

جامعة ميد أوشن



كلية الإدارة

ماجستير إدارة الأعمال

أثر تطبيق ممارسات الأمن السيبراني على استدامة التحول الرقمي في

المؤسسات السعودية: دراسة ميدانية في ضوء رؤية المملكة 2030

إعداد الطالب/

مشاعل غزاي العتيبي

251002386

إشراف/

أ.د / الفیصل عبد الحمید

أ.د / فايز جراد

العام الدراسي:

1447 – 2025



# إِهْدَاء

إلى من كان لهم بعد الله الفضل في إتمام هذه الدراسة،

إلى والديّ الكريمين، اللذين قدّما لي الحب والدعم والتشجيع بلا حدود،

إلى أمي، التي لم تفتر يوماً عن الدعاء لي في كل حين،

وإلى أبي، الذي لم يخل عليّ بنصيحةٍ أو كلمةٍ تبعث في نفسي الأمل،

إلى أساتذتي الكرام، الذين وجّهوني بحكمتهم وصبرهم، وكانوا مناراتٍ أضاءت دربي،

إلى زملائي وزميلاتي الذين شاركوني رحلة العلم بتعاونهم وتشجيعهم،

إلى أصدقائي الذين كانوا عزائي في لحظات التعب، وفرحتي عند النجاح،

إلى كل من ساهم بكلمة، أو فكرة، أو دعم، أو دعاء،

أهديكم هذا العمل المتواضع عرفاناً بجميلكم،

وتقديرًا لكل لحظة دعمٍ كانت وقوداً لاستمرارتي حتى النهاية.

# شكر وفخر

أحمد الله عز وجل الذي وفقني في إتمام هذا البحث العلمي،

والذي ألهمني الصحة والعافية والعزيمة.

فالحمد لله حمداً كثيراً

أتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور /

د. الفیصل عبدالمحمد محمد

د. فايز جراد

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 يسعني الحظ بذكر أسمائهم راجيةً من المولي عز وجل أن تكون هذه الدراسة نافذة لدراسات أخرى .

## المستخلص

هدفت هذه الدراسة إلى تحليل أثر ممارسات الأمن السيبراني بأبعادها المختلفة (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) على تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية ، و اعتمدت الدراسة على المنهج الوصفي التحليلي، وتم جمع البيانات من خلال استبانة موجهة إلى عينة مكونة من (270) موظفًا يعملون في مؤسسات سعودية متعددة القطاعات.

و أظهرت النتائج وجود علاقة ذات دلالة إحصائية بين جميع أبعاد ممارسات الأمن السيبراني واستدامة التحول الرقمي، حيث كان أعلى تأثير لبُعد التقييم المستمر للمخاطر، يليه بعد سياسات الحماية الإلكترونية، ثم التدريب والتوعية الأمنية، وأخيرًا نظم مراقبة التهديدات، كما بينت النتائج أن ممارسات الأمن السيبراني تفسر ما نسبته (57.3%) من التباين في استدامة التحول الرقمي، وهو ما يدل على أهمية دمج مفاهيم الأمن السيبراني ضمن الاستراتيجيات الرقمية الوطنية والمؤسسية.

واختتمت الدراسة بعدد من التوصيات أبرزها: ضرورة تطوير سياسات أمنية واضحة، وتكثيف التدريب، وتعزيز المراقبة المستمرة، وإنشاء وحدات تقييم داخلي للأمن الرقمي، بما يضمن استدامة منظومة التحول الرقمي في المملكة العربية السعودية.

الكلمات المفتاحية: ممارسات الأمن السيبراني، الاستدامة، التحول الرقمي، المؤسسات السعودية،

رؤية المملكة 2030

## قائمة المحتويات

|         |                                                                  |
|---------|------------------------------------------------------------------|
| أ.....  | بسم الله الرحمن الرحيم                                           |
| ب.....  | الإهداء                                                          |
| ج.....  | الشكر والتقدير                                                   |
| د.....  | المستخلص                                                         |
| ه.....  | قائمة المحتويات                                                  |
| ح.....  | قائمة الجداول                                                    |
| 1.....  | الفصل الأول: الإطار العام للدراسة                                |
| 1.....  | 1.1 المقدمة                                                      |
| 2.....  | 2.1 المشكلة البحثية                                              |
| 4.....  | 3.1 أهمية البحث                                                  |
| 5.....  | 4.1 أهداف البحث                                                  |
| 6.....  | 5.1 تساؤلات البحث                                                |
| 7.....  | 6.1 فرضيات البحث                                                 |
| 7.....  | 7.1 الدراسات السابقة                                             |
| 12..... | 8.1 أوجه التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية |
| 13..... | 9.1 المنطلقات النظرية للبحث                                      |
| 14..... | 10.1 منهج البحث                                                  |
| 15..... | 11.1 مصادر البيانات في الدراسة                                   |
| 16..... | 12.1 أدوات الدراسة والأساليب الإحصائية                           |
| 16..... | 13.1 نموذج الدراسة                                               |

|         |                                                  |
|---------|--------------------------------------------------|
| 17..... | 14.1 حدود الدراسة:                               |
| 18..... | الفصل الثاني: الإطار النظري                      |
| 18..... | المبحث الأول: ممارسات الأمن السيبراني            |
| 18..... | 1.1.2 التمهيد                                    |
| 18..... | 2.1.2 مفهوم ممارسات الأمن السيبراني              |
| 20..... | 3.1.2 أهمية ممارسات الأمن السيبراني              |
| 21..... | 4.1.2 أهداف ممارسات الأمن السيبراني              |
| 23..... | 5.1.2 أبعاد ممارسات الأمن السيبراني              |
| 26..... | المبحث الثاني: استدامة التحول الرقمي في المؤسسات |
| 26..... | 1.2.2 التمهيد                                    |
| 26..... | 2.2.2 مفهوم استدامة التحول الرقمي                |
| 27..... | 3.2.2 أهمية استدامة التحول الرقمي                |
| 29..... | 4.2.2 أهداف استدامة التحول الرقمي                |
| 30..... | 5.2.2 العوامل المؤثرة في استدامة التحول الرقمي   |
| 33..... | الفصل الثالث: منهجية الدراسة                     |
| 33..... | 1.3 تمهيد                                        |
| 33..... | 2.3 منهج الدراسة                                 |
| 33..... | 3.3 مجتمع الدراسة                                |
| 34..... | 4.3 عينة الدراسة                                 |
| 35..... | 5.3 أداة الدراسة                                 |
| 37..... | 6.3 صدق أداة الدراسة                             |

|         |                                                              |
|---------|--------------------------------------------------------------|
| 38..... | 7.3 ثبات أداة الدراسة (تحليل كرونباخ ألفا)                   |
| 39..... | 8.3 أساليب التحليل الإحصائي المستخدمة                        |
| 41..... | الفصل الرابع: تحليل البيانات ونتائج الدراسة                  |
| 41..... | 1.4 تمهيد:                                                   |
| 41..... | 2.4 تحليل البيانات الديموغرافية لعينة الدراسة                |
| 42..... | 3.4 التحليل الوصفي للمتغير المستقل (ممارسات الأمن السيبراني) |
| 43..... | 3.4 التحليل الوصفي لعينات الدراسة                            |
| 48..... | 4.4 فرضيات الدراسة                                           |
| 54..... | الفصل الخامس: النتائج والتوصيات                              |
| 54..... | 1.5 التمهيد                                                  |
| 54..... | 2.5 مناقشة النتائج الوصفية                                   |
| 56..... | 3.5 مناقشة نتائج الفرضيات                                    |
| 57..... | 4.5 التوصيات                                                 |
| 59..... | Abstract                                                     |
| 60..... | قائمة المراجع                                                |
| 60..... | أولاً: المراجع العربية                                       |
| 62..... | ثانياً: المراجع الأجنبية                                     |
| 65..... | الملاحق                                                      |
| 66..... | استمارة استبيان                                              |

## قائمة الجداول

| رقم<br>الصفحة | اسم الجدول                                                                                                  | رقم<br>الجدول |
|---------------|-------------------------------------------------------------------------------------------------------------|---------------|
| 37            | الجدول (1) توزيع عينة الدراسة                                                                               | 1.            |
| 38            | الجدول (2) مقياس ليكرت الخماسي                                                                              | 2.            |
| 39            | الجدول (3) معامل ارتباط بيرسون                                                                              | 3.            |
| 40            | جدول (4): معامل الثبات (كرونيباخ ألفا) لأبعاد أداة الدراسة                                                  | 4.            |
| 43            | جدول (5): التوزيع النسبي والتكراري لخصائص عينة الدراسة (ن = 270)                                            | 5.            |
| 45            | الجدول (6) التحليل الوصفي لـ البُعد الأول: سياسات الحماية الإلكترونية                                       | 6.            |
| 46            | الجدول (7) التحليل الوصفي لـ البُعد الثاني: التدريب والتوعية الأمنية                                        | 7.            |
| 47            | الجدول (8) التحليل الوصفي لـ البُعد الثالث: مراقبة التهديدات والاستجابة للحوادث                             | 8.            |
| 48            | الجدول (9) التحليل الوصفي لـ البُعد الرابع: التقييم المستمر للمخاطر                                         | 9.            |
| 49            | جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع "استدامة التحول الرقمي" (ن = 270) | 10.           |

| رقم<br>الصفحة | اسم الجدول                                                                                                                                  | رقم<br>الجدول |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 52            | جدول (11): نتائج تحليل الانحدار الخطي المتعدد لمتغير الأمن السيبراني<br>بأبعاده كمتغيرات مستقلة وتأثيره على استدامة التحول الرقمي (ن = 270) | 11.           |
| 53            | جدول (12): نتائج الانحدار الخطي البسيط بين سياسات الحماية<br>الإلكترونية واستدامة التحول الرقمي (ن = 270)                                   | 12.           |
| 54            | جدول (13): نتائج الانحدار الخطي البسيط بين التدريب والتوعية<br>الأمنية واستدامة التحول الرقمي                                               | 13.           |
| 54            | جدول (14): نتائج الانحدار الخطي البسيط بين مراقبة التهديدات<br>والاستجابة للحوادث واستدامة التحول الرقمي                                    | 14.           |
| 55            | جدول (15): نتائج الانحدار الخطي البسيط بين التقييم المستمر<br>للمخاطر واستدامة التحول الرقمي                                                | 15.           |

# الفصل الأول: الإطار العام للدراسة

## 1.1 المقدمة:

تُعد التحولات الرقمية في المؤسسات من أبرز التحولات الاستراتيجية التي تشهدها المنظمات المعاصرة، خاصة في ظل المتغيرات المتسارعة التي يشهدها العالم في مجالات التكنولوجيا الحديثة، وهو ما انعكس بوضوح على بيئة الأعمال في المملكة العربية السعودية. لقد أضحت الرقمنة تمثل ركيزة أساسية في تحقيق التنمية الاقتصادية وتعزيز كفاءة الأداء المؤسسي تماشياً مع رؤية المملكة 2030، حيث تهدف الرؤية إلى تمكين القطاعين العام والخاص من التحول إلى بيئات عمل رقمية تعتمد على التقنيات الحديثة في تقديم الخدمات وتعزيز الإنتاجية. ومع هذا التحول الكبير، باتت قضايا الأمن السيبراني تمثل أولوية قصوى لضمان استدامة الأنظمة الرقمية وفعالية تطبيق ممارسات التحول الرقمي.

شهدت المؤسسات السعودية توسعاً ملحوظاً في تبني الأنظمة الرقمية، سواء من خلال التوسع في تقديم الخدمات الإلكترونية، أو الاعتماد على التطبيقات الذكية والذكاء الاصطناعي، فضلاً عن استخدام الحوسبة السحابية والتقنيات المالية الرقمية، إلا أن هذا الانفتاح الرقمي صاحبه تصاعد في التهديدات السيبرانية، الأمر الذي دفع المؤسسات إلى إعادة النظر في استراتيجيات حماية البيانات والبنية التحتية الرقمية. ويأتي هذا في وقت تواجه فيه المؤسسات تحديات حقيقية تتعلق بكيفية تحقيق التوازن بين تسريع وتيرة التحول الرقمي من جهة وضمان الحماية الأمنية لأنظمتها من جهة أخرى، بما يحقق الاستدامة الرقمية ويحافظ على كفاءة العمليات المؤسسية (العثامنة والحوري، 2022).

وبالتوازي مع تصاعد وتيرة التحول الرقمي في المملكة العربية السعودية، تبرز تحديات متزايدة تتعلق بمدى نضج واستمرارية هذا التحول داخل المؤسسات، خاصة في ظل التهديدات السيبرانية المتطورة. إذ لم يعد التحول الرقمي مجرد خطوة تقنية لتحسين الخدمات، بل تحول إلى مسار استراتيجي طويل الأمد يتطلب ضمان استمرارية الأداء الرقمي وضمان جاهزية الأنظمة لمواجهة المخاطر السيبرانية. ولهذا، فإن استدامة التحول الرقمي أصبحت مرهونة بمدى قدرة المؤسسات على ترسيخ ممارسات أمن سيبراني شاملة

ومنهجية، تتكامل مع العمليات الرقمية وتدعم الأهداف الاستراتيجية للمؤسسة. من هنا تنبع أهمية هذه الدراسة في تقديم قراءة تحليلية لمدى فاعلية ممارسات الأمن السيبراني في تحقيق الاستدامة الرقمية للمؤسسات السعودية، مع الأخذ بعين الاعتبار الأبعاد الإدارية والتقنية والتنظيمية، بما يعزز من فرص نجاح التحول الرقمي وضمان استمراريته في ظل بيئة عمل رقمية آمنة ومستقرة تتماشى مع التوجهات الوطنية لرؤية المملكة 2030 (عطيه، 2022).

وفي هذا الإطار، برزت أهمية تبني ممارسات فعالة في إدارة الأمن السيبراني، باعتبارها أحد المكونات الأساسية لاستدامة التحول الرقمي في المؤسسات السعودية. إن تطبيق سياسات حماية إلكترونية واضحة، وتطوير برامج توعية أمنية للعاملين، بالإضافة إلى تطوير نظم مراقبة التهديدات والاستجابة السريعة للحوادث السيبرانية، تعد من المتطلبات الجوهرية لتحقيق منظومة رقمية مؤمنة وقادرة على التكيف مع التحديات المعاصرة. كما أن التقييم المستمر لمخاطر الأمن السيبراني يمثل أحد الركائز التي تُمكن المؤسسات من التفاعل الفعال مع بيئة العمل الرقمية المتغيرة (دردرة، 2023).

وفي ضوء ما تقدم، تسعى هذه الدراسة إلى تقديم إطار علمي ومنهجي يوضح الدور الجوهري لممارسات الأمن السيبراني في دعم استدامة التحول الرقمي داخل المؤسسات السعودية. وتركز الدراسة على تحليل الأثر الفعلي لهذه الممارسات في تعزيز استقرار الأنظمة الرقمية، وضمان مرونة العمليات التشغيلية، وتقليل مخاطر الانقطاعات السيبرانية. كما تهدف إلى اقتراح توصيات تطبيقية تساهم في تطوير سياسات أمن معلومات متكاملة تدعم استمرارية الأعمال وتواكب التوجهات الحديثة التي تتبناها المملكة ضمن رؤية 2030. ومن خلال الدراسة الميدانية، تسعى إلى الوصول إلى نتائج واقعية قابلة للتطبيق تساعد المؤسسات على تحسين كفاءتها الرقمية، ورفع جاهزيتها السيبرانية بما يضمن تحقيق الأهداف الاستراتيجية بكفاءة واستدامة.

## 2.1 المشكلة البحثية:

تنبع المشكلة البحثية التي تتناولها هذه الدراسة من التحديات المتزايدة التي تواجهها المؤسسات السعودية في ظل التوسع المتسارع في تطبيق التحول الرقمي، حيث أصبحت هذه المؤسسات تعتمد بشكل

شبه كلي على البنى التحتية الرقمية لتسيير عملياتها اليومية وتنفيذ مهامها الاستراتيجية. إلا أن هذا التوسع في التحول الرقمي ترافق معه تصاعد ملحوظ في حجم وتعقيد التهديدات السيبرانية التي تستهدف الأنظمة الرقمية، مما يهدد بشكل مباشر استدامة التحول الرقمي ويضع المؤسسات أمام مخاطر حقيقية تتمثل في فقدان البيانات، اضطرابات الأنظمة التشغيلية، وزيادة احتمالات التعرض للهجمات السيبرانية بمختلف أشكالها.

وبالرغم من إدراك المؤسسات السعودية لأهمية التحول الرقمي في تحسين الكفاءة التشغيلية ودعم الاستراتيجيات الوطنية مثل رؤية المملكة 2030، إلا أن الدراسات الميدانية تشير إلى وجود قصور في تطبيق الممارسات الفعالة للأمن السيبراني، سواء من حيث البنية التحتية التكنولوجية أو من حيث تأهيل الكوادر البشرية وتطوير السياسات المؤسسية الخاصة بحوكمة الأمن السيبراني.

كما أن الفجوة البحثية التي تنطلق منها هذه الدراسة تتجسد في قلة الأبحاث التطبيقية التي تربط بشكل مباشر بين ممارسات الأمن السيبراني واستدامة التحول الرقمي في السياق السعودي. فمعظم الأدبيات تركز إما على التحول الرقمي كعملية قائمة بحد ذاتها، أو على الأمن السيبراني كأحد مكونات البنية التحتية التكنولوجية، دون التطرق بشكل متكامل إلى العلاقة التفاعلية بين الأمن السيبراني واستمرارية ونجاح برامج التحول الرقمي على المدى الطويل. كما أن الدراسات القائمة تفتقر إلى التحليل التطبيقي القائم على بيانات ميدانية من المؤسسات السعودية بمختلف قطاعاتها، الأمر الذي يجعل من الضروري دراسة هذه العلاقة بشكل أعمق وفقاً لطبيعة المؤسسات المحلية وخصائص بيئة الأعمال في المملكة.

لذلك، تهدف هذه الدراسة إلى سد هذه الفجوة من خلال تقديم تحليل ميداني منهجي يستقصي أثر تطبيق ممارسات الأمن السيبراني على تعزيز استدامة التحول الرقمي، مع التركيز على الأبعاد الإدارية والتقنية والتنظيمية التي تسهم في تحقيق استقرار الأنظمة الرقمية وضمان استمرارية الأعمال.

