

## نموذج المشروع النهائي 2

أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على  
جاهزية المؤسسات الحكومية للتصدي للاختراقات

أسم الطالب

معاذ التركي

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس - كلية الإدارة - جامعة ميدأوشن

التاريخ - الفصل الدراسي

2026 – 1447



# إِهْدَاء

أهدي ثمرة جهدي المتواضع

إلى من وهبوني الحياة والأمل، والنشأة على شغف الاطلاع والمعرفة، ومن علموني أن أرتقي سلم الحياة بحكمة وصبر

براء وإحساناً، ووفاء لهما والدي العزيز، ووالدتي العزيزة. إلى من وهبني الله نعمة وجودهم في حياتي إلى العقد المتين

من كانوا عوناً لي في رحلة بحثي إخواني وأخواتي. إلى من كاتفتني ونحن نشق الطريق معاً نحو النجاح في مسيرتنا العلمية إلى رفيقة دربي وأخيراً إلى كل من ساعدني، وكان له دور من قريب أو بعيد في إتمام هذه الدراسة

سائلة المولى أن يجزي الجميع خير الجزاء في الدنيا والآخرة. ثم إلى كل طالب علم سعى بعلمه، ليفيد الإسلام والمسلمين

بكل ما أعطاه الله من علم ومعرفة

# شكر وتقدير

أحمد الله عزوجل الذي وفقني في إتمام هذا البحث العلمي

والذي ألهمني الصحة والعافية والعزيمة.

فالحمد لله حمدا كثيرا

أتقدم بجزيل الشكر والتقدير إلى الأستاذ الدكتور/

د. عبد الرحيم نادر

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 راجيا من المولي  
عزوجل أن تكون هذه الدراسة نافذة لدراسات أخرى .

## المستخلص

هدفت هذه الدراسة إلى قياس أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني للأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية. واعتمدت الدراسة على المنهج الوصفي التحليلي، وطُبقت الاستبانة كأداة رئيسية على عينة عشوائية طبقية بلغت (220) موظفاً من العاملين في إدارات تقنية المعلومات والأمن السيبراني، وحُلَّت البيانات باستخدام برنامج (SPSS). وأظهرت النتائج وجود أثر إيجابي دالّ إحصائياً عند مستوى ( $\alpha \leq 0.05$ ) لتطبيق معايير NCA بأبعادها مجتمعةً على الجاهزية للتصدي للاختراقات، إذ فسرت هذه الأبعاد ما نسبته (78.0%) من التباين في المتغير التابع، وجاء بعد حوكمة الأمن السيبراني الأكثر تأثيراً، يليه تعزيز الأمن السيبراني، ثم صمود الأمن السيبراني، فالأطراف الخارجية والحوسبة السحابية، وأخيراً التقنية التشغيلية. وأوصت الدراسة بضرورة تسريع دورات مراجعة السياسات، وتبني نموذج الثقة الصفريّة، وإجراء تمارين محاكاة دورية للحوادث السيبرانية، وتعزيز مراقبة مزودي الخدمات السحابية، وتأهيل كوادر متخصصة في أمن التقنية التشغيلية، إضافة إلى إنشاء منصة وطنية موحدة لتبادل معلومات التهديدات السيبرانية بين الجهات الحكومية.

الكلمات المفتاحية: الأمن السيبراني، الهيئة الوطنية للأمن السيبراني (NCA)، الجاهزية السيبرانية، الاختراقات السيبرانية، المؤسسات الحكومية، المنطقة الشرقية، المملكة العربية السعودية.

## قائمة المحتويات

|                                         |    |
|-----------------------------------------|----|
| بسم الله الرحمن الرحيم .....            | ب  |
| الإهداء .....                           | ج  |
| الشكر والتقدير .....                    | د  |
| المستخلص .....                          | هـ |
| قائمة المحتويات .....                   | و  |
| قائمة الجداول .....                     | ط  |
| 1.1 المقدمة .....                       | 1  |
| الفصل الأول: الإطار العام للدراسة ..... | 1  |
| 2.1 مشكلة الدراسة .....                 | 3  |
| فجوات على المستوى النظري .....          | 4  |
| فجوات على المستوى التطبيقي .....        | 4  |
| 3.1 أهمية الدراسة .....                 | 5  |
| على المستوى النظري: .....               | 5  |
| على المستوى التطبيقي: .....             | 6  |
| 4.1 أسئلة الدراسة .....                 | 6  |
| 5.1 أهداف الدراسة .....                 | 7  |
| 6.1 فرضيات الدراسة .....                | 8  |
| 7.1 نموذج الدراسة .....                 | 9  |
| 8.1 منهجية الدراسة .....                | 10 |
| مجتمع وعينة الدراسة .....               | 10 |
| مصادر جمع البيانات .....                | 11 |
| أدوات الدراسة .....                     | 11 |
| الأساليب الإحصائية المستخدمة .....      | 11 |
| حدود الدراسة .....                      | 12 |
| أداة الدراسة (توزيع الفقرات) .....      | 12 |

|       |                                                                          |    |
|-------|--------------------------------------------------------------------------|----|
| 9.1   | الدراسة الميدانية .....                                                  | 13 |
| 10.1  | مخطط المشروع المقترح (هيكل الدراسة) .....                                | 13 |
| 1.2   | المقدمة .....                                                            | 15 |
|       | الفصل الثاني: الإطار النظري .....                                        | 15 |
| 2.2   | المتغير المستقل: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) ..... | 16 |
| 1.2.2 | تمهيد ومفهوم تطبيق معايير الهيئة الوطنية للأمن السيبراني .....           | 16 |
| 2.2.2 | أهمية تطبيق معايير الهيئة الوطنية للأمن السيبراني .....                  | 18 |
| 3.2.2 | أهداف تطبيق معايير الهيئة الوطنية للأمن السيبراني .....                  | 19 |
| 4.2.2 | أبعاد تطبيق معايير الهيئة الوطنية للأمن السيبراني .....                  | 20 |
| 5.2.2 | الدراسات السابقة المرتبطة بالمتغير المستقل .....                         | 22 |
| 3.2   | المتغير التابع: جاهزية المؤسسات الحكومية للتصدي للاختراقات .....         | 24 |
| 1.3.2 | تمهيد ومفهوم جاهزية المؤسسات الحكومية .....                              | 24 |
| 2.3.2 | أهمية جاهزية المؤسسات الحكومية للتصدي للاختراقات .....                   | 25 |
| 3.3.2 | أهداف تحقيق جاهزية المؤسسات الحكومية للتصدي للاختراقات .....             | 26 |
| 4.3.2 | أبعاد جاهزية المؤسسات الحكومية للتصدي للاختراقات .....                   | 27 |
| 5.3.2 | الدراسات السابقة المرتبطة بالمتغير التابع .....                          | 29 |
| 4.2   | العلاقة بين المتغير المستقل والمتغير التابع .....                        | 31 |
| 5.2   | الخاتمة .....                                                            | 34 |
| 1.3   | المقدمة .....                                                            | 36 |
|       | الفصل الثالث: منهجية الدراسة .....                                       | 36 |
| 2.3   | التعريفات الإجرائية لمتغيرات البحث .....                                 | 37 |
| 3.3   | تصميم البحث (البوصلة البحثية) .....                                      | 38 |
| 4.3   | مجتمع البحث وطرق وتقنيات أخذ العينات .....                               | 39 |
| 5.3   | طريقة جمع البيانات .....                                                 | 40 |
| 6.3   | أنواع البيانات .....                                                     | 41 |
| 7.3   | إجراءات التحليل الإحصائي .....                                           | 42 |
| 8.3   | الخاتمة .....                                                            | 42 |
| 1.4   | المقدمة .....                                                            | 44 |

|         |                                                         |
|---------|---------------------------------------------------------|
| 44..... | الفصل الرابع: التحليل الاحصائي ومناقشة النتائج          |
| 45..... | 2.4 توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث) |
| 48..... | 3.4 اختبارات الصدق والثبات للاستبانة                    |
| 49..... | 4.4 الإحصاء الوصفي لمتغيرات البحث                       |
| 59..... | 5.4 اختبار الفرضيات ومناقشة النتائج                     |
| 68..... | 1.5 المقدمة                                             |
| 68..... | الفصل الخامس: حدود البحث والتوصيات والنتائج             |
| 69..... | 2.5 حدود الدراسة والدراسات المستقبلية                   |
| 71..... | 3.5 توصيات الدراسة                                      |
| 73..... | 4.5 الخاتمة                                             |
| 75..... | ABSTRACT                                                |
| 76..... | قائمة المراجع                                           |
| 80..... | ملحق (1): الاستبانة                                     |

