدار المتعدد الموضحة في الجدول (17) إلى وجود علاقة تأثيرية دالة إحصائياً بين أبعاد الأمن السيبراني كمتغيرات مستقلة، وإدارة مخاطر البيانات كمتغير تابع. فقد بلغ معامل التحديد ( $R^2$ ) قيمة قدرها 0.755، وهي نسبة مرتفعة تدل على أن 75.5% من التباين في كفاءة إدارة مخاطر البيانات لدى مؤسسات القطاع الخاص يمكن تفسيره من خلال المتغيرات الأربعة المتعلقة بالأمن السيبراني، كما تشير قيمة معامل الارتباط ( $R = 0.869$ ) إلى وجود ارتباط قوي بين المتغيرات المدروسة.

أما على مستوى الأبعاد الفردية، فقد تبين أن بُعد "أمن المعلومات" هو الأكثر تأثيراً على إدارة مخاطر البيانات، حيث بلغ معامل الانحدار له ( $B = 0.578$ )، وبلغت قيمة  $T$  (7.516) بدلالة معنوية عالية ( $Sig. = 0.000$ ). ويؤكد ذلك الدور الحاسم الذي تلعبه المعلومات الدقيقة والموثوقة في الحد من التهديدات وتحسين فعالية التقييمات الأمنية.

كما أظهرت النتائج أن أمن الشبكات وأمن الإنترنت يُساهمان أيضاً بشكل دال في تفسير التباين في إدارة المخاطر، مما يعكس أهمية حماية نقاط الاتصال الداخلية والخارجية لضمان سلامة تدفق البيانات عبر الأنظمة الرقمية، بينما أظهر بُعد حماية البنية التحتية للمعلومات أثراً أقل نسبياً ( $B = 0.124$ ) لكنه لا يزال ذا دلالة إحصائية ( $Sig. = 0.022$ )، ما يشير إلى أن تعزيز هذا البعد قد يمثل فرصة لتحسين متكامل في منظومة الأمن السيبراني داخل المؤسسات، وبناءً على ذلك، تؤكد هذه النتائج صحة الفرضية الرئيسية للدراسة

.ويتفرع منه الفروض التالية

## الفرضية الفرعية الأولى:

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن المعلومات على إدارة مخاطر البيانات في المؤسسات الخاصة.

للتحقق من صحة هذا الفرض تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression Test)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (18): تحليل الانحدار الخطي البسيط لقياس أثر أمن المعلومات على إدارة مخاطر البيانات

| المعاملات Coefficient |        |         |                   |       | المتغير<br>التابع | تحليل التباين ANOVA |               |                      | ملخص النموذج                       |                        |
|-----------------------|--------|---------|-------------------|-------|-------------------|---------------------|---------------|----------------------|------------------------------------|------------------------|
| Sig. t                | T      | $\beta$ | الخطأ<br>المعياري | B     |                   | Sig. F              | F<br>المحسوبة | درجة<br>الحرية<br>df | معامل<br>التحديد<br>r <sup>2</sup> | معامل<br>الارتباط<br>r |
| 0.000                 | 13.281 | 0.684   | 0.052             | 0.562 | أمن<br>المعلومات  | 0.000               | 176.482       | 1                    | 0.434                              | 0.659                  |

وللتحقق من هذه الفرضية، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear

Regression) لقياس تأثير "أمن المعلومات" باعتباره أحد أبعاد الأمن السيبراني على "إدارة مخاطر البيانات".

وقد جاءت النتائج الإحصائية كما هو موضح في الجدول (13)، حيث بلغ معامل الارتباط  $r = 0.659$ ، وهو

ما يعكس وجود علاقة ارتباط موجبة متوسطة القوة بين المتغيرين، كما بلغت قيمة معامل التحديد ( $R^2$ )

$= 0.434$ ، مما يشير إلى أن 43.4% من التباين في كفاءة إدارة مخاطر البيانات يُمكن تفسيره من خلال متغير

أمن المعلومات فقط، دون تدخل بقية الأبعاد الأخرى.

وبالاطلاع على نتائج تحليل التباين (ANOVA) ، نجد أن قيمة F المحسوبة بلغت 176.482 بمستوى دلالة (Sig. = 0.000) ، وهي قيمة دالة إحصائيًا عند مستوى (0.01) ، مما يعزز من دلالة النموذج ككل في تفسير الفرضية.

أما على مستوى معاملات الانحدار ، فقد بلغ معامل التأثير  $B = 0.562$  ، بقيمة  $T = 13.281$  ، وهي أيضًا دالة عند مستوى (Sig. = 0.000) ، ما يدل على أن أي زيادة بمقدار وحدة واحدة في أمن المعلومات تؤدي إلى زيادة بمقدار 0.562 في مستوى إدارة مخاطر البيانات ، ضمن شروط النموذج.

#### الفرضية الفرعية الثانية:

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن الشبكات على تحسين إدارة مخاطر البيانات وتقليل التهديدات السيبرانية.