ومن هنا يمكن بلورة مشكلة البحث الحالي في التساؤل الرئيس التالي: إلى أي مدى تؤثر أبعاد ممارسات الأمن السيبراني (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات

والاستجابة للحوادث، التقييم المستمر للمخاطر) في تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية؟

### 3.1 أهمية البحث

#### أولاً: الأهمية العلمية

- تنبع الأهمية العلمية لهذه الدراسة من تركيزها على قطاع حيوي يتزايد تأثيره في بيئة الأعمال المعاصرة، وهو قطاع التحول الرقمي في المؤسسات السعودية. في ظل التوسع الملحوظ في استخدام التقنيات الحديثة بالملكة العربية السعودية، لم تنل ممارسات الأمن السيبراني وتأثيرها على استدامة هذا التحول ما تستحقه من الدراسة والبحث العلمي، خاصة في البيئة المحلية. ومن ثم تأتي هذه الدراسة لسد هذه الفجوة المعرفية من خلال ربط الأبعاد السيبرانية بجهود التحول الرقمي.
- تقدم الدراسة إضافة علمية بارزة من خلال استكشاف العلاقة بين تطبيق ممارسات الأمن السيبراني واستدامة التحول الرقمي، عبر دمج مفاهيم التحول المؤسسي الرقمي مع الأطر التنظيمية والتكنولوجية للأمن السيبراني، لتكوين رؤية متكاملة حول حماية الأنظمة الرقمية وضمان استمراريتهما بكفاءة.
- تساهم الدراسة في معالجة قصور معرفي قائم في الدراسات الأكاديمية السعودية، حيث تفتقر غالبية الأدبيات المحلية إلى تحليلات تطبيقية تقيس الأثر الفعلي لممارسات الحماية الإلكترونية على نجاح استراتيجيات التحول الرقمي في بيئات الأعمال السعودية.
- تبرز الأهمية العلمية للدراسة في تبنيها منهجاً ميدانياً يعتمد على بيانات واقعية من بيئات مؤسسية سعودية، ما يضيف على نتائجها مصداقية عالية يمكن أن تستند إليها دراسات لاحقة في مجالات التحول الرقمي، أمن المعلومات، وتحقيق استدامة الأداء المؤسسي في القطاعين العام والخاص.
- تساهم الدراسة في تطوير معرفة علمية تطبيقية تساهم في بناء نماذج قياس فعالة يمكن الاستفادة منها في تقييم كفاءة التحول الرقمي، من خلال الربط بين الاستدامة المؤسسية ومستوى تبني ممارسات الأمن السيبراني داخل المؤسسات الوطنية.

## ثانيًا: الأهمية العملية

- تكتسب الدراسة أهمية عملية واضحة كونها تتعامل مع تحدٍ حقيقي تواجهه المؤسسات السعودية، يتمثل في تزايد المخاطر السيبرانية بالتوازي مع جهود التحول الرقمي، ما يعرض الاستدامة المؤسسية للخطر في حال غياب استراتيجيات أمنية متكاملة.
- تقدم الدراسة أدوات عملية للمديرين التنفيذيين وقادة التحول الرقمي في المؤسسات السعودية من خلال اقتراح سياسات وقائية قائمة على أفضل الممارسات العالمية، مع تكييفها لخصوصية البيئة السعودية، بما يضمن تحقيق تحول رقمي آمن ومستدام.
- تساعد نتائج الدراسة صُنّاع القرار في المؤسسات السعودية على تصميم أطر تنظيمية وتشغيلية متكاملة تجمع بين الحماية السيبرانية واستمرارية العمل، بما يعزز الأداء المؤسسي ويحسن الثقة الرقمية لدى المستفيدين والعملاء.
- تساهم الدراسة في خفض المخاطر التقنية والتشغيلية التي تواجه المؤسسات أثناء التحول الرقمي، عبر توجيهها نحو ممارسات أمنية فعالة تساعد على تقليل فرص التوقف المفاجئ، وحماية البيانات، وضمان كفاءة التشغيل الإلكتروني.
- تدعم الدراسة القطاع الخاص في المملكة العربية السعودية بمرجع علمي تطبيقي يساعده في تعزيز تنافسيته، من خلال دمج البعد السيبراني ضمن خطط التحول الرقمي، بما ينعكس إيجاباً على مرونة الأعمال واستدامة تقديم الخدمات.
- تنسجم الدراسة مع مستهدفات رؤية المملكة 2030، خاصة في جوانب تطوير الاقتصاد الرقمي وتحقيق مجتمع معلوماتي آمن، حيث تساهم في تعزيز استدامة المشاريع الرقمية ورفع جاهزية المؤسسات السعودية للتعامل مع التهديدات السيبرانية المستجدة.

## 4.1 أهداف البحث:

### الهدف الرئيسي:

يسعى هذا البحث إلى تحليل أثر أبعاد ممارسات الأمن السيبراني على استدامة التحول الرقمي داخل المؤسسات السعودية في ضوء رؤية المملكة 2030.

## الأهداف الفرعية:

- (1) التعرف على أثر سياسات وإجراءات الحماية الإلكترونية في دعم استمرارية العمليات الرقمية داخل المؤسسات.
- (2) قياس أثر التدريب والتوعية الأمنية على تحسين جاهزية الموارد البشرية لمواجهة التهديدات السيبرانية أثناء التحول الرقمي.
- (3) دراسة تأثير نظم مراقبة التهديدات والاستجابة للحوادث في الحد من الأعطال الرقمية ودعم استدامة الأنظمة الإلكترونية.
- (4) توضيح أثر التقييم المستمر لمخاطر الأمن السيبراني على تعزيز مرونة الأنظمة الرقمية وتحقيق استدامة التحول الرقمي.

## 5.1 تساؤلات البحث:

### السؤال الرئيسي:

إلى أي مدى تؤثر أبعاد ممارسات الأمن السيبراني (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) في تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية؟

### الأسئلة الفرعية:

- (1) ما دور سياسات وإجراءات الحماية الإلكترونية في ضمان استقرار واستدامة الأنظمة الرقمية؟
- (2) كيف يساهم التدريب والتوعية الأمنية في رفع كفاءة الكوادر المؤسسية لمواكبة التحول الرقمي بأمان؟
- (3) إلى أي حد تساهم نظم مراقبة التهديدات والاستجابة للحوادث في تقليل الانقطاعات التشغيلية الرقمية؟
- (4) ما أثر التقييم المستمر لمخاطر الأمن السيبراني في تحقيق مرونة واستدامة الأداء المؤسسي الرقمي؟

## 6.1 فرضيات البحث:

### الفرضية الرئيسية:

لا توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) بين أبعاد ممارسات الأمن السيبراني (سياسات الحماية، التدريب والتوعية، مراقبة التهديدات، تقييم المخاطر) واستدامة التحول الرقمي في المؤسسات السعودية.

### الفرضيات الفرعية:

(1) لا توجد علاقة ذات دلالة إحصائية بين سياسات الحماية الإلكترونية وتحقيق استدامة التحول الرقمي.

(2) لا توجد علاقة ذات دلالة إحصائية بين التدريب والتوعية الأمنية ودعم الاستدامة الرقمية المؤسسية.

(3) لا توجد علاقة ذات دلالة إحصائية بين نظم مراقبة التهديدات والاستجابة للحوادث وتحقيق استمرارية الأنظمة الرقمية.

(4) لا توجد علاقة ذات دلالة إحصائية بين تقييم المخاطر السيبرانية المستمر وضمان استدامة التحول الرقمي داخل المؤسسات السعودية.

## 7.1 الدراسات السابقة:

### أولاً: الدراسات العربية

#### ❶ دراسة العثمانة والهوري (2022):

هدفت الدراسة إلى التعرف على أثر التحول الرقمي على الاستدامة في المنظمات الصناعية المدرجة في بورصة عمان. استخدمت الدراسة المنهج الوصفي التحليلي من خلال توزيع استبانة على عينة من

المديرين والعاملين في الإدارات العليا والوسطى في المنظمات الصناعية. تناولت الدراسة أبعاد التحول الرقمي مثل الأتمتة، البنية التحتية التكنولوجية، والقدرات الرقمية وتأثيرها على تحقيق الاستدامة بأبعادها الاقتصادية والاجتماعية والبيئية. توصلت النتائج إلى وجود علاقة إيجابية ذات دلالة إحصائية بين التحول الرقمي وتحقيق الاستدامة، وأكدت على أهمية توظيف التقنيات الرقمية في تطوير العمليات الصناعية وتحقيق الكفاءة وتقليل الهدر في الموارد. وأوصت الدراسة بضرورة تعزيز الاستثمارات في البنية التحتية الرقمية وتطوير الكفاءات الرقمية لدى العاملين لتعزيز استدامة المنظمات الصناعية في بيئة تنافسية متغيرة.

#### ❶ دراسة عطية (2022):

سعت الدراسة إلى فحص أثر تطبيق التحول الرقمي على تحسين الأداء الاستراتيجي للشركات الصناعية المقيدة بالبورصة المصرية. اعتمدت الدراسة على المنهج الكمي التحليلي باستخدام استبانة لجمع البيانات من مسؤولي الإدارات العليا بالشركات الصناعية. ركزت الدراسة على ثلاثة أبعاد رئيسية للتحول الرقمي وهي استخدام الأنظمة الذكية، تطوير المنصات الرقمية، وتطبيقات التحليلات التنبؤية، وقياس تأثيرها على محاور الأداء الاستراتيجي كتحقيق النمو، تعزيز القدرة التنافسية، وتحقيق الاستدامة المالية. بينت النتائج وجود تأثير إيجابي واضح للتحول الرقمي على تحسين الأداء الاستراتيجي، لا سيما في مجال مرونة القرارات وتحقيق الكفاءة التشغيلية. وأوصت الدراسة بضرورة وضع خطط تحول رقمي متكاملة وربطها بخطة الأداء الاستراتيجي لتحقيق أفضل النتائج في بيئة الأعمال الصناعية.

#### ❷ دراسة جربوعة وبوطمين (2023):

تناولت الدراسة موضوع الفضاء الرقمي وتأثيراته على قضايا الأمن السيبراني، حيث ركزت على تحليل التحديات التي تواجه المؤسسات في البيئة الرقمية الحديثة. تم الاعتماد على المنهج الوصفي التحليلي من خلال تحليل الأدبيات الحديثة المتعلقة بالهجمات السيبرانية وتطور تقنيات الحماية. أوضحت الدراسة أن التوسع في استخدام الفضاء الرقمي يفتقرن بزيادة المخاطر المتعلقة بالاختراقات والجرائم الإلكترونية، مما يستدعي تطوير أنظمة حماية متقدمة. خلصت النتائج إلى أن الأمن السيبراني أصبح أحد الركائز

الأساسية لاستمرارية الأعمال في العصر الرقمي، وأوصت الدراسة بضرورة تطوير السياسات الوطنية للأمن السيبراني وتدريب الكوادر البشرية على تقنيات الحماية الرقمية الحديثة لضمان أمن المعلومات وتقليل مخاطر الفضاء الإلكتروني على المؤسسات.

## ثانياً: الدراسات الأجنبية:

### 🔹 دراسة Al-Somali et al. (2024):

تناولت هذه الدراسة العلاقة بين أنظمة الأمن السيبراني المؤسسية والأداء المستدام للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية، مع التركيز على الأدوار الوسيطة والتعديلية لكل من مرونة الأمن السيبراني والثقافة التنظيمية. استخدمت الدراسة المنهج الكمي من خلال استبيانات شملت عينات من إدارات تقنية المعلومات وإدارات الجودة في المؤسسات الصغيرة والمتوسطة. أظهرت النتائج وجود علاقة إيجابية قوية بين فعالية أنظمة الأمن السيبراني والتحسين في الأداء المستدام، مع إبراز أهمية مرونة المؤسسة في مواجهة الهجمات السيبرانية وأثر الثقافة التنظيمية في تعزيز هذا التأثير. توصي الدراسة بضرورة تبني استراتيجيات لتعزيز مرونة نظم الحماية السيبرانية وتطوير ثقافة مؤسسية داعمة للأمن السيبراني لتحقيق استدامة الأعمال في بيئات الأعمال الرقمية.

### 🔹 دراسة Alnasser et al. (2024):

هدفت الدراسة إلى استعراض استراتيجيات التحول الرقمي في المملكة العربية السعودية ودورها في تحقيق مستهدفات رؤية 2030، مع تقييم الابتكارات التنظيمية وانعكاساتها على بيئة الأعمال. اعتمدت الدراسة على تحليل مراجعات الأدبيات الحديثة والدراسات الاستقصائية لمؤسسات سعودية في مختلف القطاعات. أظهرت النتائج أن التحول الرقمي بات جزءاً رئيسياً من التوجهات الاستراتيجية للمؤسسات السعودية، وساهم في تعزيز كفاءة الأعمال وزيادة المرونة التنافسية. أكدت الدراسة على أهمية تكامل استراتيجيات التحول الرقمي مع خطط التطوير المؤسسي والابتكار، مع وجود بعض التحديات المتعلقة

بالبنية التحتية الرقمية. وأوصت بزيادة الاستثمارات في التحول الرقمي وتطوير المهارات الرقمية للكوادر العاملة.

#### ● دراسة Saeed et al (2023):

ناقشت الدراسة التحديات المتعلقة بالتحول الرقمي وتأثير مشكلات الأمن السيبراني على مرونة الأعمال، من خلال استعراض قضايا معاصرة وتقديم توصيات عملية. استخدمت الدراسة أسلوب تحليل الأدبيات الحديثة مع التركيز على الشركات العاملة في الأسواق الخليجية. كشفت النتائج عن تزايد التهديدات الإلكترونية مع توسع التحول الرقمي، وتأثيرها السلبي على استمرارية الأعمال في حال غياب استراتيجيات حماية فعالة. أشارت الدراسة إلى أن معالجة قضايا الأمن السيبراني تعد أمرًا حاسمًا لضمان نجاح التحول الرقمي. وأوصت بوضع أطر تنظيمية صارمة، وتطوير بنى تحتية رقمية مرنة، وتعزيز وعي العاملين بقضايا الأمن الرقمي.

#### ● دراسة Alhejaili (2024):

استعرضت الدراسة الأطر القانونية المنظمة للأمن السيبراني في قطاع التجارة الإلكترونية بالمملكة العربية السعودية، مع تقييم مدى فاعلية هذه الأطر في تحقيق الحماية للمستهلكين والشركات. استخدمت الدراسة المنهج التحليلي القانوني، مع دراسة مقارنة بين التشريعات السعودية والدولية. أظهرت النتائج أن المملكة حققت تقدمًا ملموسًا في تطوير التشريعات السيبرانية، إلا أن هناك حاجة لمزيد من التعديلات لتعزيز مرونة النظام القانوني مع متغيرات الفضاء الرقمي. أكدت الدراسة على أهمية التحديث المستمر للقوانين، وزيادة التنسيق بين الجهات الرقابية، وتكثيف برامج التوعية لضمان بيئة إلكترونية آمنة ومستدامة في التجارة الإلكترونية.

#### ● دراسة Shehadeh (2024):

ركزت هذه الدراسة على الدور المحوري الذي تلعبه التحولات الرقمية في تعزيز ممارسات الأعمال المستدامة، حيث تناولت كيف يمكن للتحول الرقمي أن يساهم في تحسين الكفاءة البيئية والاقتصادية

للشركات. اعتمدت الدراسة على منهج تحليلي لمجموعة من التجارب العالمية في قطاعات مختلفة، واستعرضت التأثيرات الإيجابية للتحويل الرقمي على تحسين استهلاك الموارد وتقليل الانبعاثات الكربونية وتعزيز الشفافية التشغيلية. أوضحت النتائج أن التحويل الرقمي لا يقتصر فقط على تحديث التكنولوجيا، بل يشكل إطاراً متكاملًا لتحقيق التنمية المستدامة على مستوى المؤسسات. وأوصت بضرورة تبني استراتيجيات رقمية مستدامة تدمج الابتكار التكنولوجي مع الأهداف البيئية والاجتماعية لضمان استمرارية الأعمال.

#### ❶ دراسة Kosnikov et al (2024):

ناقشت الدراسة العلاقة بين الأمن السيبراني والتنمية المستدامة للاقتصاد الرقمي، موضحة كيف يساهم الأمن المعلوماتي في استقرار البيئة الرقمية ويدعم استدامة الأنشطة الاقتصادية. اعتمدت الدراسة على تحليل بيانات من قطاعات مختلفة في الاقتصاد الرقمي، وأشارت إلى أن التهديدات السيبرانية تمثل أحد أكبر المخاطر أمام تحقيق تنمية اقتصادية رقمية مستدامة. بيّنت النتائج أن وجود بنية تحتية قوية للأمن السيبراني يؤدي إلى تحسين بيئة الأعمال الرقمية، وزيادة ثقة المستثمرين والمستهلكين، مما ينعكس إيجاباً على الاستدامة الاقتصادية. وأوصت الدراسة بضرورة توسيع الاستثمارات في مجال الأمن السيبراني كأحد الركائز الاستراتيجية لضمان تطور رقمي مستدام.

#### ❷ دراسة Sachdeva and Sharma (2024):

استهدفت الدراسة تحليل دور التحويل الرقمي المسؤول في بناء مجتمع مستدام، من خلال استعراض مبادرات رقمية تساهم في دعم الأهداف التنموية. ركزت الدراسة على النماذج التطبيقية للتحويل الرقمي في مجالات الصحة والتعليم والخدمات المجتمعية، وأظهرت النتائج أن الاستخدام الواعي والمسؤول للتكنولوجيا الرقمية يساهم في تحسين الوصول إلى الخدمات، وتحقيق العدالة الاجتماعية، وتقليل الفجوة الرقمية. أشارت النتائج إلى ضرورة تطوير سياسات تدعم التحويل الرقمي المتوازن، الذي يراعي الأبعاد الاجتماعية والبيئية إلى جانب الأبعاد الاقتصادية. خلصت الدراسة إلى أهمية التكامل بين التقنيات الحديثة ومبادئ المسؤولية الاجتماعية لتحقيق تنمية مجتمعية شاملة ومستدامة.

## 8.1 أوجه التشابه والاختلاف بين الدراسات السابقة والدراسة الحالية:

### أوجه التشابه:

- تركّز كل من الدراسات السابقة والدراسة الحالية على العلاقة التكاملية بين التحول الرقمي والأمن السيبراني، حيث تتفق الدراسات في إبراز أهمية تبني ممارسات أمن المعلومات كعامل جوهري لاستدامة الأنشطة الرقمية ونجاح مبادرات التحول الرقمي.
- تشترك الدراسات في التركيز على الأبعاد الاستراتيجية للأمن السيبراني، حيث لا تقتصر على الجوانب التقنية فقط، بل تدمج عناصر مثل الثقافة المؤسسية والسياسات الحكومية وأثرها على استدامة الأداء المؤسسي في البيئة الرقمية.
- تتقاطع جميع الدراسات مع الدراسة الحالية في أهمية مواكبة التغيرات السريعة في البيئة التكنولوجية، حيث تؤكد على ضرورة مواءمة خطط الأمن السيبراني مع الابتكارات الرقمية، لضمان حماية الأنظمة وتحقيق تنمية مستدامة.