## قائمة الجداول

| رقم<br>الصفحة | اسم الجدول                                                                                                        | رقم<br>الجدول |
|---------------|-------------------------------------------------------------------------------------------------------------------|---------------|
| 45            | جدول (1): التوزيع التكراري والنسبي لأفراد عينة الدراسة وفقاً للمتغيرات الديموغرافية                               | 1.            |
| 48            | جدول (2): معاملات ألفا كرونباخ لأبعاد الاستبانة                                                                   | 2.            |
| 49            | جدول (3): معاملات ارتباط بيرسون بين أبعاد الاستبانة والدرجة الكلية للمتغير                                        | 3.            |
| 50            | جدول (4): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد حوكمة الأمن السيبراني                              | 4.            |
| 51            | جدول (5): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تعزيز الأمن السيبراني                              | 5.            |
| 53            | جدول (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد صمود الأمن السيبراني                               | 6.            |
| 54            | جدول (7): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني للأطراف الخارجية والحوسبة السحابية | 7.            |
| 55            | جدول (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني للتقنية التشغيلية                  | 8.            |
| 56            | جدول (9): الترتيب العام لأبعاد المتغير المستقل (تطبيق معايير NCA)                                                 | 9.            |
| 57            | جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع (الجاهزية للتصدي للاختراقات)            | 10.           |

| رقم<br>الجدول | اسم الجدول                                                                                                                               | رقم<br>الصفحة |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 11.           | جدول (11): نتائج تحليل الانحدار المتعدد لأثر أبعاد تطبيق معايير NCA على الجاهزية للتصدي للاختراقات                                       | 59            |
| 12.           | جدول (12): تحليل الانحدار الخطي البسيط لقياس أثر حوكمة الأمن السيبراني على الجاهزية للتصدي للاختراقات                                    | 62            |
| 13.           | جدول (13): تحليل الانحدار الخطي البسيط لقياس أثر تعزيز الأمن السيبراني على الجاهزية للتصدي للاختراقات                                    | 63            |
| 14.           | جدول (14): تحليل الانحدار الخطي البسيط لقياس أثر صمود الأمن السيبراني على الجاهزية للتصدي للاختراقات                                     | 64            |
| 15.           | جدول (15): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني للأطراف الخارجية والحوسبة السحابية على الجاهزية للتصدي للاختراقات       | 65            |
| 16.           | جدول (16): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على الجاهزية للتصدي للاختراقات | 66            |



الفصل الأول: الإطار  
العام للدراسة

## 1.1 المقدمة

يشهد العالم اليوم تحولاً رقمياً متسارعاً أعاد تشكيل طبيعة العمل المؤسسي وأسلوب تقديم الخدمات الحكومية، إذ باتت البنى التحتية الرقمية ركيزة أساسية لاقتصادات الدول وأمنها الوطني. وقد أفرز هذا التحول واقعاً جديداً تتعاظم فيه المخاطر السيبرانية بوصفها أحد أبرز التهديدات التي تواجه الحكومات والمنظمات على حد سواء؛ حيث تستهدف الهجمات السيبرانية البيانات الحساسة والأنظمة الحيوية والخدمات العامة، بما يهدد استقرار المؤسسات وثقة المواطنين فيها. وفي ضوء ذلك، أصبح الأمن السيبراني عنصراً استراتيجياً لا غنى عنه ضمن منظومة الحوكمة الرقمية الحديثة، خاصة في القطاعات الحكومية التي تتعامل مع بيانات وطنية حساسة وتقدم خدمات لا تحتمل التوقف. (Pemmasani, 2023)

وفي هذا السياق العالمي المتغير، أولت المملكة العربية السعودية الأمن السيبراني اهتماماً بالغاً انسجاماً مع مستهدفات رؤية المملكة 2030، فأنشأت الهيئة الوطنية للأمن السيبراني (NCA) عام 1438هـ بوصفها الجهة المختصة بتنظيم الأمن السيبراني على المستوى الوطني وتعزيزه وحماية المصالح الحيوية للدولة. وقد أصدرت الهيئة منظومة متكاملة من الأطر والضوابط، يأتي في مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) التي تتضمن في نسختها المحدثّة (ECC-2:2024) خمسة مكونات رئيسية و(29) مكوناً فرعياً و(114) ضابطاً، تمثل الحد الأدنى الإلزامي الذي يتعين على الجهات الوطنية الالتزام به لحماية أصولها المعلوماتية والتقنية. كما أصدرت الهيئة ضوابط متخصصة مثل ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC) وضوابط التقنية التشغيلية (OTCC)، بهدف توحيد مستويات النضج السيبراني وتقليل المخاطر الوطنية.

ويتقاطع هذا التوجه الوطني مع توجهات دولية مماثلة تركز على بناء قدرات المؤسسات الحكومية لمواجهة الاختراقات، إذ تشير الأدبيات الحديثة إلى أن الجاهزية السيبرانية (Cybersecurity Readiness) أصبحت محدداً جوهرياً لأداء المؤسسات وقدرتها على الصمود في وجه التهديدات، وأن الالتزام بأطر الحوكمة السيبرانية ينعكس إيجاباً على فاعلية الاستجابة للحوادث وإدارة المخاطر (Mohamed Noor et al., 2026)؛ Majeed et

(al., 2026). كما بينت دراسات مقارنة بين بيئات مختلفة أن وجود إطار تنظيمي وطني واضح يُمتثل عاملاً حاسماً في رفع مستوى النضج السيبراني وتقليل الفجوة بين السياسات والتطبيق الفعلي. (Rawindaran et al., 2023)

غير أن الواقع التطبيقي يكشف أن إصدار الضوابط وحده لا يكفي لتحقيق الجاهزية المطلوبة، إذ تتفاوت المؤسسات الحكومية في مستوى التزامها وقدرتها على ترجمة هذه الضوابط إلى ممارسات فعلية وإجراءات تشغيلية مؤثرة. وتتأثر هذه الجاهزية بعوامل متعددة منها: مستوى الوعي السيبراني، توافر الكفاءات البشرية، كفاية الموازنات المخصصة، ومدى تكامل الحوكمة السيبرانية مع باقي منظومات الحوكمة المؤسسية. وتُعد المنطقة الشرقية في المملكة العربية السعودية بيئة ذات أهمية خاصة في هذا السياق، نظراً لاحتضانها قطاعات حيوية تجعل وزاراتها وفروعها الحكومية مستهدفة بصفة متكررة من الهجمات السيبرانية.

ومن هذا المنطلق، تأتي الدراسة الحالية لتسليط الضوء على أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات، من خلال دراسة ميدانية على وزارات المنطقة الشرقية، وذلك بهدف قياس مستوى الالتزام الفعلي بهذه المعايير، وتحديد طبيعة العلاقة بينها وبين مؤشرات الجاهزية، والوقوف على الفجوات التي تحول دون تحقيق الفاعلية المرجوة، بما يسهم في تقديم توصيات عملية تدعم صناع القرار في تعزيز المنظومة السيبرانية الوطنية.

## 2.1 مشكلة الدراسة

على الرغم من الجهود التشريعية والتنظيمية التي بذلتها الهيئة الوطنية للأمن السيبراني (NCA) في إصدار حزمة متكاملة من الضوابط الإلزامية، وفي مقدمتها الضوابط الأساسية للأمن السيبراني (ECC) بنسختها الأحدث (ECC-2:2024)، إلا أن مؤشرات الواقع تشير إلى استمرار وقوع الجهات الحكومية ضحايا لاختراقات سيبرانية متفاوتة الخطورة، وإلى تباين واضح بين المؤسسات في مستوى تطبيقها للضوابط وفي درجة جاهزيتها الفعلية

للتصدي للتهديدات. وهذا يطرح تساؤلاً جوهرياً حول العلاقة بين الالتزام الشكلي بالمعايير من جهة، وتحقيق الجاهزية التشغيلية الحقيقية من جهة أخرى، خاصة في ظل ندرة الدراسات الميدانية التي تناولت هذه العلاقة في السياق السعودي عموماً، وفي وزارات المنطقة الشرقية على وجه التحديد.

### فجوات على المستوى النظري

تتمثل الفجوات النظرية التي تسعى الدراسة إلى معالجتها في أن معظم الأدبيات السابقة التي تناولت الأمن السيبراني الحكومي ركزت على الجوانب التقنية أو السياساتية بمعزل عن قياس الأثر الفعلي للأطر الوطنية على الجاهزية المؤسسية. فقد بحثت دراسة (Pemmasani, 2023) في أطر الأمن السيبراني الوطنية للبنى التحتية الحرجة من منظور مقارنة دون التعمق في إطار تنظيمي قطري بعينه، كما تناولت دراسة (Rawindaran et al., 2023) حوكمة الأمن السيبراني في المنشآت الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة دون التطرق إلى المؤسسات الحكومية. وفي المقابل، ركزت دراسة (Mohamed Noor et al., 2026) على أثر الجاهزية السيبرانية على الأداء الأمني التنظيمي في البيئة الماليزية، بينما تناولت دراسة (Majeed et al., 2026) حوكمة الأمن السيبراني في السياق الباكستاني، وهو ما يكشف عن غياب دراسات نظرية تربط مباشرة بين منظومة معايير NCA السعودية ومؤشرات الجاهزية للتصدي للاختراقات في القطاع الحكومي. كما يلاحظ ندرة الأطر النظرية التي تكامل بين أبعاد الحوكمة وإدارة المخاطر والصمود التنظيمي ضمن نموذج واحد يُختبر في السياق السعودي، وهو ما تسعى هذه الدراسة إلى الإسهام في معالجته من خلال بناء إطار مفاهيمي يربط بين متغيرات تطبيق الضوابط ومخرجات الجاهزية.