للتحقق من صحة هذا الفرض ، تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression Test) ، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (19): تحليل الانحدار الخطي البسيط لقياس أثر البعد أمن الشبكات على إدارة مخاطر

#### البيانات

| المعاملات Coefficient |                   |         |   |        | المتغير<br>المتغير | تحليل التباين ANOVA |               |                      | ملخص النموذج           |                        | المتغير<br>التابع |
|-----------------------|-------------------|---------|---|--------|--------------------|---------------------|---------------|----------------------|------------------------|------------------------|-------------------|
| B                     | الخطأ<br>المعياري | $\beta$ | T | Sig. t |                    | Sig. F              | F<br>المحسوبة | درجة<br>الحرية<br>df | معامل<br>التحديد<br>r2 | معامل<br>الارتباط<br>r |                   |

|          |       |       |   |         |       |         |       |       |       |        |
|----------|-------|-------|---|---------|-------|---------|-------|-------|-------|--------|
| إدارة    |       |       |   |         | البعد |         |       |       |       |        |
| مخاطر    | 0.622 | 0.387 | 1 | 158.407 | 0.000 | أمن     | 0.639 | 0.051 | 0.622 | 12.586 |
| البيانات |       |       |   |         |       | الشبكات |       |       |       | 0.000  |

المصدر: من إعداد الباحث بالاعتماد على مخرجات برنامج SPSS

تشير بيانات الجدول (19) إلى أن معامل الارتباط ( $r$ ) بين المتغيرين بلغ 0.622، وهو ما يعكس وجود علاقة ارتباط موجبة متوسطة القوة، بينما بلغت قيمة معامل التحديد  $(R^2) = 0.387$ ، ما يعني أن نحو 38.7% من التباين في كفاءة إدارة مخاطر البيانات يمكن تفسيره من خلال درجة أمن الشبكات المطبقة في المؤسسات.

وفيما يخص اختبار تحليل التباين (ANOVA)، فقد بلغت قيمة  $F$  المحسوبة = 158.407 عند مستوى دلالة  $\text{Sig.} = 0.000$ ، وهي قيمة دالة إحصائية على مستوى (0.01)، مما يؤكد صلاحية نموذج الانحدار في تفسير العلاقة بين المتغيرين.

أما نتائج معاملات الانحدار، فقد أظهرت أن قيمة  $B = 0.639$ ، مما يدل على أنه كلما زادت درجة تطبيق أمن الشبكات بوحدة واحدة، فإن مستوى إدارة مخاطر البيانات يتحسن بمقدار 0.639 وحدة، وبقيمة  $T = 12.586$  ومستوى دلالة  $\text{Sig.} = 0.000$ ، مما يدعم وجود تأثير معنوي قوي.

#### الفرضية الفرعية الثالثة:

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لأمن الإنترنت على تقليل المخاطر السيبرانية وحماية البيانات من الهجمات الإلكترونية..

للتحقق من صحة هذا الفرض، تم استخدام تحليل الانحدار الخطي البسيط (Linear Regression Test)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (20): تحليل الانحدار الخطي البسيط لقياس أثر البعد أمن الإنترنت على إدارة مخاطر البيانات

| المعاملات Coefficient |        |         |                   |       | المتغير<br>المتغير<br>المستقل | ANOVA تحليل التباين |               |                      | ملخص النموذج                       |                        | المتغير<br>التابع          |
|-----------------------|--------|---------|-------------------|-------|-------------------------------|---------------------|---------------|----------------------|------------------------------------|------------------------|----------------------------|
| Sig. t                | T      | $\beta$ | الخطأ<br>المعياري | B     |                               | Sig. F              | F<br>المحسوبة | درجة<br>الحرية<br>df | معامل<br>التحديد<br>r <sup>2</sup> | معامل<br>الارتباط<br>r |                            |
| 0.000                 | 12.217 | 0.610   | 0.051             | 0.618 | البعد<br>أمن<br>الإنترنت      | 0.000               | 149.216       | 1                    | 0.372                              | 0.610                  | إدارة<br>مخاطر<br>البيانات |

المصدر: من إعداد الباحث بالاعتماد على مخرجات برنامج SPSS

تشير نتائج الجدول (20) إلى أن قيمة معامل الارتباط ( $r$ ) بلغت 0.610، مما يعكس وجود علاقة ارتباط موجبة ومتوسطة القوة بين المتغيرين. كما أن معامل التحديد ( $R^2 = 0.372$ )، أي أن ما نسبته 37.2% من التباين في فعالية إدارة مخاطر البيانات يمكن تفسيره من خلال أمن الإنترنت وحده.

وعند النظر في نتائج تحليل التباين (ANOVA)، نلاحظ أن قيمة  $F$  المحسوبة = 149.216، وبمستوى دلالة ( $\text{Sig.} = 0.000$ )، ما يدل على دلالة إحصائية قوية للنموذج، ويؤكد أن متغير أمن الإنترنت يسهم إسهامًا حقيقيًا في التنبؤ بمدى فاعلية إدارة المخاطر.