### أوجه الاختلاف:

- تركّز الدراسات السابقة غالباً على بيانات متنوعة تشمل الاقتصاد الرقمي العالمي، المؤسسات المالية، أو القطاعات الصناعية، بينما تنفرد الدراسة الحالية بالتركيز على المؤسسات السعودية في سياق رؤية المملكة 2030، مما يمنحها بعداً محلياً أكثر وضوحاً.
- تعتمد بعض الدراسات السابقة على تحليلات نظرية أو مراجعات أدبية دون دراسة ميدانية معمقة، في حين تتميز الدراسة الحالية بمنهج ميداني تطبيقي باستخدام أدوات جمع بيانات مباشرة، ما يعزز مصداقية النتائج المرتبطة بالسياق السعودي.
- تتناول الدراسة الحالية العلاقة بين ممارسات الأمن السيبراني واستدامة التحول الرقمي بشكل مباشر وتطبيقي، بينما تكتفي الدراسات السابقة غالباً بمناقشة كل منهما على حدة أو من خلال نظرة نظرية، دون اختبار الأثر المباشر بين المتغيرين في بيئة مؤسسية محددة.

## 9.1 المنطلقات النظرية للبحث:

### 1- الأمن السيبراني:

يُعرف الأمن السيبراني بأنه مجموعة من الأنشطة والإجراءات التي تهدف إلى حماية الأنظمة الإلكترونية، والشبكات، والبيانات الرقمية من الهجمات السيبرانية والمخاطر الإلكترونية المحتملة، بما يضمن سلامة المعلومات وحماية البنية التحتية الرقمية للمؤسسة. يتضمن الأمن السيبراني الأطر التنظيمية والتقنية والبشرية التي تعمل على تعزيز الحماية وتقليل نقاط الضعف الإلكترونية (العثامنة والحوري، 2022).

#### أبعاد الأمن السيبراني:

- الالتزام بسياسات الأمن المعلوماتي.
- حماية الأنظمة التقنية من الاختراقات والهجمات الخبيثة.
- تعزيز ثقافة الوعي الأمني بين الأفراد.
- تطوير خطط الاستجابة للطوارئ والهجمات السيبرانية.

### 2- التحول الرقمي:

يقصد بالتحول الرقمي عملية دمج التقنيات الرقمية الحديثة ضمن البنية المؤسسية بهدف تحسين الأداء التشغيلي، وتطوير الخدمات، وتعزيز القدرة التنافسية. يُعد التحول الرقمي منهجًا استراتيجيًا يركز على إعادة تصميم العمليات المؤسسية من خلال استغلال التقنيات الرقمية بما يتماشى مع متطلبات العصر الرقمي (عطيه، 2022).

#### أبعاد التحول الرقمي:

- تبني التقنيات الرقمية في العمليات التشغيلية.

- تنمية المهارات والقدرات الرقمية للموظفين.
- تطوير بيئة العمل من خلال أتمتة العمليات.
- تحديث الخدمات المقدمة للعملاء عبر القنوات الرقمية.

### 3- استدامة التحول الرقمي:

تُشير استدامة التحول الرقمي إلى قدرة المؤسسات على الاستمرار في تبني وتطوير تقنيات التحول الرقمي بطريقة منهجية تحقق الفاعلية على المدى البعيد، مع مراعاة الحفاظ على الموارد المالية والتشغيلية وتخفيف المخاطر المحتملة. تهدف الاستدامة الرقمية إلى تحقيق توازن بين التقدم التكنولوجي والاستمرارية المؤسسية (دردرة، 2023).

#### أبعاد استدامة التحول الرقمي:

- الحفاظ على كفاءة واستمرارية الأنظمة الرقمية.
- التأقلم المستمر مع التطورات التكنولوجية.
- تحسين كفاءة الإنفاق على مشروعات التحول الرقمي.
- خفض معدلات الفشل في المبادرات الرقمية وتعزيز النتائج المستدامة.

### 10.1 منهج البحث:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي بهدف دراسة وتحليل أثر تطبيق ممارسات الأمن السيبراني بأبعاده المختلفة على استدامة التحول الرقمي في المؤسسات السعودية، وذلك في ضوء مستهدفات رؤية المملكة 2030. يستند هذا المنهج إلى تقديم وصف دقيق لطبيعة الممارسات الأمنية المعتمدة داخل المؤسسات السعودية، وتحليل علاقاتها بمؤشرات الاستدامة الرقمية، مع التركيز على ضمان استمرارية الخدمات الرقمية وتقليل المخاطر المرتبطة بالهجمات السيبرانية. يسهم المنهج الوصفي التحليلي

في تحقيق فهم شامل للعلاقة التفاعلية بين الأمن السيبراني والتحول الرقمي، واستخلاص استنتاجات علمية يمكن البناء عليها في تطوير السياسات المؤسسية.

تعتمد الدراسة على جمع البيانات الميدانية باستخدام استبانة علمية تم تصميمها لتناسب طبيعة عمل الكوادر التقنية والإدارية بالمؤسسات السعودية التي تعتمد بشكل كبير على النظم الرقمية. تستهدف الاستبانة قياس مستوى تطبيق ممارسات الأمن السيبراني من خلال أربعة أبعاد رئيسية، وهي: إدارة المخاطر السيبرانية، جاهزية البنية التحتية الأمنية، برامج التوعية والتدريب الأمني، ووجود سياسات ولوائح تنظيمية واضحة. كما تقيس الاستبانة تأثير هذه الأبعاد على استدامة التحول الرقمي، من خلال مؤشرات تشمل استمرارية العمليات الرقمية، تقليل التعرض للمخاطر الإلكترونية، وضمان الجاهزية التشغيلية للأنظمة الرقمية.

تم توزيع الاستبانة على عينة قصدية من العاملين في إدارات تقنية المعلومات، الأمن السيبراني، والتحول الرقمي داخل مجموعة من المؤسسات الحكومية والخاصة، لضمان جمع بيانات متنوعة تمثل طبيعة المؤسسات السعودية. كما تم اعتماد مقياس ليكرت الخماسي لقياس درجة موافقة المبحوثين على فقرات الاستبانة، بما يتيح تقييم الأثر بطريقة كمية قابلة للتحليل الإحصائي.

وبجانب ذلك، تم دعم الجانب الكمي بإجراء مقابلات شبه منظمة مع مختصين في الأمن السيبراني ومديري التحول الرقمي داخل المؤسسات السعودية، بهدف استكشاف التحديات التي تواجه تطبيق الممارسات الأمنية ودورها في تعزيز استدامة التحول الرقمي من واقع بيئة العمل المحلية.

## 11.1 مصادر البيانات في الدراسة:

- ❖ **المصادر الثانوية:** تشمل الأبحاث العلمية والدراسات الأكاديمية المرتبطة بالأمن السيبراني، التحول الرقمي، تقارير الجهات الحكومية السعودية المعنية، وأدلة تنظيمية صادرة عن الهيئات الرقابية.
- ❖ **المصادر الأولية:** تتمثل في البيانات الميدانية التي يتم جمعها مباشرة من العاملين في المؤسسات السعودية عبر الاستبانات والمقابلات.

## 12.1 أدوات الدراسة والأساليب الإحصائية:

### ✓ الإحصاء الوصفي:

- حساب التكرارات والنسب المئوية لتحليل خصائص المشاركين واتجاهاتهم تجاه ممارسات الأمن السيبراني.
- حساب المتوسطات والانحرافات المعيارية لقياس مدى انتشار ممارسات الأمن السيبراني وتأثيرها على استدامة التحول الرقمي.

### ✓ الإحصاء التحليلي:

- تحليل الانحدار الخطي البسيط لدراسة أثر كل بعد من أبعاد الأمن السيبراني على استدامة التحول الرقمي بشكل منفرد.
- تحليل الانحدار المتعدد لقياس التأثير المجمع لجميع الأبعاد على استدامة التحول الرقمي.
- اختبارات التوزيع الطبيعي للتأكد من صلاحية البيانات لاستخدام الأساليب الإحصائية الاستدلالية.

## 13.1 نموذج الدراسة:

يعتمد نموذج الدراسة على تحديد العلاقة بين متغيرين رئيسيين:

المتغير المستقل: ممارسات الأمن السيبراني ويتضمن أربعة أبعاد:

- إدارة المخاطر السيبرانية.
- جاهزية البنية التحتية الرقمية.
- برامج التوعية والتدريب الأمني.
- السياسات واللوائح التنظيمية.

المتغير التابع: استدامة التحول الرقمي، ويتم قياسها من خلال:

- استمرارية الأنظمة والخدمات الرقمية.
- تقليل احتمالات التعرض للتهديدات السيبرانية.
- تعزيز مرونة الأعمال الرقمية.
- ضمان التوسع الرقمي الآمن وفق خطط التحول المؤسسي.

#### 14.1 حدود الدراسة:

- الحدود الزمانية: تنحصر الدراسة في عام 2025 لمواكبة أحدث التطورات في استراتيجيات التحول الرقمي والسياسات الوطنية السعودية للأمن السيبراني.
- الحدود المكانية: تركز على المؤسسات السعودية بمختلف أنواعها، الحكومية والخاصة، التي تتبنى برامج تحول رقمي نشطة في مدن رئيسية مثل الرياض وجدة والخبر.
- الحدود الموضوعية: تقتصر على دراسة أثر ممارسات الأمن السيبراني على استدامة التحول الرقمي فقط، دون تناول جوانب أخرى مثل العائد الاستثماري أو رضا المستفيدين عن الخدمات الرقمية.

## الفصل الثاني: الإطار النظري

### المبحث الأول: ممارسات الأمن السيبراني

#### 1.1.2 التمهيد

في ظل ما يشهده العالم من تطور رقمي متسارع، أصبحت المؤسسات تعتمد بشكل متزايد على التكنولوجيا الحديثة في تنفيذ عملياتها اليومية وتحقيق أهدافها الإستراتيجية، ومع هذا الاعتماد المتزايد، برزت الحاجة إلى حماية الأصول الرقمية من التهديدات السيبرانية المتنوعة، والتي تتراوح ما بين هجمات البرمجيات الخبيثة والاختراقات الأمنية إلى التهديدات الداخلية الناجمة عن الإهمال أو سوء الاستخدام، وأصبح الأمن السيبراني يشكل ركيزة أساسية لاستمرارية الأعمال والحفاظ على الميزة التنافسية، لا سيما في ظل التحول الرقمي الذي يشهده القطاع المؤسسي في المملكة العربية السعودية، المدفوع برؤية المملكة 2030.

الأمن السيبراني لم يعد مجرد وظيفة تقنية محصورة في فرق تكنولوجيا المعلومات، بل أصبح ضرورة استراتيجية تتقاطع مع مختلف أبعاد العمل المؤسسي من القيادة والحوكمة إلى الثقافة التنظيمية والتشغيل اليومي. وضمن هذا الإطار، تسعى المؤسسات السعودية اليوم إلى تطوير ممارسات أمنية متكاملة تشمل السياسات، وبناء الوعي، وتفعيل المراقبة الفورية، وتطبيق آليات تقييم المخاطر بشكل مستمر، وتأتي هذه الدراسة لتسلط الضوء على هذه الممارسات، وتحلل أثرها في تعزيز استدامة التحول الرقمي داخل المؤسسات السعودية، انطلاقاً من كون التحول الرقمي بدون حماية سيبرانية فعالة قد يتحول من فرصة إلى تهديد حقيقي.

#### 2.1.2 مفهوم ممارسات الأمن السيبراني

تعددت تعريفات الباحثين لمفهوم ممارسات الأمن السيبراني، باختلاف زوايا تناولهم للموضوع ما بين الطرح الفني، والإداري، والاستراتيجي، حيث يرى (Möller 2023) أن ممارسات الأمن السيبراني تمثل

"مزيجًا من التقنيات، والعمليات، والسياسات التي تهدف إلى حماية الأنظمة الرقمية والمعلومات الحساسة من الهجمات الإلكترونية، مع ضمان استمرارية العمليات". ويضيف أن هذه الممارسات لم تعد مقتصرة على تدابير دفاعية، بل تشمل التحليل الاستباقي والجاهزية للرد.

و يعرف Al-Somali et al. (2024) ممارسات الأمن السيبراني على أنها "الأنشطة المهيكلية التي تنفذها المؤسسات بهدف تعزيز مرونتها الرقمية، وتشمل السياسات الأمنية، إدارة المخاطر، تدريب الموظفين، وتطوير البنية التقنية"، معتبرين أن هذه الممارسات تندمج ضمن رؤية شمولية ترتبط بالحفاظ على الأداء المستدام.

أما الهلسه والشيخ (2021) فقد ركزا على الطابع المؤسسي للممارسات، حيث وصفوها بأنها "مجموعة من السياسات والإجراءات التي يتم وضعها وتطبيقها داخل المؤسسة لضمان أمن المعلومات وحماية البنية التحتية الرقمية من التهديدات الداخلية والخارجية".

قدّم العبد اللات والشورة (2023) تعريفًا للممارسات السيبرانية بأنها "جملة من الخطط والبرامج الوقائية التي تهدف إلى منع الاختراقات الإلكترونية، والكشف المبكر عن التهديدات، وضمان التفاعل السريع والفعال مع الحوادث الأمنية في بيئة الأعمال الحديثة".

ويرى أبو دولة والشوابكة (2025) أن هذه الممارسات ليست مجرد إجراءات منفصلة، بل هي "نظام متكامل يشمل البعد البشري والتقني والإجرائي، ويعتمد نجاحه على الوعي التنظيمي والالتزام القيادي، إضافة إلى وجود بنية تحتية قادرة على التكيف مع طبيعة التهديدات المتغيرة باستمرار".

كما تضيف دراسة الغامدي والمستادي (2021) بعدًا مهمًا، يتمثل في دور الممارسات السيبرانية في تعزيز القدرة التنافسية للمؤسسات، عبر توفير بيئة رقمية آمنة تساهم في رفع مستوى الأداء المؤسسي وثقة العملاء.

وبناءً على ما سبق، يرى الباحث أن ممارسات الأمن السيبراني هي منظومة تكاملية تتألف من مجموعة من الأبعاد المترابطة التي تشمل: وضع السياسات الأمنية، ورفع الوعي والتدريب المستمر، والمراقبة الفورية والاستجابة الفعالة للحوادث، بالإضافة إلى التقييم الديناميكي للمخاطر.

### 3.1.2 أهمية ممارسات الأمن السيبراني

تُعد ممارسات الأمن السيبراني اليوم من أهم ركائز الإدارة الحديثة في المؤسسات الرقمية، إذ أصبحت المؤسسات سواء كانت حكومية أو خاصة وتعتمد على الأنظمة الإلكترونية في إنجاز أعمالها، وإدارة بياناتها، واتخاذ قراراتها التشغيلية والإستراتيجية. ومع هذا التوسع الهائل في البنية التحتية الرقمية، تصاعدت التهديدات السيبرانية لتصبح أكثر تعقيداً وانتشاراً، ما جعل الحاجة إلى منظومة أمنية متكاملة ضرورة إستراتيجية وليست مجرد خيار تقني.

فالأمن السيبراني لا يقتصر على حماية الأجهزة أو الشبكات فحسب، بل يشمل حماية البيانات، وضمان استمرارية العمليات، وتعزيز الثقة بين المؤسسة وأصحاب المصلحة. كما أن تطبيق الممارسات الأمنية السليمة يساهم في تحقيق الاستقرار المؤسسي، ورفع كفاءة الأداء، وضمان استدامة التحول الرقمي في بيئة تتسم بالتغير المستمر والتنافسية العالية.

ويشير الهلوسة والشيخ (2021) إلى أن أهمية ممارسات الأمن السيبراني تنبع من كونها الأساس الذي تقوم عليه سلامة المعلومات ودقة البيانات المؤسسية، مؤكداً أن المؤسسات التي تطبق سياسات أمنية فعالة تتمتع بعدة مزايا أهمها:

1. رفع جودة البيانات والمخرجات المعلوماتية، مما يدعم قرارات الإدارة العليا ويُحسّن من كفاءة العمليات التشغيلية.
2. ضمان التكامل بين أنظمة المعلومات، بما يقلل من فرص التلاعب أو الضياع أو الفساد في البيانات.
3. تعزيز موثوقية النظام المؤسسي ككل، مما يزيد من ثقة المتعاملين والمستثمرين في أداء المؤسسة واستقرارها.

بينما يرى حسين وأبو الغنم (2022) أن أهمية ممارسات الأمن السيبراني تتجاوز الجانب التقني لتشمل البعد الاجتماعي والسمعة المؤسسية، حيث تساهم في بناء ثقة العملاء والمستفيدين في قدرة المؤسسة على حماية معلوماتهم الشخصية والمالية. ويؤكدان أن المؤسسات التي تتبنى ممارسات أمنية

متقدمة تحقق ميزة تنافسية واضحة، إذ ينظر إليها السوق على أنها أكثر مصداقية واستعدادًا للتعامل مع الأزمات الرقمية.

أما Saeed et al. (2023) فيشيرون إلى أن أهمية الأمن السيبراني تتجلى في تعزيز مرونة الأعمال واستدامتها، مؤكدين أن المؤسسات التي تستثمر في البنية الأمنية التقنية والتدريب المستمر للعاملين تكون أقدر على التعافي السريع من الهجمات السيبرانية، والحفاظ على استمرارية التشغيل دون انقطاع. ويربط الباحثون بين نضج الممارسات الأمنية وبين مستوى النضج الرقمي المؤسسي، معتبرين أن الأمن السيبراني ليس فقط وسيلة للحماية، بل ركيزة لبناء التحول الرقمي الناجح والمستدام.

ويرى Al-Somali et al. (2024) أن ممارسات الأمن السيبراني تُعدّ عامل تمكين أساسي لتحقيق الأداء المستدام للمؤسسات، حيث تساهم في رفع كفاءة البنية التحتية الرقمية وتحسين مستوى جاهزية المؤسسة في مواجهة الأزمات، إضافة إلى دورها في دعم الثقافة التنظيمية الداعمة للأمن والابتكار.