### فجوات على المستوى التطبيقي

أما على المستوى التطبيقي، فإن قاعدة الدراسات الميدانية التي قيّم الأثر الفعلي لتطبيق معايير NCA على جاهزية الجهات الحكومية السعودية لا تزال محدودة، ولم يُرصد

حسب علم الباحث وجود دراسة ميدانية مخصصة لوزارات المنطقة الشرقية تحديداً، مع ما تتميز به هذه المنطقة من ثقل اقتصادي وحضور لقطاعات حيوية يجعل مؤسساتها هدفاً متكرراً للهجمات السيبرانية. كما يلاحظ في الواقع التطبيقي تفاوت واضح بين الجهات الحكومية في مستوى نضج الأمن السيبراني، وفي مدى ترجمة الالتزام التنظيمي بالضوابط إلى ممارسات تشغيلية فاعلة على أرض الواقع، إضافة إلى وجود تحديات تتعلق بنقص الكوادر المتخصصة، ومحدودية الوعي السيبراني لدى الموظفين، وضعف تكامل منظومات الاستجابة للحوادث، وهو ما أشارت إليه ضمناً تقارير الجهات الرقابية ومؤشرات النضج السيبراني الوطنية. ويضاف إلى ذلك غياب أدوات قياس عملية تربط بين كل بُعد من أبعاد الضوابط الأساسية ومؤشر محدد من مؤشرات الجاهزية للتصدي للاختراقات، مما يصعب على الجهات الحكومية تشخيص فجواتها الفعلية وتحديد أولويات التحسين.

وفي ضوء ما تقدم من فجوات نظرية وتطبيقية، يمكن صياغة السؤال الرئيسي للدراسة على النحو الآتي: ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

### 3.1 أهمية الدراسة

تستمد هذه الدراسة أهميتها من حداثة موضوعها وارتباطه المباشر بأحد أهم محاور رؤية المملكة 2030 المتعلق ببناء اقتصاد رقمي آمن ومستدام، فضلاً عن كونها تتناول قطاعاً حساساً يتمثل في المؤسسات الحكومية التي تعدّ خط الدفاع الأول عن البيانات الوطنية والخدمات العامة. وتنقسم أهمية الدراسة إلى بُعدين متكاملين:

#### على المستوى النظري:

تُسهم الدراسة في إثراء الأدبيات العربية والسعودية المتعلقة بالأمن السيبراني الحكومي من خلال تقديم إطار نظري يربط بين معايير NCA بوصفها متغيراً مستقلاً متعدد الأبعاد يشمل الحوكمة وتعزيز الأمن السيبراني وصموده ومكوناته المتعلقة بالأطراف الخارجية

والحوسبة السحابية والأنظمة الصناعية - ومتغير الجاهزية للتصدي للاختراقات بوصفه متغيراً تابعاً يشمل أبعاد الوقاية والاكتشاف والاستجابة والتعافي. كما تُعدّ الدراسة إضافة معرفية تُقلّص الفجوة في الأبحاث التي تناولت أثر الأطر التنظيمية الوطنية على الأداء السيبراني للمؤسسات الحكومية في السياق السعودي، وتفتح المجال أمام دراسات لاحقة لاختبار النموذج في قطاعات أو مناطق جغرافية أخرى، أو لإجراء دراسات مقارنة مع أطر مماثلة في دول الخليج والشرق الأوسط. ويُتوقع أن تسهم نتائج الدراسة في تطوير الأدوات المفاهيمية المستخدمة في قياس النضج السيبراني المؤسسي، وفي تعميق فهم العلاقة بين الامتثال التنظيمي والصمود السيبراني الفعلي.

### على المستوى التطبيقي:

تكتسب الدراسة أهميتها التطبيقية من كونها تُقدّم تشخيصاً ميدانياً لواقع تطبيق معايير NCA في وزارات المنطقة الشرقية، وتُوفّر للقيادات الحكومية ومسؤولي الأمن السيبراني صورة واضحة عن مستوى الجاهزية الفعلية ومواطن القوة والضعف في تطبيق الضوابط. كما تسهم نتائج الدراسة في تزويد الهيئة الوطنية للأمن السيبراني (NCA) بمؤشرات ميدانية مفيدة في مراجعة آليات الإشراف والمتابعة ودعم الجهات الحكومية في رحلة الامتثال، بما يُعزّز فاعلية المنظومة الوطنية ككل. ومن المتوقع أن تُفيد الدراسة الجهات الحكومية في توجيه استثماراتها في الأمن السيبراني نحو الأبعاد الأكثر تأثيراً في الجاهزية، وفي تطوير برامج بناء القدرات والتدريب وفقاً للفتحات المُشخّصة. كما قد تُشكّل التوصيات العملية للدراسة مرجعاً مساعداً لصنّاع القرار في تطوير السياسات الداخلية للوزارات، وتعزيز ثقافة الأمن السيبراني، وبناء قدرات الاستجابة للحوادث، بما يسهم في النهاية في حماية الأصول الوطنية وتعزيز ثقة المستفيدين بالخدمات الحكومية الرقمية.

### 4.1 أسئلة الدراسة

السؤال الرئيسي : ما أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية؟

ويتفرع من السؤال الرئيسي مجموعة من الأسئلة الفرعية على النحو الآتي:

1. ما أثر تطبيق بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟
2. ما أثر تطبيق بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟
3. ما أثر تطبيق بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟
4. ما أثر تطبيق بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟
5. ما أثر تطبيق بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية؟

## 5.1 أهداف الدراسة

تهدف هذه الدراسة إلى دراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

وينبثق من هذا الهدف الرئيسي مجموعة من الأهداف الفرعية التي تُسهم مجتمعة في تحقيقه، وهي على النحو الآتي:

- قياس أثر بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- قياس أثر بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- الخروج بمجموعة من التوصيات والمقترحات العملية التي تُسهم في رفع كفاءة تطبيق معايير NCA، وتعزيز جاهزية المؤسسات الحكومية للتصدي للاختراقات، بما يدعم صناع القرار في الهيئة الوطنية للأمن السيبراني وفي الوزارات المعنية.

## 6.1 فرضيات الدراسة

في ضوء مشكلة الدراسة وأسئلتها وأهدافها، تسعى الدراسة إلى اختبار الفرضية الرئيسية الآتية:

- الفرضية الرئيسية: ( $H_0$ ) لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية  $(\alpha \leq 0.05)$  لتطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها مجتمعة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة

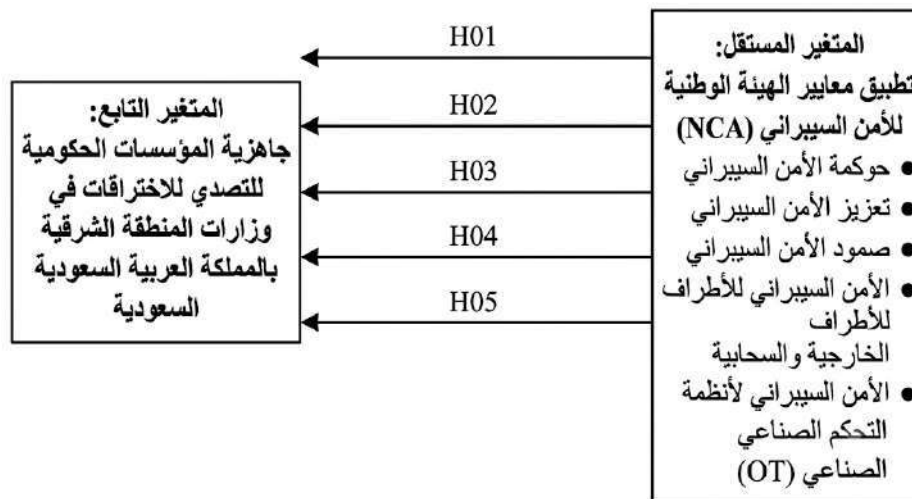
التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

وتتفرع من الفرضية الرئيسية الفرضيات الفرعية الآتية:

- $H_{01}$ : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لتطبيق بُعد حوكمة الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- $H_{02}$ : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لتطبيق بُعد تعزيز الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- $H_{03}$ : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لتطبيق بُعد صمود الأمن السيبراني على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- $H_{04}$ : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لتطبيق بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.
- $H_{05}$ : لا يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ( $\alpha \leq 0.05$ ) لتطبيق بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية.

## 7.1 نموذج الدراسة

يوضح نموذج الدراسة العلاقة السببية بين المتغير المستقل المتمثل في تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعاده الخمسة، والمتغير التابع المتمثل في جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك على النحو الآتي:



## 8.1 منهجية الدراسة

سوف يعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي، باعتباره الأنسب لطبيعة الدراسة وأهدافها، إذ سيقوم بوصف الظاهرة محل الدراسة وصفاً دقيقاً من خلال استعراض الإطار النظري والدراسات السابقة المتعلقة بمعايير الهيئة الوطنية للأمن السيبراني (NCA) وجاهزية المؤسسات الحكومية للتصدي للاختراقات، ثم تحليل البيانات التي سيتم جمعها ميدانياً للوصول إلى نتائج علمية دقيقة تُسهم في اختبار فرضيات الدراسة والإجابة عن تساؤلاتها.

كما سوف يستخدم الباحث المنهج الكمي في مرحلة الدراسة الميدانية، من خلال تصميم استبانة إلكترونية تُوزع على مجتمع الدراسة، ثم معالجة البيانات إحصائياً باستخدام برنامج (SPSS) للوصول إلى استنتاجات تعكس واقع تطبيق معايير NCA وأثرها على جاهزية المؤسسات الحكومية في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

## مجتمع وعينة الدراسة

سوف يتكون مجتمع الدراسة من العاملين في إدارات تقنية المعلومات والأمن السيبراني في الوزارات والجهات الحكومية العاملة في المنطقة الشرقية بالمملكة العربية السعودية،

والبالغ عددهم التقريبي (1,250) موظفاً موزعين على مختلف الوزارات والفروع الحكومية في المنطقة.