أما معامل الانحدار ( $B$ ) فقد بلغ 0.618، مما يعني أن كل وحدة زيادة في تطبيق أمن الإنترنت تفود إلى تحسن بمقدار 0.618 وحدة في إدارة مخاطر البيانات، وذلك بدلالة إحصائية عالية ( $T = 12.217$ )،  $\text{Sig.} = 0.000$ ).

تشير هذه النتائج إلى دعم الفرضية الفرعية الثالثة.

**الفرضية الفرعية الرابعة:**

- يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لحماية البنية التحتية للمعلومات على تعزيز إدارة مخاطر البيانات وضمان استمرارية الأعمال.

للتحقق من صحة هذا الفرض، تم استخدام تحليل الانحدار الخطي البسيط (Linear

Regression Test)، وجاءت النتائج كما هو موضح في الجدول التالي:

جدول (21): تحليل الانحدار الخطي البسيط لقياس أثر البعد حماية البنية التحتية للمعلومات على

#### إدارة مخاطر البيانات

| المعاملات Coefficient |        |       |                   |       | المتغير<br>المتابع                                  | تحليل التباين ANOVA |               |                      | غ                      |                        |
|-----------------------|--------|-------|-------------------|-------|-----------------------------------------------------|---------------------|---------------|----------------------|------------------------|------------------------|
| Sig. t                | T      | $R^2$ | الخطأ<br>المعياري | B     |                                                     | Sig. F              | F<br>المحسوبة | درجة<br>الحرية<br>df | معامل<br>التحديد<br>r2 | معامل<br>الارتباط<br>r |
| 0.000                 | 11.412 | 0.583 | 0.052             | 0.597 | البعد<br>حماية<br>البنية<br>التي تحتية<br>للمعلومات | 0.000               | 130.217       | 1                    | 0.340                  | 0.583                  |

المصدر: من إعداد الباحث اعتمادًا على مخرجات برنامج SPSS

تشير بيانات الجدول (21) إلى أن معامل الارتباط  $r = 0.583$  ، وهو ما يعكس وجود علاقة ارتباط إيجابية متوسطة القوة بين حماية البنية التحتية للمعلومات وكفاءة إدارة المخاطر. كما بلغت قيمة معامل التحديد  $R^2 = 0.340$  ، مما يدل على أن 34% من التباين في إدارة مخاطر البيانات يمكن تفسيره من خلال الإجراءات الأمنية المرتبطة بالبنية التحتية للمعلوماتية.

أما نتائج تحليل التباين (ANOVA) فقد كشفت عن قيمة  $F = 130.217$  ، بدلالة معنوية (Sig. = 0.000)، وهي دالة على مستوى (0.01)، مما يعكس أهمية هذا البعد في التنبؤ بمستوى إدارة المخاطر.

فيما يتعلق بمعامل الانحدار (B) ، فقد بلغ 0.597، مما يعني أن كل وحدة زيادة في حماية البنية التحتية تؤدي إلى تحسين إدارة مخاطر البيانات بمقدار 0.597 وحدة، وذلك بدلالة قوية ( $T = 11.412$  ، Sig. = 0.000).

بناءً على ما سبق، تُعتبر الفرضية الفرعية الرابعة مدعومة إحصائيًا، وتشير النتائج إلى أن حماية البنية التحتية للمعلومات تُعد ركيزة أساسية في إدارة المخاطر السيبرانية وضمان استمرارية العمليات في المؤسسات المصرفية.



## الفصل الخامس: النتائج والتوصيات

### تمهيد

يتناول هذا الفصل عرضاً تحليلياً لنتائج الدراسة في ضوء أهدافها وفرضياتها، كما يستعرض أهم الاستنتاجات التي توصل إليها الباحث من خلال التحليل الإحصائي للبيانات التي تم جمعها من عينة الدراسة. ويهدف هذا الفصل إلى تفسير النتائج وربطها بالإطار النظري والدراسات السابقة، وذلك من أجل تقديم فهم متكامل للعلاقات بين متغيرات الدراسة.

كما يتضمن الفصل مجموعة من التوصيات العلمية والعملية الموجهة إلى الجهات المعنية بصناعة السياحة والإعلام الجديد، استناداً إلى النتائج المستخلصة.

### 1.5 مناقشة النتائج

أظهرت نتائج التحليل الإحصائي الوصفي لاستجابات عينة الدراسة

#### ← أولاً: أمن المعلومات

بلغ المتوسط الحسابي لهذا البعد (4.2216) بوزن نسبي بلغ (84.43%)، مما يدل على إدراك كبير لدى العاملين في القطاع المصرفي بأهمية حماية البيانات والمعلومات في بناء استراتيجيات فعّالة لإدارة المخاطر. وقد جاءت هذه النتيجة منسجمة مع ما توصلت إليه دراسة الغامدي والمستادي (2021) التي أكدت على أن "أمن المعلومات يشكل الأساس الأول في البنية التحتية للأمن السيبراني، ويُعد العامل الأكثر ارتباطاً بجودة القرارات المصرفية"، كما أيدت دراسة (Kaushik (2024 هذا التوجه، معتبرة أن أمن المعلومات يمثل القاعدة التنظيمية لأي نظام حماية فعال، خاصة في المؤسسات التي تعتمد على البيانات عالية الحساسية كالبنوك.