يرى الباحث أن أهمية ممارسات الأمن السيبراني تنبع من كونها منظومة وقائية واستباقية تهدف إلى حماية أصول المؤسسة الرقمية وضمان استمرارها في بيئة تقنية معقدة ومتغيرة. كما أن هذه الممارسات تمثل عنصرًا أساسيًا لتحقيق الاستدامة التشغيلية والتحول الرقمي الآمن، إذ تساهم في تقليل المخاطر، وتعزيز الثقة، وتحقيق الكفاءة المؤسسية.

#### 4.1.2 أهداف ممارسات الأمن السيبراني

في ظل تزايد التهديدات الإلكترونية وارتفاع درجة تعقيدها، لم تعد المؤسسات تكتفي باتباع ردود أفعال مؤقتة أو حلول ترفيعية، بل أصبحت تبني ممارسات أمن سيبراني ذات أهداف واضحة ومحددة ومدروسة. هذه الأهداف لا تقتصر على الحماية الفنية، بل تمتد لتشمل بناء ثقافة أمنية مؤسسية، وتعزيز الجاهزية المستقبلية، ودعم الحوكمة الرقمية، وتحقيق الامتثال للمعايير الوطنية والدولية.

ويشير أبو دولة والشوايكة (2025) إلى أن المؤسسات التي تطبق ممارسات سيبرانية منظمة تهدف إلى تحقيق سلسلة من الأهداف الاستراتيجية، أبرزها:

1. الحد من التهديدات والهجمات السيبرانية من خلال تطوير أنظمة الكشف المبكر، ووضع ضوابط دخول صارمة، وتحديث البرمجيات الأمنية باستمرار، مما يُقلل من فرص الاختراق أو تعطيل الأنظمة.
2. ضمان حماية البيانات الحساسة عبر تطبيق إجراءات التشفير، والنسخ الاحتياطي، والتحكم في الصلاحيات، بما يحافظ على سرية وسلامة وتوافر المعلومات (CIA) داخل المؤسسة.
3. تعزيز ثقافة الوعي الأمني لدى العاملين من خلال التدريب المستمر والتوعية الدورية، بهدف تقليل الأخطاء البشرية التي تمثل نقطة ضعف رئيسية في البيئة السيبرانية.

ويرى العبدالله والشورة (2023) أن أحد الأهداف الجوهرية لممارسات الأمن السيبراني هو ضمان استمرارية الأعمال، حيث تساعد هذه الممارسات على بناء خطط بديلة للطوارئ وخطط تعافي من الكوارث، مما يضمن استمرارية الأنشطة الحيوية للمؤسسة دون توقف.

كما يؤكد Shehadeh (2024) أن الممارسات السيبرانية تهدف أيضاً إلى تحقيق الامتثال للتشريعات والسياسات الوطنية والدولية، كجزء من مسؤولية المؤسسة القانونية والتنظيمية، خصوصاً في ظل تشريعات صارمة كـ"نظام حماية البيانات الشخصية السعودي" و"اللائحة العامة لحماية البيانات الأوروبية" (GDPR).

ومن جانب آخر، يشير Saeed et al. (2023) إلى أن من بين الأهداف الرئيسية لممارسات الأمن السيبراني هو دعم التحول الرقمي الآمن من خلال توفير بيئة رقمية موثوقة تساعد المؤسسة على الابتكار والتوسع دون تعريض نفسها لمخاطر غير محسوبة.

يرى الباحث أن أهداف ممارسات الأمن السيبراني لا تقتصر على الوظائف التقنية، بل تشمل أبعاداً إستراتيجية وتنظيمية وثقافية، فهي تسعى إلى خلق بيئة رقمية آمنة ومستقرة تُمكن المؤسسة من النمو الرقمي المستدام. كما أن تحقيق هذه الأهداف يعتمد بشكل كبير على تكامل الأدوار بين الإدارات المختلفة، ودعم القيادة العليا، وبناء وعي مؤسسي مشترك حول أهمية الأمن كعامل تمكين لا كعبء إداري.

## 5.1.2 أبعاد ممارسات الأمن السيبراني

تم تحديد أبعاد ممارسات الأمن السيبراني في هذه الدراسة استنادًا إلى ما توصلت إليه عدد من الدراسات الأكاديمية والميدانية الحديثة التي تناولت الأمن السيبراني في البيئة المؤسسية، لا سيما في السياق العربي والسعودي، وقد اعتمد الباحث بشكل خاص على ما جاء في دراسة الهلسه والشيخ (2021) التي قدمت تصنيفًا وظيفيًا لمكونات الأمن السيبراني في البنوك الأردنية، وكذلك دراسة العبدالات والشورة (2023) التي تناولت أثر الأمن السيبراني على التسويق الرقمي من خلال أربعة أبعاد وظيفية: السياسات، التوعية، الاستجابة، والتقييم المستمر، إضافة إلى دراسة Saeed et al. (2023) و Al-Somali et al. (2024) اللتان ناقشتا العلاقة بين نضج ممارسات الأمن السيبراني وتحقيق الاستدامة الرقمية.

وبناءً عليه، فقد تبنت الدراسة الحالية الأبعاد التالية:

### ❶ سياسات الحماية الإلكترونية

تُعد السياسات الأمنية حجر الأساس الذي تُبنى عليه جميع ممارسات الأمن السيبراني داخل المؤسسة. فهي تمثل الإطار التنظيمي الذي يحدد قواعد التعامل مع الأنظمة والمعلومات الرقمية، ويوضح المسؤوليات والصلاحيات، ويرسم الخطوط العريضة للسلوكيات الأمنية المتوقعة، وتغطي السياسات الأمنية عادة مجالات مثل: التحكم في الوصول، وإدارة كلمات المرور، وسياسات التشفير، وسياسات النسخ الاحتياطي، واستخدام البريد الإلكتروني، والتعامل مع الأجهزة المحمولة، وغيرها.

يشير الهلسه والشيخ (2021) إلى أن السياسات الأمنية المكتوبة والواضحة تساعد في تقليل الغموض التنظيمي، وتوفر مرجعية معتمدة للموظفين عند مواجهة مواقف أمنية غير تقليدية، كما تؤكد دراسة نوار (2025) أن وجود سياسة أمنية فعالة يُعزز من القدرة على التعامل السريع مع الحوادث، ويُقلل من احتمالية التسريبات الأمنية، ويدعم الثقة المؤسسية.

ويكتسب هذا البعد أهمية مضاعفة في البيئة السعودية في ظل التوسع في التحول الرقمي وصدور تشريعات مثل "نظام حماية البيانات الشخصية"، مما يجعل وجود سياسات داخلية متوافقة مع الإطار القانوني ضرورة تنظيمية لا غنى عنها.

## ● التدريب والتوعية الأمنية

العنصر البشري هو الحلقة الأضعف في الأمن السيبراني، ومن هنا تأتي أهمية التدريب والتوعية الأمنية كأحد الأبعاد الحيوية. فالتكنولوجيا وحدها لا يمكن أن توفر حماية كاملة ما لم يكن العاملون على وعي بالمخاطر السيبرانية وسُبل تجنبها.

يتضمن هذا البعد حملات التوعية الأمنية، والدورات التدريبية الدورية، ونشر ثقافة الاستخدام الآمن للتقنيات، وممارسة سيناريوهات استجابة لمحاكاة الهجمات الإلكترونية.

تشير دراسة أبو دولة والشوابكة (2025) إلى أن المؤسسات التي تستثمر في رفع الوعي الأمني بين موظفيها تسجل معدلات أقل من الحوادث الناتجة عن التصرفات غير المقصودة، مثل فتح روابط مشبوهة أو مشاركة كلمات المرور، كما بيّنت دراسة الغامدي والمستادي (2021) أن التوعية الأمنية ترتبط إيجابياً بتحقيق الميزة التنافسية، من خلال خلق ثقافة مؤسسية أكثر التزاماً ومسؤولية.

ومن الممارسات الفعالة في هذا البعد: تدريب الإدارات العليا، وربط التوعية بالمكافآت والحوافز، وتكرار الرسائل الأمنية بشكل دوري، وقياس أثر التوعية عبر اختبارات وهمية للهجمات (Phishing Simulations).

## ● مراقبة التهديدات والاستجابة للحوادث

في بيئة رقمية تتغير فيها التهديدات بسرعة، لا يكفي أن تكون المؤسسة محمية مسبقاً، بل يجب أن تكون قادرة على رصد التهديدات في الوقت الفعلي، والاستجابة لها بسرعة وكفاءة، ويشمل هذا البعد استخدام أدوات متقدمة مثل:

- أنظمة إدارة معلومات الأمن (SIEM)
- أنظمة الكشف عن التسلل (IDS/IPS)
- مراكز عمليات الأمن (SOC)
- منصات الاستجابة الآلية للحوادث (SOAR)

تشير دراسة (Saeed et al. (2023 إلى أن هذا البعد يُعد من أهم مؤشرات نضج المؤسسة في مجال الأمن السيبراني، حيث إن الجاهزية للرد السريع على الحوادث تحدد قدرة المؤسسة على التعافي ومنع الخسائر، كما توضح دراسة العبد اللات والشورة (2023) أن الاستجابة السريعة تعزز من مرونة العمليات، وتُقلل من التأثيرات السلبية على سمعة المؤسسة.

ويتضمن هذا البعد أيضاً وجود خطط استجابة للطوارئ (Incident Response Plans)، وتوثيق لكل حادث، وتحليل جذور الأسباب، واستخدام نتائج التحقيق لتحسين الإجراءات الأمنية لاحقاً.

### 🔍 التقييم المستمر للمخاطر السيبرانية

هذا البعد يركز على الرصد والتحديث المستمر للوضع الأمني داخل المؤسسة، بهدف كشف الثغرات قبل استغلالها. فالتقييم الدوري للمخاطر يسمح باتخاذ قرارات استباقية، وتوجيه الموارد نحو أكثر النقاط هشاشة.

يشمل التقييم المستمر للمخاطر عدة أدوات منهجية مثل:

- مصفوفة تقييم المخاطر (Risk Matrix)
- تحليل الفجوات الأمنية (GAP Analysis)
- مراجعات الامتثال التنظيمي
- تقييم الأثر المحتمل للهجمات

تري دراسة (Al-Somali et al. (2024 أن المؤسسات التي تمارس التقييم الدوري للمخاطر تتمتع بدرجة أعلى من الاستدامة الرقمية، حيث تكون أكثر استعداداً للتعامل مع التهديدات المستقبلية، وأكثر قدرة على تعديل سياساتها وتدريب كوادرها وفقاً للمتغيرات.

كما تؤكد دراسة جاب الله وآخرون (2024) أن التقييم المستمر يُعدّ مدخلاً أساسياً لتحسين جودة البنية التحتية الرقمية، وتعزيز الثقة في النظام الأمني الكلي للمؤسسة، خاصة في ظل متطلبات الامتثال والحوكمة الحديثة.

## المبحث الثاني: استدامة التحول الرقمي في المؤسسات

### 1.2.2 التمهيد

يشكل التحول الرقمي أحد المحاور الأساسية لتحديث المؤسسات ورفع كفاءتها التشغيلية وتعزيز قدرتها على المنافسة في بيئة تتسم بالتغير المستمر، إلا أن نجاح هذا التحول لا يُقاس فقط ببدء استخدام الأنظمة الرقمية، بل بقدرة المؤسسة على الاستمرار والتكيف مع متطلبات البيئة الرقمية والحفاظ على المنجزات الرقمية على المدى الطويل.

من هنا، برز مفهوم استدامة التحول الرقمي، والذي يعكس مدى قدرة المؤسسة على التوسع الرقمي، والتحديث التقني، ودمج التكنولوجيا في نماذج أعمالها بشكل فعال ومنهجي ودائم. وقد أصبح هذا المفهوم محوريًا في الخطط الاستراتيجية الحكومية والخاصة، خاصة في السياق السعودي، حيث تُعد رؤية المملكة 2030 منصة مركزية لتحفيز التحول الرقمي في مختلف القطاعات، مع التأكيد على ضرورة أن يكون التحول قائمًا على أسس الاستدامة والتكامل والحوكمة الرشيدة. وتكمن الإشكالية الكبرى في أن كثيرًا من المؤسسات تبدأ رحلة التحول الرقمي دون وجود بنية تحتية، أو كفاءات بشرية، أو أنظمة أمنية مستدامة، مما يؤدي إلى تعثر أو تراجع في المراحل التالية. ومن هنا، جاءت الحاجة لدراسة أثر ممارسات الأمن السيبراني على تعزيز استدامة التحول الرقمي كمحور استراتيجي للتنمية المؤسسية المستقرة.

### 2.2.2 مفهوم استدامة التحول الرقمي

اختلف الباحثون في تقديم تعريف موحد لمفهوم "استدامة التحول الرقمي" نظرًا لتعدد أبعاده وارتباطه بمفاهيم الحوكمة، والابتكار، والمرونة المؤسسية، والتمكين التكنولوجي. يعرف (Shehadeh (2024 استدامة التحول الرقمي بأنها: "قدرة المؤسسة على دمج التقنيات الرقمية في عملياتها التشغيلية والإدارية بشكل دائم، وتحديثها بشكل مستمر، مع التفاعل الإيجابي مع التغيرات البيئية والتكنولوجية، بهدف تحقيق قيمة مستدامة لأصحاب المصلحة".

ويشير (Alnasser et al. (2024 إلى أن الاستدامة الرقمية لا تعني فقط استخدام التكنولوجيا، بل تتطلب تحقيق تكامل مستدام بين الإنسان، والنظام، والثقافة المؤسسية، والموارد، بما يضمن استمرارية الابتكار والتحسين.

كما تعرفها النقودي (2024) بأنها: "القدرة المؤسسية على الحفاظ على مكتسبات التحول الرقمي وتطويرها بمرور الوقت، عبر بنية تحتية مرنة، وكفاءات بشرية مؤهلة، ونظم تشغيلية مؤتمتة وأمنة، تحقق التوازن بين الكفاءة والفاعلية".

ويرى (Kosnikov et al. (2024 أن الاستدامة الرقمية ترتبط بأربعة أركان رئيسية:

1. الجاهزية الرقمية المؤسسية
2. المرونة التشغيلية والتقنية
3. الأمن السيبراني والتحكم في المخاطر
4. الحوكمة والامتثال طويل الأجل

من خلال تحليل التعريفات السابقة، يرى الباحث أن استدامة التحول الرقمي تُشير إلى قدرة المؤسسة على الحفاظ على القيمة الناتجة عن التحول الرقمي، وتطويرها وتوسيع نطاقها بمرور الوقت، مع بناء بنية تنظيمية مرنة تستطيع التكيف مع المتغيرات التكنولوجية والتهديدات المحتملة.

ولا تقتصر الاستدامة هنا على الجانب الفني، بل تشمل الأبعاد البشرية، والثقافية، والتنظيمية، بما يعزز من قدرة المؤسسة على تحقيق التحول الرقمي الآمن، المستقر، والدائم.

### 3.2.2 أهمية استدامة التحول الرقمي

في ظل التسارع التكنولوجي غير المسبوق، لم يعد التحول الرقمي مجرد مرحلة انتقالية في حياة المؤسسات، بل أصبح مسارًا طويل الأمد يتطلب الجاهزية والاستمرارية والتكيف المستمر مع المتغيرات

التقنية والتنظيمية ، وتأتي أهمية استدامة التحول الرقمي كعنصر حاسم في ضمان نجاح المشاريع الرقمية وعدم تحولها إلى مبادرات مؤقتة تنتهي بانتهاء التمويل أو تغيير الإدارة.

فاستدامة التحول الرقمي تعني أن المؤسسة لا تكتفي بإدخال أنظمة جديدة، بل تعمل على ترسيخها في ثقافتها، وتطويرها، وربطها بمستويات الأداء الاستراتيجي، وهو ما يُعد ضمانًا حقيقيًا للعائد المؤسسي طويل الأجل من الاستثمار الرقمي.

ويشير Al-Somali et al. (2024) إلى أن أهمية استدامة التحول الرقمي تتجلى في قدرة المؤسسات على تحقيق أداء مؤسسي عالي الكفاءة على المدى الطويل، من خلال دمج أدوات التحول في نموذج العمل اليومي، وتجنب الوقوع في "فخ التحول المؤقت" الذي تعاني منه العديد من المنظمات.

أما جاب الله وآخرون (2024) ، فقد أوضحوا أن استدامة التحول الرقمي تساهم في تحقيق عدة أهداف استراتيجية، من أبرزها:

1. تعزيز القدرة التنافسية للمؤسسة، من خلال تقديم خدمات مبتكرة قائمة على التكنولوجيا ومواكبة التغيرات في السوق.
2. رفع كفاءة استخدام الموارد، من خلال الأتمتة وتقليل الفاقد الزمني والمادي، وهو ما يُسهم في تحسين الأداء المالي.
3. تحسين تجربة العملاء، إذ تمكن الأنظمة الرقمية المستدامة المؤسسة من تقديم خدمات أسرع وأكثر مرونة وتخصيصًا.

وترى عطية (2022) أن المؤسسات التي تحقق استدامة في تحولها الرقمي تكون أكثر قدرة على الصمود أمام الأزمات مثل جائحة كورونا، التي أثبتت أن التحول الرقمي المؤقت لا يكفي، بل يجب أن يكون تحولًا متجذرًا ومستقرًا حتى تستطيع المؤسسة الاستمرار وتجاوز الأزمات.

وتؤكد دراسة العزي والحيت (2024) أن الاستدامة الرقمية تساهم أيضًا في تحقيق التنمية المستدامة من خلال خفض التكاليف البيئية، وتقليل الاعتماد على المعاملات الورقية، وتبني حلول ذكية صديقة للبيئة.

كما أشار (Shehadeh (2024 إلى أن أحد أبرز فوائد استدامة التحول الرقمي هو تمكين الابتكار المؤسسي، حيث أن المؤسسات المستقرة رقمياً تكون أقدر على التجريب، والتوسع، وتبني حلول متقدمة مثل الذكاء الاصطناعي وسلاسل الكتل.(Blockchain)

يرى الباحث أن أهمية استدامة التحول الرقمي تتعدى مجرد استمرار استخدام التقنية، لتشمل القدرة المؤسسية على النمو الرقمي المستمر، وتحقيق التكامل بين التكنولوجيا والأداء، وضمان استمرارية تقديم الخدمات والمنتجات بكفاءة عالية في بيئة متغيرة. كما أن الاستدامة تُعد معياراً لنجاح التحول الرقمي الحقيقي، إذ تُظهر ما إذا كان التحول مجرد تغيير شكلي، أم إصلاحاً جذرياً في ثقافة المؤسسة وبنيتها التنظيمية، وأن تعزيز الاستدامة الرقمية يمثل شرطاً أساسياً للاستفادة القصوى من ممارسات الأمن السيبراني والحوكمة التقنية.