وسوف يقوم الباحث بسحب عينة عشوائية طبقية حجمها (295) مفردة، وقد تم تحديد هذا الحجم بالاعتماد على معادلة (Steven K. Thompson) عند مستوى ثقة (95%) وهامش خطأ (5%)، حيث سيتم توزيع (330) استبانة إلكترونية تحسباً لعدم اكتمال بعض الاستجابات، ويتوقع استرداد ما لا يقل عن (300) استبانة صالحة للتحليل الإحصائي.

### مصادر جمع البيانات

سوف يعتمد الباحث في جمع البيانات على مصدرين رئيسيين هما: المصادر الثانوية، والتي تشمل الكتب والمراجع العلمية والدوريات المحكمة والرسائل الجامعية والتقارير الرسمية الصادرة عن الهيئة الوطنية للأمن السيبراني، إضافةً إلى قواعد البيانات العلمية ذات الصلة بموضوع الدراسة؛ والمصادر الأولية، والتي ستُجمع بياناتها من الميدان مباشرةً عبر استبانة إلكترونية مصممة خصيصاً لأغراض هذه الدراسة.

### أدوات الدراسة

سوف يستخدم الباحث الاستبانة أداة رئيسية لجمع البيانات، وسيتم تصميمها وفقاً لمقياس ليكرت الخماسي، بعد التحقق من صدقها وثباتها من خلال عرضها على مجموعة من المحكمين الأكاديميين والمهنيين المتخصصين، وحساب معامل ثبات ألفا كرونباخ للتأكد من الاتساق الداخلي لفقراتها.

### الأساليب الإحصائية المستخدمة

سوف يعتمد الباحث على مجموعة من الأساليب الإحصائية المناسبة لطبيعة الدراسة، تشمل: مقاييس الإحصاء الوصفي (المتوسطات الحسابية والانحرافات المعيارية والتكرارات والنسب المئوية)، ومعامل ألفا كرونباخ لقياس الثبات، ومعامل ارتباط بيرسون للصدق البنائي، واختبار التوزيع الطبيعي، ومعاملات VIF و Tolerance لاختبار التداخل الخطي،

فضلاً عن تحليل الانحدار الخطي المتعدد لاختبار الفرضيات وقياس أثر المتغيرات المستقلة على المتغير التابع.

## حدود الدراسة

تقتصر حدود الدراسة على النحو الآتي: الحدود الموضوعية وتتمثل في دراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة على جاهزية المؤسسات الحكومية للتصدي للاختراقات؛ والحدود المكانية وتشمل الوزارات والجهات الحكومية في المنطقة الشرقية بالمملكة العربية السعودية؛ والحدود البشرية وتتضمن العاملين في إدارات تقنية المعلومات والأمن السيبراني في تلك الوزارات؛ والحدود الزمانية وتتمثل في الفترة الزمنية التي سيتم فيها تنفيذ الدراسة الميدانية خلال عام 2026م.

## أداة الدراسة (توزيع الفقرات)

سوف تتكون الاستبانة من قسمين رئيسيين؛ يتضمن القسم الأول البيانات الديموغرافية للمستجيبين، بينما يشتمل القسم الثاني على فقرات قياس متغيرات الدراسة موزعة على النحو الآتي:

| المحور          | المتغير                                                     | عدد الفقرات |
|-----------------|-------------------------------------------------------------|-------------|
| المتغير المستقل | حوكمة الأمن السيبراني                                       | 4           |
| المتغير المستقل | تعزيز الأمن السيبراني                                       | 4           |
| المتغير المستقل | صمود الأمن السيبراني                                        | 4           |
| المتغير المستقل | الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية | 4           |

|    |                                                          |                 |
|----|----------------------------------------------------------|-----------------|
| 4  | الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية | المتغير المستقل |
| 10 | جاهزية المؤسسات الحكومية للتصدي للاختراقات               | المتغير التابع  |
| 30 | إجمالي فقرات المقياس                                     |                 |

## 9.1 الدراسة الميدانية

سوف يقوم الباحث بتنفيذ الدراسة الميدانية وفق خطوات علمية منظمة، تبدأ بتصميم الاستبانة الإلكترونية اعتماداً على الإطار النظري والدراسات السابقة والوثيقة التنظيمية لمعايير الهيئة الوطنية للأمن السيبراني (NCA)، ثم عرضها على مجموعة من المحكمين المتخصصين للتحقق من صدقها الظاهري والمحتوى، يليها تطبيق دراسة استطلاعية على عينة محدودة قوامها (30) مفردة من مجتمع الدراسة لاختبار ثبات الأداة وصلاحياتها.

وبعد التأكد من صلاحية الأداة، سوف يتم توزيعها إلكترونياً على أفراد العينة المستهدفة في وزارات المنطقة الشرقية، ثم تُجمع الاستجابات وتُفرغ في برنامج (SPSS) لإجراء التحليلات الإحصائية اللازمة، وصولاً إلى النتائج التي سيتم مناقشتها في ضوء فرضيات الدراسة والدراسات السابقة، لتخرج الدراسة في نهايتها بمجموعة من التوصيات العملية.

## 10.1 مخطط المشروع المقترح (هيكل الدراسة)

سوف يتم تنظيم الدراسة في خمسة فصول رئيسية على النحو الآتي:

الفصل الأول: الإطار العام للدراسة يتضمن: المقدمة، مشكلة الدراسة، أهمية الدراسة، أسئلة الدراسة، أهداف الدراسة، فرضيات الدراسة، نموذج الدراسة، منهجية الدراسة، حدود الدراسة، ومصطلحات الدراسة.

### الفصل الثاني: الإطار النظري والدراسات السابقة

- المبحث الأول: معايير الهيئة الوطنية للأمن السيبراني (NCA) وأبعادها.

- المبحث الثاني: جاهزية المؤسسات الحكومية للتصدي للاختراقات.
- المبحث الثالث: الدراسات السابقة العربية والأجنبية، والتعليق عليها، وموقع الدراسة الحالية منها.

الفصل الثالث: منهجية الدراسة وإجراءاتها يتضمن: منهج الدراسة، مجتمع وعينة الدراسة، أداة الدراسة، صدق الأداة وثباتها، الأساليب الإحصائية المستخدمة، وإجراءات تطبيق الدراسة الميدانية.

الفصل الرابع: عرض نتائج الدراسة الميدانية ومناقشتها يتضمن: الخصائص الديموغرافية للعينة، تحليل نتائج المحاور، اختبار الفرضيات، ومناقشة النتائج في ضوء الدراسات السابقة.

الفصل الخامس: النتائج والتوصيات يتضمن: خلاصة النتائج، التوصيات العملية، المقترحات للدراسات المستقبلية.

قائمة المراجع والملاحق.



الفصل الثاني: الإطار  
النظري

## 1.2 المقدمة

يُعدّ هذا الفصل حجر الأساس في البناء المعرفي والنظري للدراسة الحالية، إذ يستعرض الأدبيات والدراسات السابقة المرتبطة بمتغيرات البحث، ويسهم في تكوين رؤية علمية متكاملة حول موضوع الدراسة. وتتبع أهمية هذا الفصل من كونه يوفر خلفية نظرية عميقة حول تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بوصفه المتغير المستقل، وجاهزية المؤسسات الحكومية للتصدي للاختراقات بوصفها المتغير التابع، فضلاً عن استعراض العلاقة التي تربط بينهما في ضوء التحوّل الرقمي المتسارع الذي تشهده المؤسسات الحكومية في المملكة العربية السعودية عموماً، وفي وزارات المنطقة الشرقية على وجه الخصوص.

ويسعى هذا الفصل إلى تقديم إطار مفاهيمي متكامل لكل متغير من متغيرات الدراسة، بدءاً بتوضيح المفهوم والأهمية والأهداف والأبعاد، ومروراً باستعراض مجموعة من الدراسات العربية والأجنبية الحديثة التي تناولت هذه المتغيرات في سياقات متنوعة، ووصولاً إلى تحليل طبيعة العلاقة التي تربط بين المتغيرين المستقل والتابع. كما يهدف الفصل إلى تحديد الفجوة البحثية التي تسعى الدراسة الحالية إلى سدّها، من خلال المقارنة بين ما تم تناوله في الأدبيات السابقة وما ستضيفه هذه الدراسة من إسهام علمي جديد.

وقد جاء تنظيم هذا الفصل ليعكس التسلسل المنطقي في عرض المتغيرات ومناقشتها، حيث يبدأ بعرض المتغير المستقل ودراساته المرتبطة، ثم ينتقل إلى المتغير التابع بالمنهجية ذاتها، ثم يتناول العلاقة بين المتغيرين، ويختتم بخاتمة تلخص أبرز ما تم استعراضه من أدبيات ودراسات.