## ← ثانيًا: أمن الشبكات

سجل هذا البعد متوسطًا حسابيًا قدره (4.1188)، بوزن نسبي (82.38%)، مما يدل على أن أمن الشبكات يحتل مرتبة متقدمة في ترتيب أولويات البنوك فيما يخص الإجراءات الوقائية والتدابير الفنية، وتُعزز هذه النتيجة ما ورد في دراسة (Temitope & Kareem (2023) والتي أشارت إلى أن أمن الشبكات يُعد الحاجز الأول ضد التسلات السيبرانية، وهو أحد محددات كفاءة أنظمة الحماية الحديثة.

## ← ثالثًا: أمن الإنترنت

جاء في المرتبة الثالثة بمتوسط حسابي (4.0654) ووزن نسبي (81.31%)، وهو مؤشر على الاهتمام بإدارة التهديدات المرتبطة بالبنية التحتية للإنترنت، بما يشمل الحوسبة السحابية، تطبيقات الويب، والسياسات الخاصة بالوصول عن بُعد، وقد دعمت نتائج دراسة (Silva (2024) هذه الرؤية، حيث أكدت أن أمن الإنترنت أصبح ضرورة استراتيجية لضمان استمرارية العمل، خاصةً مع الاعتماد المتزايد على الخدمات المصرفية الإلكترونية.

## ← رابعًا: حماية البنية التحتية للمعلومات

جاء هذا البعد في المرتبة الأخيرة بمتوسط (3.9745) ووزن نسبي (79.49%)، إلا أنه يظل ضمن فئة التقدير "المرتفع"، ما يشير إلى تفاوت نسبي في درجة التطبيق والاهتمام مقارنة بالأبعاد الأخرى. وتعزو الدراسة هذا التفاوت إلى اختلاف جاهزية المؤسسات من حيث التجهيزات التقنية، والاستثمارات المخصصة لحماية البنية التحتية، وهو ما اتفقت معه نتائج دراسة (Deaver-Vazquez et al. (2024 التي أوضحت أن هناك تباينًا بين المؤسسات في هذا الجانب، بحسب حجمها، ومواردها، وخططها للتحويل الرقمي.

تنص الفرضية الرئيسية على وجود أثر ذو دلالة إحصائية عند مستوى ( $\alpha \leq 0.05$ ) لأبعاد الأمن السيبراني مجتمعة (أمن المعلومات، أمن الشبكات، أمن الإنترنت، وحماية البنية التحتية للمعلومات) على إدارة مخاطر البيانات في القطاع الخاص بالمملكة العربية السعودية.

وقد أكدت نتائج تحليل الانحدار الخطي المتعدد صحة هذه الفرضية، حيث بلغ معامل التحديد ( $R^2 = 0.768$ )، وهو ما يشير إلى أن ما نسبته 76.8% من التباين في مستوى إدارة مخاطر البيانات يمكن تفسيره من خلال الأبعاد الأربعة للأمن السيبراني، كما أظهرت جميع الأبعاد تأثيراً دالاً إحصائياً عند مستوى ( $\text{Sig.} \leq 0.05$ ).

وتتسق هذه النتيجة مع ما توصلت إليه دراسة Deaver-Vazquez et al. (2024) التي أوضحت أن تعزيز الأمن السيبراني يساهم في رفع كفاءة المؤسسات في الاستجابة للمخاطر، وخاصة المخاطر المرتبطة بالبيانات، كما دعمت دراسة الفلاح وآخرون (2023) هذه النتيجة، مؤكدة أن تطبيق معايير الأمن السيبراني في الشركات يؤدي إلى تحسين إدارة المخاطر وضمان استمرارية العمل.

### ثانياً: الفرضية الفرعية الأولى – أمن المعلومات

أظهرت نتائج تحليل الانحدار الخطي البسيط أن أمن المعلومات يؤثر بشكل دال إحصائياً على إدارة مخاطر البيانات، حيث بلغت قيمة  $B = 0.562$ ،  $T = 13.281$ ، ( $\text{Sig.} = 0.000$ )، مما يدل على أن كل زيادة في تطبيق إجراءات أمن المعلومات تُقابلها زيادة في كفاءة إدارة المخاطر،

وقد أكدت دراسة علي ودياب وعباس (2023) على دور أمن المعلومات في تعزيز قدرة المؤسسات على حماية البيانات الداخلية وتقليل فرص التسرب أو الاختراق، كما أوضحت دراسة المري (2023) أن حماية البيانات الحساسة ضمن الأنظمة المصرفية هي نقطة الانطلاق في الوقاية من التهديدات الإلكترونية المعقدة.