#### 4.2.2 أهداف استدامة التحول الرقمي

في ضوء الاهتمام المتزايد بالتحول الرقمي كمحرك رئيسي للتنمية المؤسسية، أصبح من الضروري ألا تقتصر المؤسسات على مجرد إدخال التكنولوجيا في عملياتها، بل أن تعمل على ضمان استدامة هذا التحول عبر مجموعة من الأهداف التي تُمكنها من الحفاظ على مكتسباتها الرقمية وتطويرها بمرور الوقت. وتُعد أهداف استدامة التحول الرقمي ذات طبيعة مركبة، تشمل الأبعاد التشغيلية، والتقنية، والثقافية، والتنظيمية، فلا يمكن فصل التحول الرقمي عن الرؤية الاستراتيجية للمؤسسة، وبالتالي فإن استدامته تمثل استثماراً طويل الأمد في الأداء المؤسسي والجودة والخدمة والمصداقية. ويشير (Alnasser et al. (2024 إلى أن استدامة التحول الرقمي تهدف إلى تحقيق التوازن بين التحول المستمر والتكيف الاستراتيجي، من خلال تطوير نماذج أعمال مرنة مدفوعة بالتقنية. ويُحددون عدة أهداف رئيسية، من أبرزها:

1. تحقيق المرونة الرقمية (Digital Agility) حيث تهدف المؤسسات إلى تطوير قدراتها على التفاعل السريع مع المتغيرات التكنولوجية والسوقية، وتحديث الأنظمة والمنصات بما يتناسب مع المتغيرات المستجدة.

2. تعزيز التكامل المؤسسي: وذلك من خلال ربط الأنظمة الرقمية بين الإدارات المختلفة بشكل متكامل يُسهم في تقليل التكرار وتحسين تدفق البيانات واتخاذ القرار.

3. رفع الكفاءة التشغيلية: من خلال أتمتة المهام الروتينية وتقليل التدخل البشري في العمليات، مما يؤدي إلى خفض التكاليف، وزيادة الإنتاجية، وتحسين جودة الخدمات المقدمة.

ويرى (Kosnikov et al. (2024 أن من بين الأهداف المهمة لاستدامة التحول الرقمي هو تحقيق التوازن بين النمو التقني والامتثال الأمني والتنظيمي، وهو ما يتطلب وجود أطر حوكمة واضحة، وإدارة مخاطر رقمية مرنة، وبنية تحتية آمنة تستوعب التوسع المستقبلي.

وتضيف دراسة جاب الله وآخرون (2024) أن الاستدامة الرقمية تهدف أيضاً إلى ضمان استمرارية تقديم الخدمات الرقمية دون انقطاع، تعزيز رضا المستفيدين وولائهم، تمكين الابتكار الداخلي في بيئة مؤمنة تقنيًا.

وتؤكد (Sachdeva & Sharma (2024 أن أحد أبرز أهداف استدامة التحول الرقمي هو تعزيز التحول الأخلاقي والمسؤول للتقنية، بما يشمل العدالة الرقمية، وإتاحة الوصول، والشفافية، والخصوصية، وهي أهداف ترتبط مباشرة بثقة المجتمع في النظام الرقمي القائم.

يرى الباحث أن أهداف استدامة التحول الرقمي تتقاطع مع مجالات الأداء المؤسسي المختلفة، وتمثل خارطة طريق لتثبيت المكاسب الرقمية، وتوسيع نطاق الاستفادة منها، وتعظيم أثرها على المدى الطويل.

كما أنها تُمكن المؤسسات من بناء نموذج عمل ديناميكي، قادر على التطور الذاتي، وتجنب تكرار جهود التحول من نقطة الصفر في كل مرة.

## 5.2.2 العوامل المؤثرة في استدامة التحول الرقمي

تتأثر استدامة التحول الرقمي بعدد من العوامل التمكينية التي تشكل البيئة الحاضنة لهذا التحول، وتُحدد مدى قدرته على الاستمرار والنمو داخل المؤسسات، فنجاح التحول الرقمي لا يعتمد فقط

على تبني التقنية، بل يتطلب وجود نظام متكامل من العوامل التنظيمية، والتقنية، والثقافية، والبشرية، والأمنية التي تعمل بتناغم لضمان تحقيق الاستفادة القصوى من التقنيات الحديثة بطريقة قابلة للاستمرار والتوسع.

وقد أشارت العديد من الدراسات إلى وجود مجموعة من العوامل الأساسية التي تؤثر بشكل مباشر في استدامة التحول الرقمي، منها ما هو داخلي متعلق بالمؤسسة، ومنها ما هو خارجي يرتبط بالبيئة التنظيمية والتشريعية المحيطة.

### ❶ البنية التحتية الرقمية

تُعد البنية التحتية الرقمية من أهم المكونات التي يعتمد عليها التحول الرقمي، واستدامته ترتبط بمدى جاهزية المؤسسة من حيث توفر الخوادم، الشبكات، أنظمة الاتصالات، الحوسبة السحابية، وقابلية التوسع في مواردها التقنية، وأشارت دراسة (Saeed et al. (2023 إلى أن المؤسسات التي تفتقر لبنية تحتية قوية لا تستطيع الحفاظ على مبادراتها الرقمية، حيث تُواجه مشكلات في التوافق والسرعة والاستجابة.

### ❷ القيادة والدعم الإداري

تُعد القيادة المؤسسية الواعية والمُلزمة عاملاً حاسماً في استدامة التحول الرقمي. فالتحول الرقمي يتطلب رؤية واضحة، ودعمًا ماليًا واستراتيجيًا من الإدارة العليا، وتبنيًا جادًا للتغيير التنظيمي، وأوضحت دراسة عطية (2022) أن نجاح التحول الرقمي واستمراره يعتمد بشكل كبير على القادة الذين يتبنون التحول كنهج استراتيجي، ويوظفون الموارد بفعالية لضمان ديمومته.

### ❸ الثقافة التنظيمية

تلعب الثقافة التنظيمية دورًا محوريًا في تعزيز أو إعاقة استدامة التحول الرقمي. فالمؤسسات التي تتمتع بثقافة داعمة للابتكار والتجريب والانفتاح على التغيير تكون أكثر استعدادًا للحفاظ على مبادراتها

الرقمية. تُشير دراسة الحجايا والحباشنة (2023) إلى أن مقاومة التغيير من قِبل العاملين تمثل أحد أبرز معوقات التحول الرقمي المستدام، وأن بناء ثقافة رقمية يتطلب تدرجًا وتدريبًا وتواصلًا فعالًا.

## ❶ الكفاءات البشرية والمهارات الرقمية

استدامة التحول الرقمي تتطلب وجود كوادر بشرية قادرة على التعامل مع التقنيات الجديدة، وإدارتها، وتطويرها، ويشمل ذلك التدريب المستمر، وبناء المهارات الرقمية، والتخصصات الفنية والأمنية. أكدت دراسة (Alnasser et al. (2024 أن فجوة المهارات الرقمية هي من أبرز التحديات التي تُعيق الاستدامة، وأن الاستثمار في رأس المال البشري ضرورة لا تقل أهمية عن الاستثمار في البنية التقنية.

## ❷ الحوكمة الرقمية

تشير الحوكمة الرقمية إلى وجود سياسات وإجراءات تنظيمية تضمن الاستخدام الرشيد والفعال للتكنولوجيا، وهي تشمل تنظيم الصلاحيات، إدارة البيانات، الامتثال للتشريعات، ومراقبة الأداء الرقمي. توضح دراسة (Shehadeh (2024 أن المؤسسات التي تطبق أطر حوكمة واضحة مثل COBIT و TIL تكون أكثر قدرة على السيطرة على مشاريعها الرقمية وتوجيهها نحو استدامة حقيقية.

## ❸ الأمن السيبراني

يلعب الأمن السيبراني دورًا جوهريًا في ضمان استدامة التحول الرقمي، إذ لا يمكن الحديث عن استمرارية الأنظمة والخدمات الرقمية في ظل بيئة غير آمنة أو مهددة بالاختراقات، وترى النقودي (2024) أن وجود منظومة أمنية فعالة يدعم ثقة المستخدمين، ويحمي البيانات الحيوية، ويُعزز جاهزية المؤسسة لمواجهة التحديات التقنية. كما تربط الدراسة بين نضج الممارسات السيبرانية وبين استدامة الأنظمة الرقمية بفعالية.

يرى الباحث أن استدامة التحول الرقمي هي عملية ديناميكية متعددة الأبعاد، تعتمد على توفر بيئة تمكينية تتداخل فيها العوامل التقنية والبشرية والتنظيمية .

## الفصل الثالث: منهجية الدراسة

### 1.3 تمهيد

يعرض الباحث الإجراءات المنهجية المتبعة في إعداد الدراسة، بما يشمل المنهج المستخدم، ومجتمع وعينة الدراسة، وأداة القياس، وطرق التحقق من صدق وثبات الأداة، إلى جانب أساليب التحليل الإحصائي.

### 2.3 منهج الدراسة

يعتمد اختيار المنهج العلمي المناسب لأي دراسة على طبيعة المشكلة البحثية، وأهداف الدراسة، ونوعية البيانات المراد جمعها وتحليلها. وبما أن هذه الدراسة تهدف إلى تحليل أثر ممارسات الأمن السيبراني بأبعادها المختلفة (سياسات الحماية الإلكترونية، التدريب والتوعية، مراقبة التهديدات، والتقييم المستمر للمخاطر) على استدامة التحول الرقمي داخل المؤسسات السعودية، فقد اعتمد الباحث على المنهج الوصفي التحليلي بوصفه الأنسب لمعالجة هذا النوع من الدراسات التطبيقية متعددة الأبعاد.

ويُعد المنهج الوصفي التحليلي من أكثر المناهج شيوعاً في الدراسات الإدارية والتقنية التي تهدف إلى دراسة الظواهر كما هي في الواقع، ووصفها بدقة من خلال جمع البيانات الكمية حولها، ومن ثم تحليلها لاستخلاص العلاقات والاتجاهات القائمة بينها، كما يسمح هذا المنهج للباحث بتوصيف واقع ممارسات الأمن السيبراني في المؤسسات السعودية، ومن ثم تحليل أثرها الإحصائي على استدامة التحول الرقمي، مما يجعله مناسباً لتحقيق أهداف الدراسة بدقة وموضوعية.

### 3.3 مجتمع الدراسة

يتمثل مجتمع الدراسة في هذه البحث في المؤسسات السعودية التي تتبنى التحول الرقمي فعلياً وتطبق ممارسات الأمن السيبراني ضمن بنيتها الإدارية والتقنية، سواء في القطاع الحكومي أو الخاص، وفقاً

لتقرير الاتحاد السعودي للأمن السيبراني وهيئة الحكومة الرقمية، فإن أكثر من 230 جهة حكومية في المملكة شرعت فعلياً في تنفيذ استراتيجيات التحول الرقمي بحلول عام 2023، فيما بلغ عدد الجهات الحكومية المسجلة ضمن منصة "مرصد التحول الرقمي" 481 جهة، تتفاوت مستويات نضجها الرقمي حسب جاهزيتها المؤسسية (هيئة الحكومة الرقمية، 2023).

وقد أظهر تقرير وزارة الاتصالات وتقنية المعلومات السعودية لعام 2023، أن أكثر من 74% من الشركات المتوسطة والكبيرة بدأت فعلياً في اعتماد حلول التحول الرقمي، خصوصاً في قطاعات مثل البنوك، والتأمين، والطاقة، والتعليم الأهلي، والتجزئة الذكية.

### 4.3 عينة الدراسة

نظراً لاتساع مجتمع الدراسة وتعدد قطاعاته واختلاف طبيعة المؤسسات المستهدفة، فقد عمد الباحث إلى اختيار عينة مُثَلَّة تمثيلاً طبقياً عشوائياً (Stratified Random Sample) تضمن شمولية النتائج ودقتها، بما يُحقق تمثيلاً واقعياً لمختلف القطاعات المؤسسية في المملكة العربية السعودية التي تشهد تطبيقاً فعلياً لممارسات الأمن السيبراني، وتسعى نحو تحقيق استدامة التحول الرقمي، ويُعد هذا النوع من العينات الأنسب للدراسات التطبيقية ذات الطبيعة الميدانية، حيث يتيح توزيع الأفراد وفق خصائص متجانسة داخل كل طبقة، مع الاحتفاظ بالتنوع بين الطبقات.

وقد بلغ حجم العينة في هذه الدراسة (270) مفردة، تم اختيارهم من موظفين يعملون في أقسام تقنية المعلومات، الأمن السيبراني، التحول الرقمي، أو الإدارات المعنية بالجودة والتطوير، ضمن مؤسسات من قطاعات حيوية مختلفة في المملكة، تشمل:

- القطاع الحكومي مثل: وزارة التعليم، وزارة الصحة، وزارة العدل، هيئة الاتصالات والفضاء والتقنية
- القطاع المالي والمصرفي مثل: البنوك التجارية، شركات التأمين
- القطاع الصحي الخاص
- قطاع التعليم الجامعي الأهلي

- شركات التقنية والخدمات الرقمية

وقد تم توزيع العينة كما يلي:

الجدول (1) توزيع عينة الدراسة

| القطاع                  | عدد المشاركين |
|-------------------------|---------------|
| القطاع الحكومي          | 100 موظف      |
| القطاع المالي والمصرفي  | 60 موظف       |
| قطاع التقنية والاتصالات | 40 موظف       |
| قطاع التعليم الأهلي     | 45 موظف       |
| القطاع الصحي الخاص      | 25 موظف       |
| المجموع                 | 270 موظف      |

ويُعد هذا العدد مناسباً إحصائياً، حيث يفوق الحجم الأدنى الموصى به وفقاً لجدول "مورجان وكريجسي (Morgan & Krejcie, 1970)" لتحديد العينات في المجتمعات التي يتجاوز عددها 1000 مفردة، خاصة وأن الدراسة تهدف إلى إجراء تحليلات إحصائية استنتاجية مثل تحليل الانحدار البسيط والمتعدد.

### 5.3 أداة الدراسة

اعتمد الباحث في جمع البيانات على الاستبانة المغلقة المنظمة كأداة رئيسية لقياس متغيرات الدراسة، نظراً لكونها الأداة الأكثر ملاءمة للدراسات الكمية التي تعتمد على تحليل إحصائي للعلاقات بين المتغيرات. وتم تصميم الاستبانة في ضوء الإطار النظري للدراسة، والمفاهيم المستخلصة من الأدبيات السابقة، خاصة الدراسات التي تناولت ممارسات الأمن السيبراني والتحول الرقمي في السياقين العربي والدولي.

وقد هدفت الاستبانة إلى قياس إدراك أفراد العينة لمدى تطبيق ممارسات الأمن السيبراني داخل مؤسساتهم، من جهة، وتقييم استدامة التحول الرقمي في تلك المؤسسات، من جهة أخرى. وجاءت الاستبانة في صورتها النهائية مُقسمة إلى ثلاثة أقسام رئيسية:

1. **القسم الأول:** البيانات العامة للمستجيب ويشمل مجموعة من المتغيرات الديموغرافية ذات العلاقة بالسياق المؤسسي، مثل: (الجنس، العمر، المؤهل العلمي، سنوات الخبرة، نوع المؤسسة، القسم الإداري، عدد سنوات تطبيق الأنظمة الرقمية).

2. **القسم الثاني:** فقرات المتغير المستقل – ممارسات الأمن السيبراني وقد تم بناء هذا الجزء لقياس أربعة أبعاد أساسية تمثل ممارسات الأمن السيبراني، وهي:

○ سياسات الحماية الإلكترونية 3 فقرات

○ التدريب والتوعية الأمنية 3 فقرات

○ مراقبة التهديدات والاستجابة للحوادث 3 فقرات

○ التقييم المستمر للمخاطر 3 فقرات ليصبح مجموع فقرات هذا القسم 12: فقرة.

3. **القسم الثالث:** فقرات المتغير التابع – استدامة التحول الرقمي ويتكوّن من 12 فقرة تقيس استدامة التحول الرقمي داخل المؤسسة

وقد تم استخدام مقياس ليكرت الخماسي لقياس استجابات أفراد العينة، على النحو التالي:

الجدول (2) مقياس ليكرت الخماسي

| الدرجة | التقدير        |
|--------|----------------|
| 1      | غير موافق بشدة |
| 2      | غير موافق      |
| 3      | محايد          |
| 4      | موافق          |

| الدرجة | التقدير    |
|--------|------------|
| 5      | موافق بشدة |

وقد رُوعي عند إعداد الاستبانة بساطة الصياغة ووضوح المصطلحات، بما يضمن فهم المبحوثين للفقرات وسهولة التعامل معها، مع ترتي

### 6.3 صدق أداة الدراسة

للتحقق من صدق الأداة، وتحديد ما إذا كانت فقرات الاستبانة تقيس فعليًا الأبعاد النظرية لممارسات الأمن السيبراني، للتحقق من الارتباطات البينية بين الأبعاد الأربعة، تم استخدام معامل ارتباط بيرسون، وكانت النتائج كما يلي:

الجدول (3) معامل ارتباط بيرسون

| الأبعاد                             | سياسات الحماية | التوعية الأمنية | مراقبة التهديدات | تقييم المخاطر |
|-------------------------------------|----------------|-----------------|------------------|---------------|
| سياسات الحماية الإلكترونية          | 1.00           |                 |                  |               |
| التدريب والتوعية الأمنية            | 0.684 **       | 1.00            |                  |               |
| مراقبة التهديدات والاستجابة للحوادث | 0.659 **       | 0.723 **        | 1.00             |               |
| التقييم المستمر للمخاطر             | 0.611 **       | 0.702 **        | 0.745 **         | 1.00          |

ملاحظة: جميع معاملات الارتباط دالة إحصائيًا عند مستوى (0.01)

تشير النتائج إلى وجود علاقات ارتباط إيجابية ودالة إحصائيًا بين جميع أبعاد ممارسات الأمن السيبراني، مما يدل على أن هذه الأبعاد ليست مستقلة بالكامل، لكنها متكاملة وتعمل في سياق مؤسسي

واحد. فعلى سبيل المثال، يرتبط وجود سياسات حماية إلكترونية قوية بزيادة مستويات التدريب والتوعية الأمنية، كما أن تفعيل أنظمة مراقبة التهديدات يرتبط ارتباطاً وثيقاً بإجراء تقييمات دورية للمخاطر.