## 2.2 المتغير المستقل: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

### 1.2.2 تمهيد ومفهوم تطبيق معايير الهيئة الوطنية للأمن السيبراني

شهد العالم في العقدین الأخيرین تحولاً رقمياً عميقاً غير ملاّح العمل المؤسسي في كافة القطاعات، وأصبحت البيانات والمعلومات الرقمية من أهم الأصول الاستراتيجية التي تمتلكها المؤسسات الحكومية والخاصة. وفي ظل تصاعد التهديدات السيبرانية وتنوع أساليب الاختراق، برزت الحاجة الملحة إلى إرساء منظومات وطنية متكاملة للأمن السيبراني تضمن حماية البنى التحتية الحيوية والمعلومات الحساسة. وفي هذا السياق، أنشأت المملكة العربية السعودية الهيئة الوطنية للأمن السيبراني (NCA) عام 2017 لتكون الجهة المختصة بالأمن السيبراني في المملكة، والمرجع الوطني في شؤونه، وتعمل على تعزيزه لحماية المصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

ويُعرف تطبيق معايير الهيئة الوطنية للأمن السيبراني بأنه المنظومة المتكاملة من الضوابط والسياسات والإجراءات التي أصدرتها الهيئة، والتي تلتزم الجهات الوطنية بتطبيقها لتحقيق الحد الأدنى من متطلبات الأمن السيبراني، بهدف حماية الأصول المعلوماتية والتقنية من التهديدات الداخلية والخارجية. ويشير أبو دولة والشوابكة (2025) إلى أن معايير الأمن السيبراني تمثل مجموعة من الأطر التنظيمية والفنية والإدارية التي تُوفّر بيئة عمل آمنة، وتضمن سلامة البيانات وسريتها وتوافرها، وتُعزّز من قدرة المؤسسات على الاستمرارية في أداء مهامها. ويضيف الفلاح والنسور والعربيّات (2023) أن هذه المعايير تُشكّل خارطة طريق تنظيمية تُساعد المؤسسات على مواكبة التطورات التقنية المتسارعة، وتُوفّر مرجعية موحدة تُقاس بها مستويات النضج السيبراني.

كما يُعرفها الهاجري والبشاشة (2021) بأنها منظومة متكاملة من الضوابط الأساسية التي تُعالج الجوانب المتعلقة بالحوكمة والمخاطر والامتثال، وتُغطّي كافة الجوانب التشغيلية والفنية والاستراتيجية للأمن السيبراني. وفي السياق الدولي، يرى (Pemmasani 2023) أن الأطر الوطنية للأمن السيبراني تُمثّل الركيزة الأساسية لبناء المرونة السيبرانية على مستوى الدول، وتسهم في حماية البنى التحتية الحيوية من الهجمات المتطورة. ويؤكد Gambo, Danasabe, Binbeshr, Imam, Shinwari, and Mahmoud (2026) على أن معايير الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية تُعدّ من أكثر

الأطر شمولاً في المنطقة، إذ تُغطّي كافة الجوانب المتعلقة بالحوكمة والحماية والصمود والأطراف الخارجية وأنظمة التحكم الصناعي.

## 2.2.2 أهمية تطبيق معايير الهيئة الوطنية للأمن السيبراني

تتبع أهمية تطبيق معايير الهيئة الوطنية للأمن السيبراني من الدور المحوري الذي تلعبه في حماية المؤسسات من المخاطر السيبرانية المتزايدة، وتعزيز الثقة في الخدمات الرقمية الحكومية، وضمان استمرارية الأعمال في ظل بيئة تقنية شديدة التعقيد. وقد تناول العديد من الباحثين هذه الأهمية من زوايا متعددة، مما يعكس الاهتمام الأكاديمي والعملية المتنامي بهذا الموضوع.

ويشير الحطافي والعباس والمطيري (2026) إلى أن أهمية تطبيق معايير الأمن السيبراني تتجلى في عدة محاور، أبرزها: أولاً، الحدّ من المخاطر السيبرانية التي تواجه المؤسسات المالية والحكومية من خلال توفير ضوابط استباقية تُقلّل من احتمالية وقوع الاختراقات؛ ثانياً، تعزيز قدرة المؤسسات على الامتثال للتشريعات والأنظمة الوطنية والدولية ذات العلاقة؛ ثالثاً، حماية سمعة المؤسسات وتعزيز ثقة العملاء والمستفيدين في الخدمات المقدّمة؛ رابعاً، تحسين الكفاءة التشغيلية من خلال تبني ممارسات أمنية موحّدة وفعّالة.

ويرى الحسيني والدعيمي (2025) أن أهمية معايير الأمن السيبراني تتمثّل في قدرتها على الحدّ من القصور الذاتي للمؤسسات، من خلال: تعزيز الوعي السيبراني لدى العاملين، وبناء ثقافة أمنية مؤسسية راسخة، وتوفير آليات واضحة للاستجابة للحوادث السيبرانية، وضمان التعافي السريع بعد وقوع الاختراقات، فضلاً عن حماية الأصول المعلوماتية باعتبارها ثروة استراتيجية للمؤسسة.

ويضيف نوار (2025) أن أهمية تطبيق متطلبات الأمن السيبراني تظهر في: دعم الحوكمة الرقمية داخل المؤسسات، وتحقيق التكامل بين الأنظمة التقنية المختلفة، وتوفير بيئة آمنة لتبادل البيانات والمعلومات، وتعزيز الشفافية والمساءلة في الأداء المؤسسي، وتمكين المؤسسات من مواكبة رؤية المملكة 2030 في مجال التحوّل الرقمي.

وفي السياق الدولي، يشير (Majeed, Majeed, and Minhas (2026 إلى أن أهمية حوكمة الأمن السيبراني تتجلى في: بناء المرونة التنظيمية في مواجهة التهديدات المتطورة، ودمج إدارة المخاطر السيبرانية ضمن الاستراتيجية العامة للمؤسسة، وتعزيز الرقابة التنظيمية على الأصول الرقمية، وضمان استمرارية الأعمال في ظل الأزمات السيبرانية. كما يؤكد (Rawindaran and Nawaf (2023 على أن معايير الأمن السيبراني تُشكل عاملاً حاسماً في تعزيز تنافسية المؤسسات في عصر الصناعة 5.0، من خلال بناء ثقة الأطراف المعنية وتوفير بيئة رقمية آمنة تدعم الابتكار والنمو.

### 3.2.2 أهداف تطبيق معايير الهيئة الوطنية للأمن السيبراني

تسعى معايير الهيئة الوطنية للأمن السيبراني إلى تحقيق جملة من الأهداف الاستراتيجية والتشغيلية التي تخدم الرؤية الوطنية في بناء منظومة سيبرانية متكاملة. وقد تناول الباحثون هذه الأهداف بأساليب متعددة تعكس تنوع الزوايا التي يمكن النظر منها إلى هذا الموضوع.

ويشير السرحان والمشاقبة (2020) إلى أن أهداف تطبيق سياسة الأمن السيبراني تتمثل فيما يلي: أولاً، حماية سرية المعلومات المؤسسية من الوصول غير المصرح به؛ ثانياً، ضمان سلامة البيانات من التعديل أو التلاعب غير المشروع؛ ثالثاً، توفير المعلومات في الوقت المناسب للمستخدمين المصرح لهم؛ رابعاً، تعزيز جودة المعلومات المحاسبية والإدارية في المؤسسات المالية؛ خامساً، بناء منظومة رقابية فعّالة تحدّ من المخاطر التشغيلية.

كما يشير صمادي والعليمات (2020) إلى أن أهداف تطبيق سياسة الأمن السيبراني تتضمن: تحسين جودة التدقيق الإلكتروني، وتعزيز الثقة في المخرجات الرقمية، وتوفير بيئة آمنة للتعاملات الإلكترونية، ودعم اقتصاد المعرفة من خلال حماية الأصول المعرفية، وبناء منظومة تكامل بين المؤسسات المختلفة تُتيح تبادلاً آمناً للمعلومات.

ويرى الفلاح والنسور والعربيات (2023) أن الأهداف الجوهرية لتطبيق معايير الأمن السيبراني تشمل: تحسين الأداء المؤسسي في قطاع الاتصالات، وتعزيز رضا العملاء عن

الخدمات المُقدّمة، وحماية البنية التحتية الحيوية للاتصالات، والحدّ من الخسائر المالية الناجمة عن الحوادث السيبرانية، وتمكين المؤسسات من التوسّع الرقمي بثقة وأمان.

وفي السياق الدولي، يشير Mohamed Noor, Moghavvemi, and Tajudeen (2026) إلى أن أهداف الجاهزية السيبرانية تتضمن: تعزيز الأداء الأمني للمؤسسات، وبناء قدرات استباقية للكشف عن التهديدات، وتطوير آليات فعّالة للاستجابة للحوادث، وتحقيق التوافق بين الاستراتيجية الأمنية والاستراتيجية العامة للمؤسسة، وتعزيز ثقافة الأمن السيبراني على كافة المستويات التنظيمية. كما يشير Gambo and Danasabe (2026) إلى أن أهداف تطبيق المعايير السعودية للأمن السيبراني تشمل: بناء منظومة وطنية متكاملة، وتوحيد الممارسات الأمنية عبر القطاعات، وتعزيز التعاون الدولي في مجال الأمن السيبراني، ودعم التحوّل الرقمي الآمن ضمن رؤية 2030.

#### 4.2.2 أبعاد تطبيق معايير الهيئة الوطنية للأمن السيبراني

تم تحديد أبعاد تطبيق معايير الهيئة الوطنية للأمن السيبراني بناءً على دراسة الحلفي والعباس والمطيري (2026) ودراسة Gambo and Danasabe (2026) ودراسة أبو دولة والشوابكة (2025)، والتي تناولت الضوابط الأساسية للأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية. وتتضمن هذه الأبعاد خمسة محاور رئيسة تُشكّل الإطار المتكامل لتطبيق المعايير، وفيما يلي شرح مفصّل لهذه الأبعاد:

البُعد الأول: حوكمة الأمن السيبراني، ويمثّل هذا البُعد الركيزة الاستراتيجية التي تُبنى عليها منظومة الأمن السيبراني في المؤسسة، إذ يتضمن وضع السياسات والإجراءات الحاكمة، وتحديد الأدوار والمسؤوليات، وبناء الهيكل التنظيمي المناسب لإدارة الأمن السيبراني. ويشمل هذا البُعد إعداد استراتيجية الأمن السيبراني بما يتوافق مع الاستراتيجية العامة للمؤسسة، وتخصيص الموارد البشرية والمالية اللازمة، وضمان الالتزام بالتشريعات والأنظمة ذات العلاقة. كما يركّز على إدارة المخاطر السيبرانية من خلال تحديدها وتقييمها ومعالجتها ومراقبتها بشكل مستمر، إضافة إلى بناء برامج التوعية والتدريب لتعزيز الثقافة السيبرانية داخل المؤسسة.