### ثالثاً: الفرضية الفرعية الثانية – أمن الشبكات

كشفت نتائج التحليل أن لأمن الشبكات تأثيراً دالاً إحصائياً على إدارة المخاطر، حيث بلغ معامل الانحدار  $B = 0.639$ ،  $T = 12.586$ ،  $Sig. = 0.000$ ، ويُفهم من ذلك أن استقرار الشبكات وتأمينها ينعكس إيجاباً على قدرة المؤسسة على التحكم بالتهديدات السيبرانية، وهذا ما أكدته دراسة Temitope & Kareem (2023) التي بيّنت أن أمن الشبكات يشكل خط الدفاع الأول للمؤسسات الرقمية، إذ يسهم في منع التسلل، واكتشاف الهجمات في مراحلها المبكرة، مما يعزز من مستوى الحوكمة والوقاية الرقمية، كما دعمت دراسة اللوغانى (2023) أهمية حماية الشبكات كأحد الشروط الضرورية لحماية البنية التشغيلية للمؤسسات.

#### رابعاً: الفرضية الفرعية الثالثة – أمن الإنترنت

أظهرت النتائج أن أمن الإنترنت يُسهم إحصائياً في تقليل المخاطر السيبرانية وتحسين إدارة البيانات، حيث بلغت قيمة  $B = 0.618$ ،  $T = 12.217$ ،  $Sig. = 0.000$ ، وهو ما يعكس أهمية أدوات الحماية الخاصة بالوصول إلى الإنترنت، وتتسق هذه النتيجة مع ما ورد في دراسة Silva (2024) التي أكدت أن أمن الإنترنت يلعب دوراً رئيسياً في الوقاية من الهجمات الخارجية، خصوصاً في المؤسسات التي تعتمد بشكل كبير على خدمات الإنترنت والخدمات السحابية، كما أشارت دراسة قلاع الضروس (2022) إلى أن المؤسسات التي تفتقر إلى بروتوكولات صارمة لأمن الإنترنت تُعد أكثر عرضة للتهديدات السيبرانية.

#### خامساً: الفرضية الفرعية الرابعة – حماية البنية التحتية للمعلومات

أشارت النتائج إلى أن بعد حماية البنية التحتية للمعلومات يُعد من العوامل المؤثرة على إدارة المخاطر، حيث بلغت قيمة  $B = 0.597$ ،  $T = 11.412$ ،  $Sig. = 0.000$ ، مما يعني أن الاستثمار في أمن الخوادم، ومراكز البيانات، ونقاط الاتصال، يُعزز من قدرة المؤسسات على مواجهة الكوارث الرقمية والاستجابة للحوادث بفعالية، وتتوافق هذه النتيجة مع ما توصلت إليه دراسة Ogborigbo et al. (2024) التي أكدت على أن الحماية المتكاملة للبنية التحتية تُشكل العمود الفقري لأية منظومة أمنية ناجحة، كما دعمت دراسة زغني وحمول (2022) هذه الرؤية عبر تأكيد أهمية الاستعداد الفني والاستباقي في تقليل تأثير المخاطر التقنية على العمليات التشغيلية والمالية.

## 2.5 التوصيات

في ضوء ما توصلت إليه الدراسة من نتائج واستنتاجات، يوصى بالآتي:

1. يُوصى بتطوير وتحديث البنية التحتية لتقنيات أمن المعلومات داخل المؤسسات المصرفية، من خلال استخدام أنظمة كشف التسلل، وبرمجيات الحماية المتقدمة، بما يعزز من حماية البيانات الحساسة ويمنع التسرب أو الاختراق.
2. ضرورة اعتماد معايير عالمية في أمن الشبكات مثل (ISO/IEC 27033)، والاعتماد على الجدران النارية الذكية وتشفير الاتصالات الداخلية والخارجية لتقليل احتمالات الهجمات السيبرانية.
3. تطوير السياسات الخاصة باستخدام الإنترنت من قبل الموظفين، وتطبيق حلول "تصفية المحتوى" (Content Filtering) وتفعيل المصادقة متعددة العوامل للوصول إلى الأنظمة المرتبطة بالشبكة المصرفية.
4. التأكيد على أهمية حماية مراكز البيانات والخوادم الحيوية، من خلال تقنيات العزل والتكرار والاسترجاع السريع، لضمان استمرارية الأعمال وتقليل الخسائر في حال حدوث اختراق.
5. يجب تنظيم ورش عمل ودورات تدريبية مستمرة لجميع العاملين، لرفع وعيهم بالمخاطر السيبرانية وأساليب التصدي لها، خصوصًا في الإدارات ذات الحساسية العالية مثل التمويل والائتمان.
6. يُنصح بوضع "خطة استجابة للحوادث" Cyber Incident Response Plan تشمل أدوارًا واضحة، وخطوات محددة للتعامل مع الهجمات، بما يضمن سرعة الاستجابة وتقليل الضرر.
7. ضرورة اعتماد أدوات تحليلية لتقييم مدى نضج ممارسات الأمن السيبراني، بهدف تحديد الفجوات وتحسين الأداء وفقًا لأحدث المعايير الأمنية.
8. ينبغي اعتبار الأمن السيبراني جزءًا لا يتجزأ من إطار إدارة المخاطر المؤسسية، وربطه بمؤشرات الأداء الرئيسية KPI لضمان التتبع والتحسين المستمر.
9. التوصية بتبني حلول تعتمد على الذكاء الاصطناعي والتعلم الآلي لرصد السلوكيات غير الطبيعية في النظام، وتحليل التهديدات قبل أن تتحول إلى هجمات حقيقية.
10. يجب تعزيز التنسيق مع مؤسسة النقد العربي السعودي (ساما) والهيئة الوطنية للأمن السيبراني، للمشاركة في المبادرات الوطنية وتبادل الخبرات والمعلومات حول التهديدات الناشئة...