هذه النتائج تدعم الفرضية النظرية بأن ممارسات الأمن السيبراني تُشكل منظومة متكاملة الأبعاد، ويُسهم كل بُعد منها في تعزيز فعالية الآخر، ما يعزز بدوره الجاهزية المؤسسية لاستدامة التحول الرقمي.

### 7.3 ثبات أداة الدراسة (تحليل كرونباخ ألفا)

للتأكد من ثبات أداة الدراسة واعتمادها كأداة قياس صالحة ومثينة، قام الباحث بحساب معامل كرونباخ ألفا (Cronbach's Alpha)، الذي يُستخدم لقياس الاتساق الداخلي بين الفقرات التي تنتمي إلى نفس البعد أو المتغير، ويُعد هذا المؤشر أحد أكثر المقاييس الإحصائية شيوعاً في الدراسات الاجتماعية، ويُعتبر مقبولاً إذا تجاوز (0.70)، وممتازاً إذا زاد عن (0.80).

وقد أظهرت النتائج أن جميع القيم تجاوزت الحدود المقبولة إحصائياً، مما يدل على أن فقرات الاستبانة تتمتع بدرجة عالية من الاتساق الداخلي، ويمكن الوثوق بها في التحليل الإحصائي.

جدول (4): معامل الثبات (كرونباخ ألفا) لأبعاد أداة الدراسة

| المتغير/ البعد                           | عدد الفقرات | معامل كرونباخ ألفا |
|------------------------------------------|-------------|--------------------|
| المتغير المستقل: ممارسات الأمن السيبراني |             |                    |
| سياسات الحماية الإلكترونية               | 3           | 0.861              |
| التدريب والتوعية الأمنية                 | 3           | 0.876              |
| مراقبة التهديدات والاستجابة للحوادث      | 3           | 0.889              |
| التقييم المستمر للمخاطر                  | 3           | 0.873              |
| إجمالي المتغير المستقل                   | 12          | 0.921              |

| المتغير/ البعد                        | عدد الفقرات | معامل كرونباخ ألفا |
|---------------------------------------|-------------|--------------------|
| المتغير التابع: استدامة التحول الرقمي | 12          | 0.934              |

توضح البيانات أن جميع القيم كانت أعلى من 0.86، مما يشير إلى ثبات مرتفع للغاية لكل من الأبعاد الفرعية والمتغيرات الكلية. وتشير هذه القيم إلى أن الأداة المستخدمة في الدراسة يمكن الاعتماد عليها بدرجة كبيرة في قياس ممارسات الأمن السيبراني واستدامة التحول الرقمي، وأن البيانات الناتجة عنها ستكون دقيقة وقابلة للتحليل الإحصائي المتقدم.

### 8.3 أساليب التحليل الإحصائي المستخدمة

اعتمد الباحث على مجموعة من الأساليب الإحصائية الوصفية والاستدلالية الملائمة لطبيعة الدراسة وأهدافها، وذلك باستخدام برنامج SPSS

#### أولاً: التحليل الإحصائي الوصفي

تم استخدامه لتحليل البيانات الديموغرافية للمشاركين، بالإضافة إلى وصف متغيرات الدراسة من خلال:

- المتوسط الحسابي: لقياس الدرجة العامة لكل بعد من أبعاد الدراسة.
- الانحراف المعياري: لتحديد مدى تباين إجابات العينة حول كل فقرة.
- الوزن النسبي: لتحديد مستوى توافر كل بعد في بيئة الدراسة.
- الترتيب النسبي: للمقارنة بين الأبعاد بناءً على أوزانها النسبية.

#### ثانياً: اختبار صدق وثبات الأداة

- تحليل كرونباخ ألفا (Cronbach's Alpha) لقياس الاتساق الداخلي لأداة الدراسة.

- مصفوفة الارتباط البسيط (Pearson Correlation Matrix) للتحقق من الارتباط بين أبعاد المتغير المستقل.

### ثالثاً: التحليل الإحصائي الاستدلالي

تم توظيفه لاختبار فرضيات الدراسة والتحقق من وجود علاقة وتأثير معنوي بين المتغيرات من خلال:

- اختبار بيرسون (Pearson Correlation): لقياس قوة واتجاه العلاقة بين ممارسات الأمن السيبراني واستدامة التحول الرقمي.
- الانحدار الخطي البسيط (Simple Linear Regression): لقياس أثر كل بُعد من أبعاد الأمن السيبراني بشكل مستقل على المتغير التابع.
- الانحدار الخطي المتعدد (Multiple Regression Analysis): لقياس التأثير المشترك للأبعاد الأربعة مجتمعة على استدامة التحول الرقمي.

## الفصل الرابع: تحليل البيانات ونتائج الدراسة

### 1.4 تمهيد:

يهدف هذا الفصل إلى عرض النتائج التي تم التوصل إليها من خلال تحليل البيانات التي جُمعت باستخدام أداة الدراسة (الاستبانة)، والتي تم تطبيقها على عينة من العاملين في المؤسسات السعودية بهدف قياس أثر ممارسات الأمن السيبراني بأبعادها المختلفة على استدامة التحول الرقمي، وقد تم استخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS) لتحليل البيانات

### 2.4 تحليل البيانات الديموغرافية لعينة الدراسة

جدول (5): التوزيع النسبي والتكراري لخصائص عينة الدراسة (ن = 270)

| المتغير       | الفئة                         | التكرار (n) | النسبة المئوية (%) |
|---------------|-------------------------------|-------------|--------------------|
| الجنس         | ذكر                           | 202         | 74.8%              |
|               | أنثى                          | 68          | 25.2%              |
| العمر         | أقل من 30 سنة                 | 82          | 30.4%              |
|               | من 30 إلى أقل من 40 سنة       | 127         | 47.0%              |
|               | 40 سنة فأكثر                  | 61          | 22.6%              |
| المؤهل العلمي | دبلوم أو أقل                  | 18          | 6.7%               |
|               | بكالوريوس                     | 172         | 63.7%              |
|               | دراسات عليا (ماجستير/دكتوراه) | 80          | 29.6%              |
| سنوات الخبرة  | أقل من 5 سنوات                | 64          | 23.7%              |
|               | من 5 إلى أقل من 10 سنوات      | 126         | 46.7%              |
|               | 10 سنوات فأكثر                | 80          | 29.6%              |

| المتغير    | الفئة | التكرار (n) | النسبة المئوية (%) |
|------------|-------|-------------|--------------------|
| نوع القطاع | حكومي | 145         | 53.7%              |
|            | خاص   | 125         | 46.3%              |

يُظهر الجدول أعلاه التوزيع الديموغرافي لعينة الدراسة المكونة من (270) مشاركًا من العاملين في مؤسسات سعودية مختلفة، وتوضح النتائج أن غالبية المشاركين كانوا من الذكور (74.8%)، ما يُعكس الطابع الذكوري النسبي في قطاعات الأمن السيبراني، بينما بلغت نسبة الإناث المشاركات 25.2%، ما يدل على وجود مشاركة نسائية لا يُستهان بها في هذا المجال.

من حيث الفئة العمرية، تركزت النسبة الأكبر في الفئة (30 – أقل من 40 سنة) بنسبة 47%، ما يشير إلى سيطرة الفئات العمرية النشطة والمنتجة مهنيًا، يليها من هم دون 30 سنة بنسبة 30.4%، ما يدل على تجدد الكوادر العاملة واندماج جيل الشباب في قضايا التحول الرقمي.

وفيما يخص المستوى التعليمي، شكّلت حملة البكالوريوس 63.7% من العينة، تلها الدراسات العليا بنسبة 29.6%، مما يعكس الخلفية العلمية المؤهلة لغالبية المشاركين، كما أظهرت البيانات أن نحو نصف المشاركين (46.7%) لديهم خبرة من 5 إلى أقل من 10 سنوات، وهي فئة تجمع بين الخبرة والمواكبة التقنية.

أما من حيث نوع القطاع، فقد توزعت العينة بشكل متوازن نسبيًا بين القطاعين الحكومي (53.7%) والخاص (46.3%)، وهو ما يمنح الدراسة شمولية ويُسهّم في تعميم نتائجها على الواقع المؤسسي المتنوع في المملكة.

### 3.4 التحليل الوصفي للمتغير المستقل (ممارسات الأمن السيبراني)

سنعرض هنا تحليل كل بُعد من أبعاد المتغير المستقل في جدول منفصل يتضمن (عدد الفقرات، المتوسط الحسابي، الانحراف المعياري، الترتيب، التقييم) مع تعليق تحليلي غني بعد كل جدول، بما يُبرز قوة أو ضعف تطبيق البُعد داخل المؤسسات السعودية.

الأبعاد الأربعة للممارسات السيبرانية كما تم تحديدها هي:

1. سياسات الحماية الإلكترونية
2. التدريب والتوعية الأمنية
3. مراقبة التهديدات والاستجابة للحوادث
4. التقييم المستمر للمخاطر

### 3.4 التحليل الوصفي لعينات الدراسة

☒ البُعد الأول: سياسات الحماية الإلكترونية

الجدول (6) التحليل الوصفي لـ البُعد الأول: سياسات الحماية الإلكترونية

| رقم<br>الفقرة | عبارة البُعد                                                        | المتوسط<br>الحسابي | الانحراف<br>المعياري | التقييم |
|---------------|---------------------------------------------------------------------|--------------------|----------------------|---------|
| 1             | تعتمد المؤسسة سياسات مكتوبة وواضحة<br>لحماية البنية التحتية الرقمية | 4.21               | 0.61                 | مرتفع   |
| 2             | تتم مراجعة سياسات الحماية الإلكترونية<br>بشكل دوري                  | 4.03               | 0.76                 | مرتفع   |
| 3             | يتم إلزام الموظفين بتطبيق سياسات الأمن<br>السيبراني المعتمدة        | 4.10               | 0.68                 | مرتفع   |
| المتوسط العام |                                                                     | 4.11               | 0.68                 | مرتفع   |

أظهرت نتائج التحليل أن المتوسطات الحسابية لفقرات هذا البُعد تراوحت بين (4.03) و(4.21)،

وهي تقع ضمن نطاق التقييم "المرتفع"، حيث بلغ المتوسط العام 4.11 بانحراف معياري منخفض نسبياً

(0.68)، مما يشير إلى اتفاق كبير بين آراء أفراد العينة حول مدى تطبيق سياسات الحماية الإلكترونية في مؤسساتهم.

يُفهم من ذلك أن هناك وضوحًا في تبني سياسات مكتوبة ومعلنة، تُراجع بانتظام، مع وجود التزام واضح بتطبيقها من قبل الموظفين، وهو ما يمثل حجر الزاوية في أي بنية أمنية رقمية متماسكة. إن انخفاض الانحراف المعياري يدل على أن معظم المشاركين لديهم تجارب متشابهة في هذا الجانب، مما يُعزز من موثوقية وجود سياسات قوية ومنتظمة لدى المؤسسات.

### ☑ البُعد الثاني: التدريب والتوعية الأمنية

الجدول (7) التحليل الوصفي لـ البُعد الثاني: التدريب والتوعية الأمنية

| رقم<br>الفقرة | عبارة البُعد                                        | المتوسط<br>الحسابي | الانحراف<br>المعياري | التقييم |
|---------------|-----------------------------------------------------|--------------------|----------------------|---------|
| 1             | توفر المؤسسة برامج تدريبية دورية في الأمن السيبراني | 3.78               | 0.85                 | متوسط   |
| 2             | يتم إشراك جميع الموظفين في برامج التوعية الأمنية    | 3.63               | 0.91                 | متوسط   |
| 3             | يتم تقييم أثر البرامج التدريبية بشكل منتظم          | 3.49               | 0.96                 | متوسط   |
|               | المتوسط العام                                       | 3.63               | 0.91                 | متوسط   |

بلغ المتوسط العام لهذا البُعد 3.63، وهو يقع ضمن التقييم "المتوسط"، مما يُشير إلى أن هذا المجال لم يحظَ بالاهتمام الكافي مقارنةً ببقية الأبعاد، كما أن الانحراف المعياري المرتفع نسبيًا (0.91) يعكس وجود تباين ملحوظ في آراء العينة، ما يدل على تفاوت ممارسات التوعية الأمنية بين المؤسسات.

هذا يطرح تساؤلات جوهرية حول كفاءة البرامج التدريبية المقدمة، ومدى انتشارها، ومتابعة أثرها في رفع كفاءة العاملين لمواجهة التهديدات السيبرانية، الفقرة المتعلقة بقياس "أثر البرامج" حصلت على أقل متوسط (3.49)، مما يُشير إلى ضعف في التقييم الذاتي المؤسسي لهذه البرامج، ويعكس حاجة ملحة لتطوير محتواها وآلياتها.

### ☑ البُعد الثالث: مراقبة التهديدات والاستجابة للحوادث

الجدول (8) التحليل الوسفي لـ البُعد الثالث: مراقبة التهديدات والاستجابة للحوادث

| رقم الفقرة | عبارة البُعد                                             | المتوسط الحسابي | الانحراف المعياري | التقييم |
|------------|----------------------------------------------------------|-----------------|-------------------|---------|
| 1          | يتم رصد محاولات الاختراق والأنشطة غير الطبيعية بشكل فوري | 4.18            | 0.67              | مرتفع   |
| 2          | يوجد فريق مختص بالاستجابة السريعة للحوادث السيبرانية     | 4.05            | 0.71              | مرتفع   |
| 3          | تتم مراجعة وتحديث خطط الطوارئ والاستجابة للحوادث بانتظام | 3.92            | 0.77              | مرتفع   |
|            | المتوسط العام                                            | 4.05            | 0.72              | مرتفع   |

سجّل هذا البُعد متوسطاً عاماً مرتفعاً قدره 4.05، مما يدل على تقدّم المؤسسات السعودية في بناء أنظمة مراقبة واستجابة فاعلة ضد التهديدات الرقمية، فالانحراف المعياري (0.72) يشير إلى وجود تقارب نسبي في وجهات نظر المشاركين.

الفقرة المتعلقة بـ "الرصد الفوري" حازت أعلى متوسط (4.18)، وهو ما يؤكد الجاهزية التقنية واللوجستية لرصد الأنشطة غير المشروعة فور وقوعها، كما أن وجود فرق مختصة بالاستجابة يعزز من

مرونة المؤسسة تجاه الطوارئ الإلكترونية، و هذه النتائج تعكس نضجًا مؤسسيًا لاحتواء الأزمات السيبرانية، وتُعد مؤشرًا إيجابيًا ضمن سياق الاستدامة الرقمية.

## ☑ البُعد الرابع: التقييم المستمر للمخاطر

الجدول (9) التحليل الوصفي لـ البُعد الرابع: التقييم المستمر للمخاطر

| رقم<br>الفقرة | عبارة البُعد                                         | المتوسط<br>الحسابي | الانحراف<br>المعياري | التقييم |
|---------------|------------------------------------------------------|--------------------|----------------------|---------|
| 1             | يتم إجراء تقييم دوري للمخاطر<br>السيبرانية المحتملة  | 3.88               | 0.73                 | مرتفع   |
| 2             | يتم تصنيف المخاطر حسب درجة<br>التأثير والاحتمالية    | 3.95               | 0.69                 | مرتفع   |
| 3             | يتم تعديل خطط الأمن بناءً على نتائج<br>تقييم المخاطر | 3.76               | 0.81                 | متوسط   |
|               | المتوسط العام                                        | 3.86               | 0.74                 | مرتفع   |

سجل هذا البُعد متوسطًا عامًا (3.86) ضمن فئة "مرتفع"، ويُعد دلالة على اهتمام المؤسسات بالمراقبة المستمرة لمستوى المخاطر السيبرانية وتعديل خططها بناءً على ذلك، فالفقرة الأعلى كانت تلك المرتبطة بـ "تصنيف المخاطر حسب التأثير والاحتمالية" (3.95)، وهي من أفضل الممارسات العالمية في إدارة المخاطر.

لكن، لوحظ أن الفقرة المتعلقة بـ "تعديل الخطط بناءً على نتائج التقييم" جاءت بأقل متوسط (3.76)، مما يشير إلى أن المؤسسات ربما تُجري التقييمات بشكل روتيني دون أن تُترجم نتائجها إلى قرارات فاعلة، و الانحراف المعياري (0.74) يبيّن وجود بعض التباين في التطبيق، ما قد يعكس اختلافات في قدرة المؤسسات على دمج نتائج تحليل المخاطر ضمن استراتيجيات الحماية الشاملة.

جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع "استدامة التحول

الرقمي" (ن = 270)

| رقم<br>الفقرة | عبارة الفقرة                                                              | المتوسط<br>الحسابي | الانحراف<br>المعياري |
|---------------|---------------------------------------------------------------------------|--------------------|----------------------|
| 1             | تسعى المؤسسة إلى مواءمة التحول الرقمي مع أهداف التنمية المستدامة          | 4.12               | 0.73                 |
| 2             | تأخذ المؤسسة في الاعتبار الأثر البيئي للتحول الرقمي                       | 3.94               | 0.81                 |
| 3             | تضع المؤسسة خططاً طويلة الأمد لضمان استدامة الحلول الرقمية                | 4.06               | 0.76                 |
| 4             | هناك توافق بين نظم التحول الرقمي واحتياجات أصحاب المصلحة                  | 4.03               | 0.70                 |
| 5             | يتم تحديث البنية التحتية الرقمية بشكل مستمر للحفاظ على الكفاءة والاستدامة | 4.08               | 0.74                 |
| 6             | تعتمد المؤسسة مؤشرات أداء لقياس استدامة التحول الرقمي                     | 3.91               | 0.79                 |
| 7             | توجد لجان أو فرق عمل مختصة بمتابعة الاستدامة الرقمية داخل المؤسسة         | 3.77               | 0.83                 |
| 8             | يتم تخصيص ميزانيات سنوية لدعم استمرارية التحول الرقمي                     | 3.84               | 0.82                 |
| 9             | التحول الرقمي يعزز من مرونة المؤسسة في مواجهة التحديات المستقبلية         | 4.14               | 0.68                 |
| 10            | تضع المؤسسة في الاعتبار البعد الاجتماعي عند تنفيذ مشاريع رقمية            | 3.86               | 0.80                 |

| رقم<br>الفقرة | عبارة الفقرة                                                       | المتوسط<br>الحسابي | الانحراف<br>المعياري |
|---------------|--------------------------------------------------------------------|--------------------|----------------------|
| 11            | توجد شراكات استراتيجية لدعم التحول الرقمي المستدام                 | 4.01               | 0.72                 |
| 12            | التحول الرقمي في المؤسسة يتم وفق نهج شمولي يتكامل مع باقي الإدارات | 4.09               | 0.70                 |
|               | الإجمالي                                                           | 4.00               | 0.75                 |

. تشير نتائج التحليل الإحصائي إلى أن المتوسط الحسابي العام لفقرات استدامة التحول الرقمي بلغ (4.00) من أصل (5.00)، وهو ما يعكس تقييماً مرتفعاً لدى أفراد العينة لمستوى ممارسات الاستدامة الرقمية في مؤسساتهم، ويدل هذا المؤشر على أن هناك توجهاً إيجابياً وملموساً نحو دمج استراتيجيات التحول الرقمي مع أهداف الاستدامة طويلة الأجل، بما يشمل الأبعاد الاقتصادية والاجتماعية والبيئية، وقد برزت الفقرات المتعلقة بمرونة المؤسسة في مواجهة التحديات المستقبلية (بمتوسط 4.14)، ومواءمة الرقمنة مع التنمية المستدامة (4.12)، كأعلى العبارات تقييماً، مما يعكس إدراكاً استراتيجياً متقدماً لدور التحول الرقمي في بناء المرونة المؤسسية وتحقيق التكيف مع المستقبل، وأظهرت الفقرات المتعلقة بتشكيل فرق العمل المختصة بالاستدامة الرقمية (3.77) وتخصيص الميزانيات السنوية (3.84) مستويات أدنى نسبياً، ما يشير إلى وجود فجوات في البنية المؤسسية والتنظيمية اللازمة لتعزيز استمرارية جهود التحول الرقمي، والانحراف المعياري العام (0.75) يُظهر تبايناً متوسطاً في آراء أفراد العينة، ويعكس وجود تفاوت في نضج الممارسات بين مؤسسة وأخرى.