البُعد الثاني: تعزيز الأمن السيبراني، ويتناول هذا البُعد الجوانب الفنية والتشغيلية المتعلقة بحماية الأصول المعلوماتية والتقنية للمؤسسة. ويتضمن إدارة الأصول من خلال حصرها وتصنيفها، وإدارة هويات المستخدمين وصلاحيات الوصول بحيث لا يحصل أي مستخدم على صلاحيات تزيد عن حاجته الوظيفية، وحماية الأنظمة والأجهزة من خلال التحديثات الأمنية الدورية وتطبيق الإعدادات الآمنة. كما يشمل حماية البريد الإلكتروني وشبكات الاتصال، وإدارة التشفير لحماية البيانات أثناء تخزينها ونقلها، وإدارة النسخ الاحتياطية لضمان استعادة البيانات عند الحاجة، وإدارة الثغرات الأمنية من خلال الفحص الدوري والمعالجة السريعة.

البُعد الثالث: صمود الأمن السيبراني، ويعنى هذا البُعد بقدرة المؤسسة على الاستمرار في تقديم خدماتها ووظائفها الأساسية في مواجهة الحوادث السيبرانية والأزمات الطارئة. ويتضمن بناء خطط استمرارية الأعمال بما يشمل الجوانب السيبرانية، وإعداد خطط التعافي من الكوارث السيبرانية، وتحديد أزمنة الاستعادة المستهدفة، وإجراء اختبارات دورية للتأكد من فاعلية هذه الخطط. كما يركز على بناء قدرات المؤسسة في الاستجابة للحوادث من خلال تشكيل فرق متخصصة، ووضع إجراءات واضحة للتعامل مع الحوادث، وتوثيق الدروس المستفادة لتحسين الأداء المستقبلي.

البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، ويتناول هذا البُعد المخاطر السيبرانية الناجمة عن التعامل مع الأطراف الخارجية كالموردين ومقدمي الخدمات، فضلاً عن استخدام خدمات الحوسبة السحابية. ويتضمن تقييم المخاطر المرتبطة بهذه الأطراف قبل التعاقد معها، وتضمين متطلبات الأمن السيبراني في العقود، والرقابة على التزامها بهذه المتطلبات طوال فترة التعاقد. كما يشمل وضع ضوابط خاصة باستخدام الخدمات السحابية بما يضمن حماية بيانات المؤسسة وسريتها، وتحديد مواقع تخزين البيانات، وضمان استعادتها عند إنهاء التعاقد.

البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية، ويعنى هذا البُعد بحماية الأنظمة التقنية التشغيلية وأنظمة التحكم الصناعي التي تُدير البنى التحتية الحيوية

كالطاقة والمياه والاتصالات. ويتضمن الفصل بين الشبكات التشغيلية وشبكات تقنية المعلومات، وتطبيق ضوابط أمنية متخصصة تراعي طبيعة هذه الأنظمة، وحمايتها من الهجمات المتطورة التي قد تستهدف تعطيل الخدمات الحيوية أو الإضرار بالبنية التحتية. كما يشمل إدارة الوصول إلى هذه الأنظمة بشكل صارم، ومراقبة الأنشطة عليها بشكل مستمر، وتحديث أنظمة الحماية بما يتوافق مع طبيعة التهديدات المتغيرة.

وإلى جانب هذه الأبعاد الخمسة، تجدر الإشارة إلى وجود عناصر مكملة تدعم تطبيق هذه المعايير، منها: التقييم الذاتي الدوري لمستوى الالتزام بالمعايير، والمراجعة الخارجية من قبل جهات متخصصة، والتحسين المستمر بناءً على نتائج التقييمات والمراجعات، فضلاً عن التكامل مع المعايير الدولية كالأيزو 27001 وإطار NIST لتعزيز الفاعلية والشمولية.

## 5.2.2 الدراسات السابقة المرتبطة بالمتغير المستقل

### أولاً: الدراسات العربية

دراسة أبو دولة والشوابكة: (2025) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني) على ممارسات إدارة الموارد البشرية في وكالة الأمم المتحدة لإغاثة وتشغيل اللاجئين الفلسطينيين (الأونروا) في إقليم الأردن. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (285) موظفاً في الوكالة. وتوصلت نتائج الدراسة إلى وجود أثر ذي دلالة إحصائية لتطبيق معايير الأمن السيبراني على ممارسات إدارة الموارد البشرية، وأوصت بضرورة تعزيز برامج التوعية السيبرانية وتطوير السياسات المتعلقة بحماية بيانات الموظفين.

دراسة الفلاح والنسور والعربيات: (2023) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (السياسات والإجراءات، البنية التحتية، الوعي والتدريب، إدارة المخاطر) على أداء شركات الاتصالات الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (310) موظفين في شركات الاتصالات. وتوصلت نتائج

الدراسة إلى وجود أثر إيجابي ذي دلالة إحصائية لتطبيق معايير الأمن السيبراني على الأداء المؤسسي، وأوصت بضرورة الاستثمار في البنية التحتية السيبرانية وتطوير برامج التدريب المتخصصة.

دراسة الحلفي والعباس والمطيري: (2026) هدفت الدراسة إلى التعرف على أثر تطبيق معايير الأمن السيبراني بأبعاده (الحوكمة، التعزيز، الصمود، الأطراف الخارجية) في الحدّ من المخاطر في البنوك التجارية بمدينة الرياض. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (240) موظفاً في البنوك التجارية. وتوصلت نتائج الدراسة إلى وجود أثر قوي لتطبيق معايير الأمن السيبراني في الحدّ من المخاطر المصرفية، وأوصت بتعزيز التعاون بين البنوك والهيئة الوطنية للأمن السيبراني.

#### ثانياً: الدراسات الأجنبية

دراسة: Pemmasani (2023) هدفت الدراسة إلى التعرف على دور الأطر الوطنية للأمن السيبراني في حماية البنية التحتية الحيوية، من خلال استخلاص الدروس المستفادة من المبادرات الحكومية للمرونة السيبرانية. واستخدمت الدراسة المنهج التحليلي المقارن، وتكونت العينة من مراجعة أطر الأمن السيبراني في عشر دول. وتوصلت نتائج الدراسة إلى أن الأطر الوطنية الشاملة تُعزّز بشكل كبير من مرونة البنية التحتية الحيوية، وأوصت الدراسة بتبني مقاربات متكاملة تجمع بين الحوكمة والضوابط الفنية والتعاون الدولي.

دراسة: Rawindaran and Nawaf (2023) هدفت الدراسة إلى التعرف على تعزيز حوكمة وسياسات الأمن السيبراني للمؤسسات الصغيرة والمتوسطة في ظل الصناعة 5.0، من خلال دراسة مقارنة بين المملكة العربية السعودية والمملكة المتحدة. واستخدمت الدراسة المنهج الوصفي المقارن، وتكونت العينة من (200) مؤسسة صغيرة ومتوسطة موزعة بين البلدين. وتوصلت نتائج الدراسة إلى وجود فروق جوهرية في مستوى نضج ممارسات الأمن السيبراني بين البلدين، وأوصت الدراسة بتعزيز برامج التوعية وتبني أفضل الممارسات الدولية في المؤسسات الصغيرة والمتوسطة.

دراسة: (Gambo and Danasabe 2026) هدفت الدراسة إلى التعرف على معايير الأمن السيبراني في المملكة العربية السعودية ومعوقات تطبيقها، وتحليل المشهد السيبراني في المملكة. واستخدمت الدراسة المنهج التحليلي النوعي، وتكونت العينة من (35) خبيراً ومسؤولاً في مجال الأمن السيبراني. وتوصلت نتائج الدراسة إلى تحديد عدد من معوقات التطبيق، منها: محدودية الكوادر البشرية المؤهلة، وقيود الميزانية، وتحديات الثقافة المؤسسية، وأوصت الدراسة بتعزيز برامج بناء القدرات، وتقوية التعاون بين الهيئة الوطنية للأمن السيبراني والمؤسسات في مختلف القطاعات.

## 3.2 المتغير التابع: جاهزية المؤسسات الحكومية للتصدي للاختراقات

### 1.3.2 تمهيد ومفهوم جاهزية المؤسسات الحكومية

تُعدّ جاهزية المؤسسات الحكومية للتصدي للاختراقات السيبرانية من أهم المفاهيم الحديثة في مجال الإدارة العامة والأمن السيبراني، إذ تعكس قدرة هذه المؤسسات على مواجهة التهديدات الرقمية المتطورة وحماية أصولها المعلوماتية وضمان استمرارية خدماتها. وقد اكتسب هذا المفهوم أهمية متزايدة في ظل التوسع الرقمي الذي تشهده الحكومات حول العالم، وارتفاع وتيرة الهجمات السيبرانية التي تستهدف القطاع الحكومي بشكل خاص لما يمتلكه من بيانات حساسة وبنى تحتية حيوية.