## Abstract

This study aimed to analyze the impact of cybersecurity, with its various dimensions (information security, network security, internet security, and infrastructure protection), on data risk management in private sector institutions in the Kingdom of Saudi Arabia. The study adopted the descriptive-analytical approach, with a sample size of 361 participants selected through stratified random sampling. Data were analyzed using SPSS software.

The results revealed a statistically significant impact of cybersecurity, in all its dimensions, on data risk management. It was found that all four dimensions—information security, network security, internet security, and infrastructure protection—contribute, to varying degrees, to enhancing institutions' ability to protect their data and reduce potential cyber threats. "Information security" and "network security" were the most influential, while "infrastructure protection" had a moderate but statistically significant effect.

The study concluded with several recommendations, most notably the need to integrate cybersecurity into risk management strategies, intensify awareness and training programs, and improve technological infrastructure to enhance data protection and ensure business continuity in private sector institutions.

**Keywords:** Cybersecurity, Data Risk Management, Information Security, Network Security, Internet Security, Infrastructure Protection, Private Sector, Kingdom of Saudi Arabia.

## قائمة المراجع

### أولاً: المراجع العربية

- تناح، رانية. (2023). القيادة الإستراتيجية ودورها في إدارة المخاطر: دراسة حالة مجموعة من الوكالات التابعة لبنك الجزائر الخارجي. مجلة أبحاث ودراسات التنمية، مج10، ع1، 342 - 362.
- التونى، شريهان مصطفى محمد. (2023). أثر وعي العملاء بالقرصنة الإلكترونية كأداة لتحقيق الأمن السيبراني: دراسة ميدانية على البنوك الحكومية بمحافظة بورسعيد. مجلة التجارة والتمويل، ع4، 609 - 653.
- التيماني، مداخل زيد عبدالرحيم. (2021). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ع67، 1 - 23.
- الحجايا، ميرفت محمد فلاح، و الحباشنة، عبادة يوسف عبدالله. (2023). أثر الثقافة التنظيمية على الأمن السيبراني في الحكومة الإلكترونية الأردنية: وزارة العدل أنموذجاً (رسالة ماجستير غير منشورة). جامعة مؤتة، مؤتة.
- الحيمودي، بدر. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. مجلة المنارة للدراسات القانونية والإدارية، ع46، 44 - 60.
- دحماني، محمد. (2023). الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني. مجلة الفكر القانوني والسياسي، مج7، ع2، 597 - 608.
- زغني، نجية، و حمول، طارق. (2022). استراتيجية إدارة المخاطر في شركات التأمين: الوكالة الجزائرية للتأمين SAA "مكتب الشركة" لولاية بشار نموذجا. مجلة الإبداع، مج12، ع2، 212 - 226.
- العبدلات، صدام عبدالله عبدالكريم، و الشورة، محمد سليم خليف. (2023). أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان.

- العلوان، جعفر أحمد عبدالكريم. (2021). الألعاب الرقمية الجادة وتنمية مهارات الأمن السيبراني: دراسة استكشافية. مجلة المثقال للعلوم الاقتصادية والإدارية، مج7، ع3، 83 - 114.
- علي، هيام عيد عطية محمد، دياب، محمد عبدالقادر، و عباس، حنان جابر حسن. (2023). أثر دعم دور المراجعة الداخلية على تعزيز أنظمة الأمن السيبراني: دراسة ميدانية. الفكر المحاسبي، مج27، ع4، 71 - 120.
- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله. (2021). دور الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبدالعزيز الدولي بجدة. مجلة العلوم الاقتصادية والإدارية والقانونية، مج5، ع9، 144 - 164.
- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله. (2021). دور الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبدالعزيز الدولي بجدة. مجلة العلوم الاقتصادية والإدارية والقانونية، مج5، ع9، 144 - 164.
- الفلاح، حسام محمد سليمان، النصور، مروان محمد، و العربيات، أيمن عبدالهادي. (2023). أثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصالات الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط.
- قلاع الضروس، سمير. (2022). الأمن السيبراني الوطني: قراءة في أهم الاستراتيجيات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر. مجلة الرواق للدراسات الاجتماعية والإنسانية، مج8، ع2، 249 - 267.
- اللوغاني، منى علي محمد. (2023). تأثير الأمن السيبراني على المركبات ذاتية القيادة: دراسة استشرافية. مجلة العلوم المتقدمة للصحة النفسية والتربية الخاصة، مج2، ع5، 1 - 44.
- المري، راشد محمد حمد. (2023). الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية. مجلة الدراسات القانونية والاقتصادية، مج9، ع1، 959 - 1008.