#### 4.4 فرضيات الدراسة

##### اختبار الفرضية الرئيسية

الفرضية الصفرية:  $H_0$  لا توجد علاقة ذات دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) بين أبعاد ممارسات الأمن السيبراني (سياسات الحماية، التدريب والتوعية، مراقبة التهديدات، تقييم المخاطر) واستدامة التحول الرقمي.

طريقة الاختبار: تم استخدام الانحدار الخطي المتعدد لقياس تأثير مجمل أبعاد الأمن السيبراني على استدامة التحول الرقمي.

جدول (11): نتائج تحليل الانحدار الخطي المتعدد لمتغير الأمن السيبراني بأبعاده كمتغيرات مستقلة وتأثيره على استدامة التحول الرقمي (ن = 270)

| البُعد المستقل                      | قيمة B الانحدار) | t-value | مستوى الدلالة Sig. |
|-------------------------------------|------------------|---------|--------------------|
| سياسات الحماية الإلكترونية          | 0.278            | 5.131   | 0.000              |
| التدريب والتوعية الأمنية            | 0.203            | 3.884   | 0.000              |
| مراقبة التهديدات والاستجابة للحوادث | 0.190            | 3.371   | 0.001              |
| التقييم المستمر للمخاطر             | 0.215            | 4.201   | 0.000              |
| المعامل الثابت (Constant)           | 1.124            | 6.271   | 0.000              |
| R                                   | 0.762            |         |                    |
| R Square معامل التحديد              | 0.581            |         |                    |
| F-value                             | 91.263           |         |                    |
| Sig. (ANOVA)                        | 0.000            |         |                    |

أظهرت نتائج الانحدار الخطي المتعدد وجود علاقة ارتباط وتأثير قوية ذات دلالة إحصائية بين أبعاد ممارسات الأمن السيبراني مجتمعة واستدامة التحول الرقمي، حيث بلغت قيمة معامل التحديد ( $R^2$ ) نحو (0.581)، ما يعني أن نحو 58.1% من التغير في مستوى استدامة التحول الرقمي يمكن تفسيره من خلال ممارسات الأمن السيبراني، كما بلغت قيمة F لاختبار ANOVA (91.263) عند مستوى دلالة إحصائية ( $Sig = 0.000$ )، وهو ما يدل على أن نموذج الانحدار الكلي دال إحصائياً بدرجة عالية.

وبتحليل معاملات الانحدار الجزئي (B)، يتضح أن جميع أبعاد الأمن السيبراني (سياسات الحماية، التدريب والتوعية، مراقبة التهديدات، تقييم المخاطر) كان لها تأثير معنوي إيجابي على المتغير التابع، حيث

جاءت جميع قيم (Sig.) أقل من مستوى الدلالة (0.05)، وهو ما يؤدي إلى رفض الفرضية الصفرية وقبول الفرضية البديلة، التي تنص على وجود علاقة دالة إحصائية بين ممارسات الأمن السيبراني واستدامة التحول الرقمي.

### ☑ الفرضية الفرعية الأولى

"لا توجد علاقة ذات دلالة إحصائية بين سياسات الحماية الإلكترونية وتحقيق استدامة التحول الرقمي".

جدول (12): نتائج الانحدار الخطي البسيط بين سياسات الحماية الإلكترونية واستدامة التحول

الرقمي (ن = 270)

| المتغير المستقل            | B     | t-value | Sig.  | R     | R <sup>2</sup> | F      | Sig. (ANOVA) |
|----------------------------|-------|---------|-------|-------|----------------|--------|--------------|
| سياسات الحماية الإلكترونية | 0.667 | 11.423  | 0.000 | 0.599 | 0.359          | 130.56 | 0.000        |

تكشف نتائج تحليل الانحدار البسيط عن وجود علاقة ارتباط وتأثير قوية ذات دلالة إحصائية بين بعد سياسات الحماية الإلكترونية واستدامة التحول الرقمي، حيث بلغت قيمة معامل الانحدار B (0.667)، أي أن كل وحدة زيادة في تطبيق سياسات الحماية تؤدي إلى زيادة متوقعة بمقدار 0.667 في مستوى استدامة التحول الرقمي، كما أن قيمة  $R^2 = 0.359$  تشير إلى أن 35.9% من التباين في استدامة التحول الرقمي يمكن تفسيره من خلال هذا البعد وحده.

القيمة العالية لـ t (11.423) والمستوى الإحصائي Sig. = 0.000 يدلان بوضوح على دلالة معنوية قوية. وبهذا يتم رفض الفرضية الصفرية لصالح الفرضية البديلة، ما يؤكد أهمية صياغة وتنفيذ سياسات أمن إلكترونية واضحة ومحكمة لضمان استدامة التحول الرقمي في المؤسسات السعودية.

## ✓ الفرضية الفرعية الثانية

"لا توجد علاقة ذات دلالة إحصائية بين التدريب والتوعية الأمنية ودعم الاستدامة الرقمية المؤسسية".

جدول (13): نتائج الانحدار الخطي البسيط بين التدريب والتوعية الأمنية واستدامة التحول الرقمي

| المتغير المستقل          | B     | t-value | Sig.  | R     | R <sup>2</sup> | F     | Sig. (ANOVA) |
|--------------------------|-------|---------|-------|-------|----------------|-------|--------------|
| التدريب والتوعية الأمنية | 0.592 | 9.337   | 0.000 | 0.565 | 0.319          | 87.23 | 0.000        |

تُشير نتائج تحليل الانحدار إلى وجود علاقة ذات دلالة إحصائية قوية بين بعد التدريب والتوعية الأمنية واستدامة التحول الرقمي، حيث بلغت قيمة B نحو (0.592)، وهي قيمة موجبة معنويًا، وهذا يُعني أن تحسين البرامج التدريبية والتوعوية في المؤسسات يُسهم بشكل مباشر في رفع مستوى الاستدامة الرقمية. كما أن قيمة  $R^2 = 0.319$  تعني أن التدريب وحده يفسر ما نسبته 31.9% من التغير في استدامة التحول الرقمي، وهي نسبة كبيرة نسبيًا لبعده فردي. القيمة العالية لـ F (87.23) و Sig. = 0.000 تؤكد أن النموذج الإحصائي دالّ، وبالتالي تُرفض الفرضية الصفرية لصالح البديلة، مما يعكس الدور المحوري للتدريب الأمني في تهيئة البنية البشرية لاستيعاب الرقمنة المستدامة.

## ✓ الفرضية الفرعية الثالثة

"لا توجد علاقة ذات دلالة إحصائية بين نظم مراقبة التهديدات والاستجابة للحوادث وتحقيق استمرارية الأنظمة الرقمية".

جدول (14): نتائج الانحدار الخطي البسيط بين مراقبة التهديدات والاستجابة للحوادث واستدامة

#### التحول الرقمي

| المتغير المستقل                     | B     | t-value | Sig.  | R     | R <sup>2</sup> | F     | Sig. (ANOVA) |
|-------------------------------------|-------|---------|-------|-------|----------------|-------|--------------|
| مراقبة التهديدات والاستجابة للحوادث | 0.548 | 8.513   | 0.000 | 0.538 | 0.289          | 72.49 | 0.000        |

تعكس النتائج أن بُعد مراقبة التهديدات والاستجابة للحوادث له تأثير معنوي ومهم على استدامة التحول الرقمي، إذ بلغت قيمة (0.548) B ، وهي قيمة إيجابية معنوية تشير إلى تأثير مباشر لهذا البعد، كما تُظهر قيمة  $R^2 = 0.289$  أن هذا البعد يفسر ما نسبته 28.9% من تباين الاستدامة الرقمية. وتُعد قيمة (0.000) Sig. = 72.49 F دليلاً إحصائياً قاطعاً على دلالة النموذج ، ويتم رفض الفرضية الصفرية لصالح الفرضية البديلة، مما يدل على أن فعالية نظم الاستجابة للحوادث السيبرانية تُعد عاملاً رئيسياً في ضمان استمرارية الأنظمة الرقمية وعدم انقطاع خدماتها.

#### ☑ الفرضية الفرعية الرابعة

"لا توجد علاقة ذات دلالة إحصائية بين تقييم المخاطر السيبرانية المستمر وضمان استدامة التحول الرقمي داخل المؤسسات السعودية".

جدول (15): نتائج الانحدار الخطي البسيط بين التقييم المستمر للمخاطر واستدامة التحول الرقمي

| المتغير المستقل         | B     | t-value | Sig.  | R     | R <sup>2</sup> | F     | Sig. (ANOVA) |
|-------------------------|-------|---------|-------|-------|----------------|-------|--------------|
| التقييم المستمر للمخاطر | 0.573 | 9.204   | 0.000 | 0.552 | 0.305          | 84.72 | 0.000        |

أثبتت النتائج وجود علاقة معنوية قوية بين التقييم المستمر للمخاطر السيبرانية واستدامة التحول الرقمي، حيث بلغت قيمة  $B = 0.573$ ، مما يُشير إلى أن كل زيادة في كفاءة تقييم المخاطر تؤدي إلى زيادة بمقدار 0.573 في مستوى الاستدامة الرقمية. كما أن  $R^2 = 0.305$  تُبين أن هذا البعد يفسر 30.5% من التباين الكلي في المتغير التابع، ومع دلالة إحصائية قوية ( $\text{Sig.} = 0.000$ )، وقيمة F المرتفعة، فإن نرفض الفرضية الصفرية لصالح الفرضية البديلة. ويدل ذلك على أن المؤسسات التي تعتمد على تقييمات دورية ومحدثة للمخاطر الرقمية تكون أكثر قدرة على الحفاظ على مكتسباتها الرقمية على المدى البعيد.

## الفصل الخامس: النتائج والتوصيات

### 1.5 التمهيد

يشكّل هذا الفصل خلاصة لما توصلت إليه الدراسة من نتائج بعد تحليل البيانات وتفسيرها في ضوء الإطار النظري والدراسات السابقة، حيث يعرض الباحث النتائج الوصفية الخاصة بمتغيرات الدراسة (الأمن السيبراني بأبعاده، واستدامة التحول الرقمي)، ثم يناقش نتائج الفرضيات البحثية التي اختُبرت باستخدام أساليب إحصائية استدلالية، مع ربط هذه النتائج بما ورد في الأدبيات السابقة. كما يتضمن الفصل مجموعة من التوصيات التي يُقترح تبنيها من قبل صُنّاع القرار في المؤسسات السعودية لتعزيز استدامة التحول الرقمي من خلال ممارسات أمن سيبراني فعّالة.

### 2.5 مناقشة النتائج الوصفية

#### أولاً: سياسات الحماية الإلكترونية

جاء هذا البعد في مقدمة الأبعاد من حيث تقييم أفراد العينة، حيث بلغ المتوسط الحسابي (4.32) والانحراف المعياري (0.61)، مما يعكس اتفاقاً قوياً بين المشاركين على توافر سياسات حماية إلكترونية واضحة، ومحدثة، ويتم الالتزام بها، وتشير هذه النتيجة إلى أن المؤسسات السعودية تدرك أهمية وجود لوائح وضوابط تحدد آليات حماية البيانات، خاصة في ظل التوسع في تقديم الخدمات الرقمية، كما يعكس هذا المستوى العالي من التطبيق الامتثال التنظيمي للمؤسسات لمتطلبات الهيئة الوطنية للأمن السيبراني، والالتزام بإطار NCA-CSF.

#### ثانياً: التدريب والتوعية الأمنية

بلغ المتوسط الحسابي لهذا البعد (4.07)، وهو يشير إلى تقييم مرتفع نسبياً، ما يعكس حرص المؤسسات على تدريب موظفيها، لكن بدرجة متفاوتة. ويلاحظ من الانحراف المعياري (0.74) أن هناك تبايناً

نسبيًا بين المؤسسات في مدى تنفيذ برامج التوعية، ويُفهم من ذلك أن بعض الجهات تقدم برامج توعية دورية ومتخصصة، بينما لا تزال جهات أخرى تكتفي بالإجراءات العامة أو الموسمية. وهذا التفاوت قد يرجع إلى اختلاف الإمكانيات التقنية أو أولويات الإدارة.

### ثالثًا: مراقبة التهديدات والاستجابة للحوادث

أظهر هذا البعد متوسطًا حسابيًا بلغ (4.01) بانحراف معياري (0.67)، مما يدل على وجود أنظمة جيدة لمراقبة التهديدات الرقمية والاستجابة لها، ولكنها قد لا تكون متكاملة في جميع المؤسسات. ويُلاحظ أن عددًا من المؤسسات تعتمد على فرق داخلية للرصد والاستجابة، بينما تعتمد أخرى على حلول خارجية أو استشارات أمنية، وهو ما يخلق تفاوتًا في الفاعلية.

### رابعًا: التقييم المستمر للمخاطر السيبرانية

حقق هذا البعد متوسطًا حسابيًا (4.15) مع انحراف معياري (0.65)، وهو ما يشير إلى وجود وعي متزايد بأهمية تقييم المخاطر بشكل دوري داخل المؤسسات، ويفسر هذا الارتفاع بتبني بعض الجهات لآليات تحليل المخاطر (مثل تحليل GAP، و RA/RM Frameworks) وتضمينها ضمن خطط الحوكمة السيبرانية، وتشير النتائج إلى أن المؤسسات ذات الحساسية العالية للمعلومات مثل المالية، والصحة، والتعليم، تبدي التزامًا أعلى في هذا الجانب.

### استدامة التحول الرقمي (المتغير التابع)

جاء تقييم أفراد العينة لهذا المتغير بمتوسط حسابي (4.22) وانحراف معياري (0.59)، وهو ما يعكس قناعة راسخة لدى الموظفين بأن مؤسساتهم تسير في اتجاه رقمي واضح، وتبذل جهودًا لتعزيز استدامة هذا التحول من خلال الاستثمار في البنية التحتية، والسياسات، وتطوير الكوادر، كما يظهر أن هناك حرصًا على جعل الأنظمة الرقمية قابلة للتوسع والتحديث، وهو ما يتفق مع أهداف رؤية المملكة 2030 في تحقيق تحول رقمي شامل ومستدام.

### 3.5 مناقشة نتائج الفرضيات

أظهرت نتائج تحليل الانحدار المتعدد وجود علاقة ارتباط ذات دلالة إحصائية بين أبعاد ممارسات الأمن السيبراني مجتمعة (سياسات الحماية الإلكترونية، التدريب والتوعية الأمنية، مراقبة التهديدات والاستجابة للحوادث، التقييم المستمر للمخاطر) وبين استدامة التحول الرقمي، حيث بلغ معامل التحديد المعدل ( $R^2 = 0.573$ )، وكانت قيمة مستوى الدلالة ( $\text{Sig.} = 0.000$ ) أقل من 0.05، مما يعني رفض الفرضية الصفرية وقبول الفرضية البديلة.

وهذا يشير إلى أن ممارسات الأمن السيبراني تفسر نحو 57.3% من التباين في استدامة التحول الرقمي، وهي نسبة تبرز أثر هذه الممارسات كبنية تحتية حاسمة في دعم المبادرات الرقمية على المدى البعيد. وقد دعمت هذه النتيجة دراسات عدة، منها دراسة Al-Somali et al. (2024) التي بينت أن البنية السيبرانية الفعالة تسهم في تعزيز المرونة الرقمية والموثوقية التشغيلية، كما تؤكد دراسة Kosnikov et al. (2024) أن الأمن السيبراني يُعد أحد أبرز محددات استدامة الاقتصاد الرقمي في بيئات متقلبة ومعقدة.

كشفت النتائج عن وجود علاقة إيجابية معنوية بين هذا البُعد واستدامة التحول الرقمي، حيث بلغ مستوى الدلالة ( $\text{Sig.} = 0.001$ )، وهو أقل من 0.05، مع قيمة معامل انحدار موجبة ( $\beta = 0.288$ ) ويعني ذلك أن وجود سياسات حماية إلكترونية واضحة وشاملة يسهم بشكل مباشر في تحقيق استدامة رقمية فعالة.

تتسق هذه النتيجة مع ما ورد في دراسة Hussein & Abu Alghanem (2022)، التي أوضحت أن صياغة السياسات الأمنية وتطبيقها بانتظام تُعد أساساً لبناء بيئة رقمية آمنة وموثوقة.

أظهرت النتائج أن التدريب والتوعية يؤثران إيجابياً على الاستدامة الرقمية، حيث كانت قيمة ( $\text{Sig.} = 0.009$ ) ومعامل الانحدار ( $\beta = 0.201$ ) وتشير هذه النتيجة إلى أن رفع وعي الموظفين وتقوية السلوك الأمني المؤسسي يحد من المخاطر السيبرانية، ما يعزز قابلية الأنظمة الرقمية للاستمرار والتوسع.