ويعرّف (Mohamed Noor and Moghavvemi 2026) الجاهزية السيبرانية بأنها الحالة التي تكون فيها المؤسسة مهيأة تنظيمياً وفنياً وبشرياً لمواجهة التهديدات السيبرانية، والاستجابة الفعالة للحوادث، والتعافي السريع منها بأقل قدر من الخسائر. ويرى (Gorenšek and Trivunčević 2025) أن الجاهزية السيبرانية تتجاوز مجرد امتلاك الأدوات التقنية إلى بناء منظومة متكاملة تشمل الاستراتيجية والحوكمة والقدرات البشرية والثقافة المؤسسية.

ويشير (Zubaidah and Monalisa 2024) إلى أن الجاهزية الإلكترونية للمؤسسات الحكومية تمثل مقياساً لمدى استعدادها للتحوّل الرقمي وتقديم الخدمات الإلكترونية بكفاءة

وأمان. كما يُعرّفها Yusuf (2021) بأنها القدرة المؤسسية على تبني التقنيات الحديثة والتكيف مع المتطلبات الرقمية المتغيرة، مع ضمان توفر الكفاءات البشرية والبنية التحتية اللازمة. وفي السياق العربي، يشير الهاجري والبشاشة (2021) إلى أن جاهزية المؤسسات الحكومية تتضمن قدرتها على استشعار التهديدات مبكراً، والاستجابة لها بفاعلية، والتعافي منها بأقل التكاليف الممكنة، مما يُعزّز من ثقة المواطنين في الخدمات الحكومية الرقمية.

### 2.3.2 أهمية جاهزية المؤسسات الحكومية للتصدي للاختراقات

تتبع أهمية جاهزية المؤسسات الحكومية للتصدي للاختراقات من الطبيعة الاستراتيجية للقطاع الحكومي والدور المحوري الذي يلعبه في تقديم الخدمات للمواطنين وحماية المصالح الوطنية. وقد تناول الباحثون هذه الأهمية من زوايا متعددة تعكس أبعاد هذا الموضوع.

ويشير Murad and Qudah (2025) إلى أن أهمية الجاهزية السيبرانية للمؤسسات الوطنية تتمثل فيما يلي: أولاً، حماية الأمن الوطني من التهديدات السيبرانية التي قد تستهدف البنى التحتية الحيوية؛ ثانياً، ضمان استمرارية الخدمات الحكومية المُقدّمة للمواطنين دون انقطاع؛ ثالثاً، حماية البيانات الحساسة للمواطنين والمؤسسات؛ رابعاً، تعزيز الثقة العامة في الحكومة الإلكترونية والخدمات الرقمية؛ خامساً، الحدّ من الخسائر المالية الناجمة عن الاختراقات السيبرانية.

ويرى Gorenšek and Trivunčević (2025) أن أهمية الجاهزية السيبرانية تتجلى في: بناء المرونة الوطنية في مواجهة الحرب السيبرانية، وتعزيز التنافسية الرقمية للدولة على المستوى الدولي، ودعم التحول الرقمي بشكل آمن ومستدام، وحماية الاستثمارات التقنية الضخمة التي تضخها الحكومات، وبناء منظومة تعاون إقليمي ودولي في مجال الأمن السيبراني.

ويضيف الهاجري والبشاشة (2021) أن أهمية جاهزية المؤسسات الحكومية تظهر في: تعزيز قدرة الأجهزة الحكومية على إدارة الأزمات السيبرانية بفاعلية، وتوفير بيئة رقمية

أمنة لتنفيذ الاستراتيجيات الوطنية، وبناء ذكاء استراتيجي يُمكن من استشعار التهديدات مبكراً، ودعم اتخاذ القرارات المبنية على معلومات دقيقة وأمنة.

ويشير نوار (2025) إلى أن أهمية الجاهزية السيبرانية للمؤسسات الحكومية تتمثل في: دعم الحوكمة الرقمية وتحقيق أهدافها، وضمان جودة الخدمات الرقمية المُقدمة، وتعزيز الشفافية والمساءلة في العمل الحكومي، وتمكين المؤسسات من مواكبة التطورات التقنية المتسارعة، وحماية سمعة المؤسسات الحكومية من الأضرار الناجمة عن الاختراقات.

كما يرى (Almaiah and Alfaisal (2022 أن أهمية الجاهزية المؤسسية تتضمن: تعزيز قدرة المؤسسات على تبني التقنيات الناشئة كالذكاء الاصطناعي بشكل آمن، وبناء ميزة تنافسية مستدامة، وتحسين تجربة المستخدمين، ودعم الابتكار المؤسسي، وتحقيق التميز في الأداء التشغيلي.

### 3.3.2 أهداف تحقيق جاهزية المؤسسات الحكومية للتصدي للاختراقات

تسعى المؤسسات الحكومية إلى تحقيق جاهزيتها السيبرانية من خلال مجموعة من الأهداف الاستراتيجية والتشغيلية التي تخدم رسالتها ورؤيتها. وقد تناول الباحثون هذه الأهداف بأساليب متنوعة.

ويشير (Mohamed Noor and Moghavvemi (2026 إلى أن أهداف الجاهزية السيبرانية تتضمن ما يلي: أولاً، تحقيق الأداء الأمني الأمثل للمؤسسة من خلال بناء قدرات دفاعية متكاملة؛ ثانياً، الكشف المبكر عن التهديدات السيبرانية قبل تحولها إلى حوادث فعلية؛ ثالثاً، الاستجابة السريعة والفعّالة للحوادث السيبرانية عند وقوعها؛ رابعاً، التعافي السريع من الحوادث بأقل الخسائر الممكنة؛ خامساً، التعلم المستمر من الحوادث لتحسين الأداء المستقبلي.

كما يشير (Gorenšek and Trivunčević (2025 إلى أن أهداف الجاهزية السيبرانية على المستوى الوطني تشمل: بناء استراتيجيات وطنية متكاملة، وتطوير مؤشرات

قياس عالمية للجاهزية السيبرانية، وتعزيز التعاون الإقليمي في منطقة الاتحاد الأوروبي المتوسطي، وبناء قدرات وطنية في مجال الاستخبارات السيبرانية، وتحسين ترتيب الدول في المؤشرات الدولية للأمن السيبراني.

ويرى (Kulin and Johansson Sevć 2021) أن أهداف بناء الثقة في المؤسسات الحكومية تتضمن: تعزيز الشفافية في اتخاذ القرارات، وبناء علاقات إيجابية مع المواطنين، ودعم المشاركة العامة في السياسات الحكومية، وضمان الحيادية والنزاهة في الأداء المؤسسي، وتحقيق التوازن بين الأهداف الأمنية والحقوق الفردية.

ويشير (Zubaidah and Monalisa 2024) إلى أن أهداف الجاهزية الإلكترونية للمؤسسات الحكومية تتمثل في: تسريع التحول نحو الحكومة الإلكترونية، وتحسين كفاءة تقديم الخدمات، وخفض التكاليف التشغيلية، وتعزيز التكامل بين المؤسسات الحكومية المختلفة، وبناء منظومة بيانات موحدة تدعم اتخاذ القرارات.

كما يشير الحسيني والدعيمي (2025) إلى أن الأهداف التي تسعى الجاهزية السيبرانية إلى تحقيقها تتضمن: الحد من القصور الذاتي للمؤسسات، وتعزيز قدرتها على التكيف مع المتغيرات، وبناء ثقافة الابتكار والتحسين المستمر، ودعم اتخاذ القرارات الاستراتيجية بمعلومات دقيقة وأمنة، وتحقيق التميز المؤسسي المستدام.

#### 4.3.2 أبعاد جاهزية المؤسسات الحكومية للتصدي للاختراقات

تم تحديد أبعاد جاهزية المؤسسات الحكومية للتصدي للاختراقات بناءً على دراسة (Mohamed Noor and Moghavvemi 2026) ودراسة (Gorenšek and Trivunčević 2025) ودراسة (Murad and Qudah 2025)، والتي تناولت هذه الجاهزية بشكل شامل ومتكامل. وتتضمن هذه الأبعاد المحاور الرئيسة التالية:

البُعد الأول: الجاهزية الاستراتيجية والتخطيطية، ويمثل هذا البُعد الركيزة الأساسية للجاهزية السيبرانية، إذ يتضمن وجود استراتيجية واضحة للأمن السيبراني على مستوى

المؤسسة، تتوافق مع الاستراتيجية الوطنية للأمن السيبراني، وتتضمن رؤية ورسالة وأهدافاً واضحة قابلة للقياس. كما يشمل هذا البُعد التخطيط طويل المدى لمواجهة التهديدات المستقبلية، وتخصيص الميزانيات اللازمة، وبناء خارطة طريق زمنية لتطوير القدرات السيبرانية، فضلاً عن ربط الاستراتيجية السيبرانية بالخطط التنموية الوطنية ومواءمتها مع رؤية المملكة 2030.