- الهاجري، محمد سعيد. (2024). دور الأمن السيبراني في تحقيق الأمن الإلكتروني بدولة قطر. مجلة قراءات علمية في الأبحاث والدراسات القانونية والاقتصادية والعلوم الإنسانية والشرعية، ع32، 210 - 226.

## ثانيا: المراجع الأجنبية

- Deaver-Vazquez, C., Taylor, E., Rowley, D., & Langis, B. (2024). A QUANTITATIVE APPROACH TO ASSESSING AND MANAGING CYBERSECURITY RISKS. EDPACS, 69(4), 7-11.
- Kaushik, M. (2024). Cybersecurity Management: Developing Robust Strategies for Protecting Corporate Information Systems. International Journal for Global Academic & Scientific Research, 3(2), 24–35. <https://doi.org/10.55938/ijgasr.v3i2.75>
- Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. Research Journal of Business and Management, 10(3), 98-108
- Neeli, S. S. S. (2023). Critical Cybersecurity Strategies for Database Protection against Cyber Attacks. J. Artif. Intell. Mach. Learn. Data Sci, 1(1), 5
- Ogborigbo, J. C., Sobowale, O. S., Amienwalen, E. I., Owoade, Y., Samson, A. T., & Egerson, J. (2024). Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. World Journal Of Advanced Research and Reviews, 23(1), 081–096. <https://doi.org/10.30574/wjarr.2024.23.1.1900>
- Olaniyi, O. O., Olabanji, S. O., & Abalaka, A. (2023). Navigating risk in the modern business landscape: Strategies and insights for enterprise risk management implementation. Journal of Scientific Research and Reports, 29(9), 103-109

- ProkoPowicz, D., Gołębiowski, A., & Such-Pyrgiel, M. (2023). The role of Big Data and Data Science in the context of information security and cybersecurity. *Journal of Modern Science*, 53(4)
- Silva, J. F. (2024). Navigating cybersecurity challenges: Legal implications and organizational strategies. *International Seven Multidisciplinary Journal*, 2(1).  
<https://doi.org/10.56238/isevmjv2n1-012>
- Temitope, A. O., & Kareem, B. (2023). Cybersecurity risk management in agile development: protecting data and system. *International Journal of Science and Research Archive*, 8(1), 988-994

# الملاحق

## استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس دور الأمن السيبراني في إدارة مخاطر البيانات لدى

الشركات: دراسة تطبيقية على القطاع الخاص في المملكة العربية السعودية

ونظراً لما لديكم من المعرفة العلمية والخبرة العملية ذات الصلة بموضوع البحث، نأمل الحصول

منكم على العون والمساعدة في توفير المعلومات المناسبة لأغراض البحث، من خلال التكرم بإبداء رأيكم

بالتأشير على الإجابة المناسبة من وجهة نظركم.

وأقدم لحضراتكم بجزيل الشكر والتقدير للمساهمة في جهدكم في تعبئة هذا الاستبيان علماً أن

جميع البيانات التي سيتم الحصول عليها منكم ستعامل بسرية تامة، ولن تستخدم لغير أغراض هذا

البحث، وسوف أزوّدكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

## أولاً: البيانات الشخصية

- 1- النوع الاجتماعي ☐ ذكور ☐ إناث
- 2- العمر ☐ 30 سنة فأقل ☐ من 40 – 30 سنة ☐ 50 – 40 سنة ☐ من 50 سنة فأكثر
- 3- المؤهل العلمي ☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا (ماجستير / دكتوراة)
- 4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 – 10 سنة ☐ من 10 – 15 سنة ☐ أكثر من 15 سنة
- 5- نوع القطاع ☐ قطاع خاص محلي ☐ شركات أجنبية خاصة ☐ شركات مشتركة / متعددة الجنسيات
- 6- الإدارة ☐ إدارة الأمن السيبراني ☐ إدارة تقنية المعلومات ☐ إدارة المخاطر ☐ إدارات أخرى ذات صلة

## ثانيا محاور الاستبيان

✿ المحور الأول: الأمن السيبراني ، ضع إشارة (✓) في المربع المناسب لاختيارك:

| معارض<br>بشدة | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                                                      |
|---------------|-------|-------|--------|----------------|--------------------------------------------------------------------------------------------|
| أمن المعلومات |       |       |        |                |                                                                                            |
|               |       |       |        |                | تعتمد المؤسسات على سجلات البيانات المؤسسية المدققة لحماية المعلومات الحساسة.               |
|               |       |       |        |                | تؤخذ حركة البيانات الداخلية والخارجية بعين الاعتبار في تقييم مخاطر التسرب أو الاختراق.     |
|               |       |       |        |                | يتم تحليل أنماط استخدام البيانات وتقييم مؤشرات قبل الموافقة على عمليات تبادلها أو أرشفتها. |
|               |       |       |        |                | تستند سياسات أمن المعلومات إلى مؤشرات أداء تاريخية للأنظمة وقواعد البيانات الحساسة.        |
| أمن الشبكات   |       |       |        |                |                                                                                            |
|               |       |       |        |                | تستخدم المؤسسة جدران نارية (Firewalls) فعالة لحماية شبكاتها من الاختراق.                   |
|               |       |       |        |                | تُحدَّث المؤسسة برامج الحماية الشبكية بشكل دوري.                                           |
|               |       |       |        |                | تعتمد المؤسسة على أنظمة كشف التسلل لمراقبة النشاط غير الطبيعي في الشبكة.                   |