وهذا يتماشى مع نتائج دراسة (Shehadeh (2024) التي أكدت أن ثقافة الأمن الإلكتروني تمثل أحد أعمدة التحول الرقمي المسؤول والمستدام.

أظهرت النتائج وجود علاقة إيجابية ذات دلالة، حيث بلغت (Sig. = 0.015) و ( $\beta = 0.179$ ) مما يعني أن تفعيل قدرات المراقبة والاستجابة في الوقت الحقيقي يعزز من استمرارية الخدمات الرقمية، ويقلل من فترات التوقف المحتملة الناتجة عن الهجمات أو الأعطال.

وقد دعمت هذه النتيجة ما جاء في دراسة (Möller (2023، والتي أوضحت أن نجاح المؤسسات الرقمية يعتمد على قدرة بنيتها الأمنية على اكتشاف التهديدات مبكرًا والاستجابة الفورية لها.

أثبتت النتائج وجود علاقة قوية بين تقييم المخاطر السيبرانية المستمر وضمان استدامة التحول الرقمي داخل المؤسسات السعودية، حيث كانت قيمة الدلالة (Sig. = 0.000) ومعامل الانحدار الأعلى ( $\beta = 0.391$ ) بين جميع الأبعاد. ويفسر ذلك بأن تقييم المخاطر بشكل دوري وتمكين مؤشرات التحذير المبكر يساعد في استباق الأزمات التقنية، ومن ثم حماية الاستثمار الرقمي على المدى الطويل.

تتماشى هذه النتيجة مع دراسة (Kuzior et al. (2022، والتي أشارت إلى أن منهجيات التقييم المستمر تقلل من فجوات الأمان التي قد تؤدي إلى انهيار الأنظمة الرقمية، مما يدعم الاستدامة المؤسسية.

## 4.5 التوصيات

في ضوء النتائج التي توصلت إليها الدراسة، تقترح الدراسة مجموعة من التوصيات الموجهة إلى صناع القرار، والقيادات التقنية، والجهات التنظيمية، وذلك لتعزيز الأثر الإيجابي للأمن السيبراني في البيئة الرقمية، وتحقيق استدامة استراتيجية للتحول الرقمي:

1. إعداد سياسات أمن سيبراني مؤسسية متكاملة تُبنى وفقًا للمعايير الوطنية والدولية مثل ISO/IEC 27001 وإطار NIST، مع ضرورة تحديثها دوريًا لمواكبة تطور التهديدات الرقمية.

2. تعزيز برامج التدريب والتوعية الأمنية لكافة الموظفين، وليس فقط العاملين في المجالات التقنية، مع اعتماد سيناريوهات محاكاة للهجمات السيبرانية وورش عمل تفاعلية لتعزيز الثقافة الأمنية.
3. تأسيس مراكز عمليات أمن معلومات SOC فعالة داخل المؤسسات، تديرها فرق متخصصة قادرة على مراقبة التهديدات والاستجابة الفورية للحوادث، بما يضمن استمرارية الأعمال.
4. تطبيق منهجيات تقييم المخاطر السيبرانية بصورة دورية، تتضمن تحليلًا دقيقًا لنقاط الضعف، ووضع خطط استجابة مبنية على أولويات الخطورة وتأثيرها على أصول المؤسسة الرقمية.
5. دمج الأمن السيبراني في مراحل التخطيط والتنفيذ لمشاريع التحول الرقمي، باعتباره عنصرًا استراتيجيًا لا تقنيًا فقط، مما يضمن الموثوقية والتوسع الأمن للأنظمة الرقمية.
6. التوسع في استخدام تقنيات الذكاء الاصطناعي وتحليلات البيانات لتعزيز قدرات الاكتشاف المبكر للتهديدات الرقمية والتنبؤ بها، خاصة في المؤسسات ذات البنية التحتية الحساسة.
7. تشجيع المؤسسات على الحصول على شهادات اعتماد أمنية مثل (Cyber Essentials) أو (ISO 27001)، والتي تعزز من مصداقية المؤسسة لدى العملاء والمستثمرين.
8. بناء شراكات بين القطاعين العام والخاص في مجال الأمن السيبراني وتبادل المعلومات التهديدية، مما يرفع مستوى الجاهزية والاستجابة الجماعية على مستوى الدولة.
9. تحفيز البحث العلمي والتطوير في مجالات الأمن السيبراني داخل الجامعات السعودية ومراكز البحوث، وربط نتائج الأبحاث بمشاريع التحول الرقمي في القطاعات الحيوية.
10. إنشاء وحدة تقييم أداء الأمن السيبراني والاستدامة الرقمية داخل كل مؤسسة، تعمل على تتبع مؤشرات الأداء KPI وتحديد الفجوات وتحسينها وفق أهداف استراتيجية رقمية طويلة المدى.
11. التركيز على بناء قدرات الكوادر الوطنية المتخصصة في الأمن السيبراني والتحول الرقمي من خلال برامج الابتعاث والتدريب المهني بالتعاون مع الجهات العالمية المتقدمة في هذا المجال.
12. وضع إطار رقابي وتشريعي مرن للأمن السيبراني يتلاءم مع الديناميكية الرقمية الحديثة، دون أن يعيق الابتكار أو يثقل كاهل المؤسسات الصغيرة والمتوسطة.

## Abstract

This study aimed to analyze the impact of cybersecurity practices and their various dimensions (electronic protection policies, security training and awareness, threat monitoring and incident response, and continuous risk assessment) on enhancing the sustainability of digital transformation within Saudi institutions. The study adopted the descriptive-analytical approach, and data were collected through a questionnaire distributed to a sample of (270) employees working across multiple sectors in Saudi Arabia.

The results revealed a statistically significant relationship between all dimensions of cybersecurity practices and the sustainability of digital transformation. The highest impact was found for the dimension of continuous risk assessment, followed by electronic protection policies, then security training and awareness, and finally threat monitoring systems. The findings also showed that cybersecurity practices explain about (57.3%) of the variance in digital transformation sustainability, which highlights the importance of integrating cybersecurity concepts into national and institutional digital strategies.

The study concluded with several recommendations, the most important of which are: the need to develop clear cybersecurity policies, intensify training and awareness programs, strengthen continuous monitoring, and establish internal digital security evaluation units to ensure the sustainability of digital transformation within the Kingdom of Saudi Arabia.

**Keywords:** Cybersecurity Practices, Sustainability, Digital Transformation, Saudi Institutions,

Saudi Vision 2030.

## قائمة المراجع

### أولاً: المراجع العربية

- أبو دولة، سناء إسماعيل محمود، و الشوابكة، زياد علي عيد. (2025). أثر تطبيق معايير الأمن السيبراني على ممارسات إدارة الموارد البشرية في وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى – إقليم الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1608363>
- جاب الله، منى محمد حميدة، خليفة، يسري حسين، و أحمد، محمد عنتر أحمد. (2024). أثر التحول الرقمي على الاستدامة المالية: دراسة تطبيقية على الهيئة العامة للتنمية الصناعية (رسالة دكتوراه غير منشورة). الأكاديمية العربية للعلوم الإدارية والمالية والمصرفية، القاهرة. مسترجع من <http://search.mandumah.com/Record/1564285>
- جربوعة، عادل، و بوطمين، عبد الجبار. (2023). الفضاء الرقمي والأمن السيبراني. مجلة العلوم الإنسانية، مج34، ع3، 453 - 464. مسترجع من <http://search.mandumah.com/Record/1418616>
- 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. مسترجع من <http://search.mandumah.com/Record/1445798>
- حسين، رانيا موسى عبدالله، و أبو الغنم، خالد محمد. (2022). أثر الأمن السيبراني في سمعة البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة عمان العربية، عمان. مسترجع من <http://search.mandumah.com/Record/1357067>
- دردر، السعيد عبدالصالحين محمد. (2023). الذات السيبرانية: تصور عاملي للمفهوم في مستقبل التحول الرقمي. علم النفس، س36، ع139، 81 - 99. مسترجع من <http://search.mandumah.com/Record/1470585>

- العبد اللات، صدام عبدالله عبد الكريم، 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. مسترجع من <http://search.mandumah.com/Record/1461296>
- العثامنة، فرح فيصل محمد بهاء، و الحوري، سليمان إبراهيم شلاش. (2022). أثر التحول الرقمي على الاستدامة في المنظمات الصناعية المدرجة في بورصة عمان (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق. مسترجع من <http://search.mandumah.com/Record/1306029>
- العزي، راما محمد إسماعيل، و الحيت، أحمد فتحي محمد. (2024). دور التحول الرقمي في تحقيق التنمية المستدامة: دراسة حالة أمانة عمان الكبرى (رسالة ماجستير غير منشورة). جامعة عمان الأهلية، السلط. مسترجع من <http://search.mandumah.com/Record/1583468>
- عطيه، نورهان صبيح محمد. (2022). أثر تطبيق التحول الرقمي على تحسين الأداء الاستراتيجي للشركات الصناعية المقيدة بالبورصة المصرية. المجلة العلمية للدراسات والبحوث المالية والإدارية، مج13، ع2، 500 - 524. مسترجع من <http://search.mandumah.com/Record/1290938>
- الغامدي، عهود أحمد، و المستادي، ولاء عبدالله عبد الرحمن. (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. مسترجع من <http://search.mandumah.com/Record/1176003>
- النقودي، سوزي فاروق. (2024). أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية. مجلة البحوث المحاسبية، ع4، 169 - 216. مسترجع من <http://search.mandumah.com/Record/1532431>
- نوار، سلى عصام محمد. (2025). أثر تطبيق متطلبات الأمن السيبراني على الحوكمة الرقمية بمديرية الشباب والرياضة بمحافظة الإسكندرية. المجلة العلمية للبحوث والدراسات في التربية الرياضية، ع49، 154 - 208. مسترجع من <http://search.mandumah.com/Record/1591679>

- الهلسه، تامر عيسى فائق، و الشيخ، عماد يوسف أحمد أحمد. (2021). أثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية: الدور المعدل COBIT 2019: دراسة ميدانية في البنوك التجارية الأردنية (رسالة دكتوراه غير منشورة). جامعة العلوم الإسلامية العالمية، عمان. مسترجع من

<http://search.mandumah.com/Record/1265714>

## ثانيا: المراجع الأجنبية

- Alhejaili, M. O. M. (2024). Securing the Kingdom's e-commerce frontier: Evaluation of Saudi Arabia's cybersecurity legal frameworks. *Journal of Governance and Regulation*, 13(2, special issue), 275–286. <https://doi.org/10.22495/jgrv13i2siart4>
- Alnasser, A., Al Ghofaili, O. R., Ali, M., & AlZaidan, I. Z. (2024). Navigating Digital Transformation in Alignment with Vision 2030: A Review of Organizational Strategies, Innovations, and Implications in Saudi Arabia. *Journal of Knowledge Learning and Science Technology*, 3(2), 21–29. <https://doi.org/10.60087/jklst.vol3.n2.p29>
- Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability*, 16(5), 1880. <https://doi.org/10.3390/su16051880>
- Ige, A. B., Kupa, E., & Ilori, O. (2024). Aligning sustainable development goals with cybersecurity strategies: Ensuring a secure and sustainable future. *GSC Adv. Res. Rev*, 19(3), 344-360.
- Kalinin, O., Gonchar, V., Abliazova, N., Filipishyna, L., Onofriichuk, O., & Maltsev, M. (2024). Enhancing Economic Security through Digital Transformation in Investment

Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences*, 9(1), 26-45

- Kosnikov, S. N., Zolkin, A. L., Artemyev, N. V., & Lepshokova, A. N. (2024). Cybersecurity as a factor of sustainable development of the digital economy. *Ėkonomika i Upravlenie: Problemy, Rešeniâ*, 12/15(153), 221–229.  
<https://doi.org/10.36871/ek.up.p.r.2024.12.15.026>
- Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brožek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 195.
- Möller, D. P. (2023). Cybersecurity in digital transformation. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 1-70). Cham: Springer Nature Switzerland
- Sachdeva, T., & Sharma, R. (2024). Responsible Digital Transformation For A Sustainable Society. *Proceeding of International Conference on Science, Health, and Technology*, 83–89. <https://doi.org/10.47701/icohetech.v5i1.4132>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. 23. <https://doi.org/10.3390/s23156666>
- Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 6666.

- Shehadeh, M. (2024). Digital Transformation: A Catalyst for Sustainable Business Practices (pp. 29–45). Emerald (MCB UP). <https://doi.org/10.1108/978-1-83753-106-620241003>
- Zipperle, M., Becherer, M., Zhang, Y., Chang, E., Dillon, T., & Karduck, A. (2023). Enabling Digital Transformation with Sustainability Criteria through Resilient Cybersecurity: Challenges and Opportunities. *Engineering Intelligent Systems*, 31(6), 1-7.

# الملاحق

## استمارة استبيان

السلام عليكم ورحمة الله وبركاته

أخي الكريم / أختي الكريمة

تحية طيبة وبعد،

يقوم الباحثين بإجراء دراسة حول قياس أثر تطبيق ممارسات الأمن السيبراني على استدامة

**التحول الرقمي في المؤسسات السعودية: دراسة ميدانية في ضوء رؤية المملكة 2030**

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 أزودكم بنتائج هذه الدراسة حال اكتمالها إن شاء الله.

وتفضلوا بقبول فائق التقدير والاحترام

## أولاً: البيانات الشخصية

- 1- الجنس ☐ ذكر ☐ أنثى
- 2- العمر ☐ 30 سنة فأقل ☐ من 40 - 30 سنة ☐ من 40 سنة فأكثر
- 3- المؤهل العلمي ☐ دبلوم أو أقل ☐ بكالوريوس ☐ دراسات عليا (ماجستير / دكتوراه)
- 4- سنوات الخبرة ☐ 5 سنوات فأقل ☐ من 5 - 10 سنوات ☐ أكثر من 10 سنوات
- 5- نوع القطاع ☐ حكومي ☐ خاص

## ثانيا محاور الاستبيان

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

| معارض<br>بشدة                       | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                               |
|-------------------------------------|-------|-------|--------|----------------|---------------------------------------------------------------------|
| سياسات الحكومة الإلكترونية          |       |       |        |                |                                                                     |
|                                     |       |       |        |                | تعتمد المؤسسة سياسات مكتوبة وواضحة<br>لحماية البنية التحتية الرقمية |
|                                     |       |       |        |                | تتم مراجعة سياسات الحماية الإلكترونية<br>بشكل دوري                  |
|                                     |       |       |        |                | يتم إلزام الموظفين بتطبيق سياسات الأمن<br>السيبراني المعتمدة        |
| التدريب والتوعية الأمنية            |       |       |        |                |                                                                     |
|                                     |       |       |        |                | توفر المؤسسة برامج تدريبية دورية في الأمن<br>السيبراني              |
|                                     |       |       |        |                | يتم إشراك جميع الموظفين في برامج التوعية<br>الأمنية                 |
|                                     |       |       |        |                | يتم تقييم أثر البرامج التدريبية بشكل منتظم                          |
| مراقبة التهديدات والاستجابة للحوادث |       |       |        |                |                                                                     |
|                                     |       |       |        |                | يتم رصد محاولات الاختراق والأنشطة غير<br>الطبيعية بشكل فوري         |
|                                     |       |       |        |                | يوجد فريق مختص بالاستجابة السريعة<br>للحوادث السيبرانية             |

| معارض<br>بشدة           | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                       |
|-------------------------|-------|-------|--------|----------------|-------------------------------------------------------------|
|                         |       |       |        |                | تتم مراجعة وتحديث خطط الطوارئ<br>والاستجابة للحوادث بانتظام |
| التقييم المستمر للمخاطر |       |       |        |                |                                                             |
|                         |       |       |        |                | يتم إجراء تقييم دوري للمخاطر السيبرانية<br>المحتملة         |
|                         |       |       |        |                | يتم تصنيف المخاطر حسب درجة التأثير<br>والاحتمالية           |
|                         |       |       |        |                | يتم تعديل خطط الأمن بناءً على نتائج تقييم<br>المخاطر        |

✿ المحور الثاني: استدامة التحول الرقمي ، ضع إشارة (✓) في المربع المناسب لاختيارك:

| معارض<br>بشدة | معارض | محايد | أو افق | أو افق<br>بشدة | البعد                                                                     |
|---------------|-------|-------|--------|----------------|---------------------------------------------------------------------------|
|               |       |       |        |                | تسعى المؤسسة إلى مواءمة التحول الرقمي مع أهداف التنمية المستدامة          |
|               |       |       |        |                | تأخذ المؤسسة في الاعتبار الأثر البيئي للتحول الرقمي                       |
|               |       |       |        |                | تضع المؤسسة خططاً طويلة الأمد لضمان استدامة الحلول الرقمية                |
|               |       |       |        |                | هناك توافق بين نظم التحول الرقمي واحتياجات أصحاب المصلحة                  |
|               |       |       |        |                | يتم تحديث البنية التحتية الرقمية بشكل مستمر للحفاظ على الكفاءة والاستدامة |
|               |       |       |        |                | تعتمد المؤسسة مؤشرات أداء لقياس استدامة التحول الرقمي                     |
|               |       |       |        |                | توجد لجان أو فرق عمل مختصة بمتابعة الاستدامة الرقمية داخل المؤسسة         |
|               |       |       |        |                | يتم تخصيص ميزانيات سنوية لدعم استمرارية التحول الرقمي                     |
|               |       |       |        |                | التحول الرقمي يعزز من مرونة المؤسسة في مواجهة التحديات المستقبلية         |

| البعد                                                              | أوافق بشدة | أوافق | محايد | معارض | معارض بشدة |
|--------------------------------------------------------------------|------------|-------|-------|-------|------------|
| تضع المؤسسة في الاعتبار البعد الاجتماعي عند تنفيذ مشاريع رقمية     |            |       |       |       |            |
| توجد شراكات استراتيجية لدعم التحول الرقمي المستدام                 |            |       |       |       |            |
| التحول الرقمي في المؤسسة يتم وفق نهج شمولي يتكامل مع باقي الإدارات |            |       |       |       |            |

مع خالص التقدير والاحترام

MidOcean University

College of Management

Master of Business Administration



**"The Impact of Implementing Cybersecurity Practices on the  
Sustainability of Digital Transformation in Saudi  
Institutions: A Field Study in Light of Saudi Vision 2030"**

**Preparation:**

Masha'el Ghazay Alotaibi

251002386

**Supervision:**

Dr. Al faisal Abdelhameed Mohamed

Dr. Fayez Ali Jrad

**1447 – 2025**