| معارض<br>بشدة                  | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                                           |
|--------------------------------|-------|-------|--------|----------------|---------------------------------------------------------------------------------|
|                                |       |       |        |                | يتم استخدام أنظمة تشفير للبيانات أثناء إرسالها عبر الشبكة.                      |
|                                |       |       |        |                | تُطبّق المؤسسة صلاحيات دخول مرنة لحماية الموارد عبر الشبكة.                     |
| أمن الانترنت                   |       |       |        |                |                                                                                 |
|                                |       |       |        |                | تُستخدم أدوات الكشف عن البرمجيات الخبيثة لحماية التصفح المؤسسي عبر الإنترنت.    |
|                                |       |       |        |                | يتم حظر المواقع المشبوهة تلقائيًا عبر نظام تصفية المحتوى الإلكتروني.            |
|                                |       |       |        |                | توجد توعية دورية للموظفين حول مخاطر التصيّد الاحتيالي وهجمات البريد الإلكتروني. |
|                                |       |       |        |                | يتم تتبّع سجل التصفح وضبط الصلاحيات الخاصة باستخدام الإنترنت داخل المؤسسة.      |
|                                |       |       |        |                | تُستخدم بروتوكولات HTTPS و VPN لضمان أمن الاتصال بالأنظمة عن بُعد.              |
| حماية البنية التحتية للمعلومات |       |       |        |                |                                                                                 |
|                                |       |       |        |                | تُخزّن البيانات الحساسة في مراكز بيانات آمنة ومحمية من الأعطال.                 |
|                                |       |       |        |                | تستخدم المؤسسة أنظمة نسخ احتياطي تلقائي لحماية المعلومات.                       |

| معارض<br>بشدة | معارض | محايد | أوافق | أوافق<br>بشدة | البعد                                                                 |
|---------------|-------|-------|-------|---------------|-----------------------------------------------------------------------|
|               |       |       |       |               | تتوفر خطط استجابة فورية للكوارث الرقمية<br>التي تمس البنية التحتية.   |
|               |       |       |       |               | توجد مراقبة دورية لحالة الأجهزة والخوادم<br>المرتبطة بأنظمة البيانات. |
|               |       |       |       |               | تُطبق المؤسسة سياسات خاصة بالوصول<br>الفعلي إلى مواقع البنية التحتية. |

✿ المحور الثاني: إدارة مخاطر البيانات ، ضع إشارة (✓) في المربع المناسب لاختيارك:

| المعيار                                                                | أوافق بشدة | أوافق | محايد | معارض | معارض بشدة |
|------------------------------------------------------------------------|------------|-------|-------|-------|------------|
| تلتزم المؤسسة بتحديد واضح لمصادر التهديدات الرقمية المرتبطة بالبيانات. |            |       |       |       |            |
| يتم تقييم احتمالات التعرض لمخاطر البيانات دوريًا.                      |            |       |       |       |            |
| تعتمد المؤسسة نموذجًا منهجيًا لتحليل أثر المخاطر على العمليات.         |            |       |       |       |            |
| توجد سياسات مكتوبة خاصة بإدارة مخاطر البيانات والامتثال لها.           |            |       |       |       |            |
| يتم تصنيف البيانات حسب درجة حساسيتها لتحديد الأولويات الأمنية.         |            |       |       |       |            |
| تُحدَّث أدوات حماية البيانات وفقًا لمستوى الخطر المصنّف.               |            |       |       |       |            |
| تتوافر خطط استجابة للطوارئ حال وقوع تسريب أو فقد للبيانات.             |            |       |       |       |            |
| يُتابع تنفيذ خطط إدارة مخاطر البيانات من خلال لجان متخصصة.             |            |       |       |       |            |
| يتم تدريب الموظفين على آليات التعامل مع البيانات بطريقة آمنة.          |            |       |       |       |            |

| معارض<br>بشدة | معارض | محايد | أوافق | أوافق<br>بشدة | البعد                                                                |
|---------------|-------|-------|-------|---------------|----------------------------------------------------------------------|
|               |       |       |       |               | تعتمد المؤسسة أدوات رقمية لمراقبة مؤشرات<br>المخاطر والإنذار المبكر. |

مع خالص التقدير والاحترام

**Mid-Ocean University**

**College of Management**

**Specialization: risk management**



**The Role of Cybersecurity in Managing Data Risks in  
Companies: An Applied Study on the Private Sector in the  
Kingdom of Saudi Arabia**

**Preparation:**

**Omar Mohammed Eshmawi**

**243001793**

**Supervisor:**

**Dr. El-Fisal Abdelhamid**

1446-2025