**البُعد الثاني:** الجاهزية التقنية والبنية التحتية، ويتناول هذا البُعد الجوانب الفنية والتكنولوجية اللازمة لبناء منظومة أمنية فعّالة. ويتضمن توفير البنية التحتية التقنية المتطورة، وتطبيق أحدث تقنيات الحماية كأنظمة كشف التسلل وأنظمة منع الاختراق وجدران الحماية المتقدمة، واستخدام تقنيات التشفير الحديثة، وتطبيق تقنيات التحليل الذكي للتهديدات باستخدام الذكاء الاصطناعي وتعلّم الآلة. كما يشمل هذا البُعد بناء مراكز عمليات أمنية (SOC) تعمل على مدار الساعة، وتوفير أدوات الاستجابة للحوادث، وضمان التحديث المستمر للأنظمة والبرامج.

**البُعد الثالث:** الجاهزية البشرية والكوادر المتخصصة، ويعنى هذا البُعد بتوفير الكوادر البشرية المؤهلة والمتخصصة في مجال الأمن السيبراني. ويتضمن استقطاب المواهب المتميزة، وتطوير برامج التدريب والتأهيل المستمر للعاملين، وبناء مسارات مهنية واضحة للمتخصصين في الأمن السيبراني، وتنظيم برامج التوعية السيبرانية لجميع العاملين في المؤسسة. كما يشمل بناء الشراكات مع الجامعات ومراكز التدريب المتخصصة، والاستفادة من الشهادات المهنية الدولية، وتطوير قدرات القيادات في اتخاذ القرارات المتعلقة بالأمن السيبراني.

**البُعد الرابع:** الجاهزية التنظيمية والإدارية، ويتناول هذا البُعد الجوانب المتعلقة بالهيكل التنظيمي والسياسات والإجراءات الداعمة للأمن السيبراني. ويتضمن وجود هيكل تنظيمي واضح لإدارة الأمن السيبراني، وتحديد الأدوار والمسؤوليات، ووضع السياسات والإجراءات المكتوبة والمعتمدة، وبناء نظام إدارة المخاطر السيبرانية. كما يشمل تفعيل مبدأ الفصل بين

المهام، وبناء آليات الرقابة الداخلية، وتوثيق الإجراءات، وضمان التحسين المستمر للممارسات التنظيمية.

البُعد الخامس: الجاهزية للاستجابة والتعافي، ويُركّز هذا البُعد على قدرة المؤسسة على الاستجابة الفعّالة للحوادث السيبرانية والتعافي منها. ويتضمن وجود خطط مكتوبة للاستجابة للحوادث، وتشكيل فرق متخصصة (CERT/CSIRT) ، وإجراء تمارين محاكاة دورية، ووجود قنوات اتصال واضحة مع الجهات المعنية داخلياً وخارجياً. كما يشمل بناء خطط استمرارية الأعمال، وضمان توفّر النسخ الاحتياطية، وتحديد أزمّة الاستعادة المستهدفة، وتوثيق الدروس المستفادة من كل حادثة.

وإلى جانب هذه الأبعاد، تُضاف عناصر مكمّلة تُعزّز جاهزية المؤسسات الحكومية، منها: الجاهزية الثقافية التي تعكس مستوى الوعي السيبراني ودمج قيم الأمن في ثقافة المؤسسة، والجاهزية للتعاون والشراكات مع الجهات الوطنية والدولية لتبادل المعلومات والخبرات، والجاهزية للتقييم والتحسين المستمر من خلال إجراء تقييمات دورية ذاتية وخارجية، ومقارنة الأداء بأفضل الممارسات العالمية.

### 5.3.2 الدراسات السابقة المرتبطة بالمتغير التابع

#### أولاً: الدراسات العربية

دراسة الهاجري والبشاشة: (2021) هدفت الدراسة إلى التعرف على أثر الذكاء الاستراتيجي على استراتيجيات إدارة الأزمات من خلال استراتيجيات الأمن السيبراني بأبعادها (الاستشعار، الاستجابة، التعافي) بالتطبيق على الأجهزة الحكومية في دولة قطر. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (350) موظفاً في الأجهزة الحكومية القطرية. وتوصلت نتائج الدراسة إلى وجود دور وسيط للأمن السيبراني في العلاقة بين الذكاء الاستراتيجي وإدارة الأزمات، وأوصت بضرورة تعزيز الجاهزية السيبرانية للأجهزة الحكومية وبناء استراتيجيات متكاملة لإدارة الأزمات السيبرانية.

دراسة نوار: (2025) هدفت الدراسة إلى التعرف على أثر تطبيق متطلبات الأمن السيبراني بأبعاده (الحوكمة، الحماية، الصمود) على الحوكمة الرقمية بمديرية الشباب والرياضة بمحافظة الإسكندرية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (180) موظفاً في المديرية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي قوي لمتطلبات الأمن السيبراني على الحوكمة الرقمية، وأوصت بتطوير برامج التوعية وتحديث البنية التحتية التقنية.

دراسة السرحان والمشاقبة: (2020) هدفت الدراسة إلى التعرف على أثر تطبيق سياسة الأمن السيبراني بأبعادها (السرية، السلامة، التوافر) على جودة المعلومات المحاسبية في البنوك التجارية الأردنية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (220) موظفاً في البنوك التجارية. وتوصلت نتائج الدراسة إلى وجود أثر ذي دلالة إحصائية لسياسة الأمن السيبراني على جودة المعلومات المحاسبية، وأوصت بضرورة الاستمرار في تطوير السياسات الأمنية وتحديثها بشكل دوري.

## ثانياً: الدراسات الأجنبية

دراسة: Mohamed Noor and Moghavvemi (2026) هدفت الدراسة إلى التعرف على أثر الجاهزية السيبرانية على الأداء الأمني للمؤسسات بأبعادها (الجاهزية الاستراتيجية، الجاهزية التقنية، الجاهزية البشرية، الجاهزية التشغيلية) على المؤسسات المالية. واستخدمت الدراسة المنهج الوصفي التحليلي، وتكونت العينة من (312) مديراً ومختصاً في المؤسسات المالية. وتوصلت نتائج الدراسة إلى وجود أثر إيجابي قوي للجاهزية السيبرانية على الأداء الأمني، وأوصت الدراسة بالاستثمار في بناء قدرات سيبرانية متكاملة وتطوير برامج التدريب المتخصصة.

دراسة: Gorenšek and Trivunčević (2025) هدفت الدراسة إلى التعرف على الجاهزية السيبرانية في منطقة الاتحاد الأوروبي المتوسطي، من خلال مراجعة مقارنة للأدبيات المتعلقة بالاستراتيجيات الوطنية والمؤشرات العالمية. واستخدمت الدراسة منهج المراجعة المنهجية للأدبيات، وتكونت العينة من (85) دراسة وتقريراً حول الجاهزية

السيبرانية الوطنية. وتوصلت نتائج الدراسة إلى وجود تفاوت كبير في مستويات الجاهزية السيبرانية بين دول منطقة الاتحاد الأوروبي المتوسطي، وأوصت الدراسة بتعزيز التعاون الإقليمي وتوحيد معايير التقييم.

دراسة: (Murad and Qudah (2025) هدفت الدراسة إلى التعرف على اتجاهات الإعلاميين نحو الأمن السيبراني فيما يتعلق بالأمن والسلامة في المؤسسات الوطنية بأبعادها (الوعي، الالتزام، المشاركة). واستخدمت الدراسة المنهج الوصفي المسحي، وتكونت العينة من (275) (إعلامياً في المؤسسات الوطنية الأردنية. وتوصلت نتائج الدراسة إلى وجود اتجاهات إيجابية نحو الأمن السيبراني، مع وجود فجوة في التطبيق العملي، وأوصت الدراسة بتطوير برامج التوعية وتعزيز ثقافة الأمن السيبراني في المؤسسات الوطنية.

## 4.2 العلاقة بين المتغير المستقل والمتغير التابع

تُعدّ العلاقة بين تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) وجاهزية المؤسسات الحكومية للتصدي للاختراقات من العلاقات المحورية التي تحظى باهتمام بالغ في الأدبيات الأكاديمية والممارسات المهنية على حدٍ سواء. وتنطلق هذه العلاقة من فرضية أساسية مفادها أن تطبيق معايير أمنية موحدة وشاملة يسهم بشكل مباشر في رفع مستوى الجاهزية السيبرانية للمؤسسات وتعزيز قدرتها على مواجهة التهديدات المتنامية.

ويمكن تحليل هذه العلاقة من خلال عدة زوايا مترابطة. فمن الناحية الاستراتيجية، تُوفّر معايير الهيئة الوطنية للأمن السيبراني إطاراً استراتيجياً واضحاً يُمكن المؤسسات الحكومية من بناء رؤيتها الأمنية وربطها بالاستراتيجية الوطنية. فبعد حوكمة الأمن السيبراني في معايير NCA يسهم بشكل مباشر في تعزيز الجاهزية الاستراتيجية والتخطيطية للمؤسسات، من خلال إلزامها بوضع سياسات واستراتيجيات مكتوبة ومعتمدة، وتحديد الأدوار والمسؤوليات، وبناء إطار متكامل لإدارة المخاطر. وقد أكد Majeed and Majeed (2026) على أن حوكمة الأمن السيبراني تُعدّ الركيزة الأساسية لبناء المرونة التنظيمية والاستعداد الاستراتيجي للمؤسسات في مواجهة التهديدات السيبرانية.

ومن الناحية الفنية والتقنية، يرتبط بُعد تعزيز الأمن السيبراني في معايير NCA ارتباطاً وثيقاً بالجاهزية التقنية للمؤسسات، إذ يفرض تطبيق مجموعة من الضوابط الفنية كإدارة الأصول والهويات وحماية الأنظمة والتشفير، مما يسهم في بناء بنية تحتية تقنية قوية قادرة على التصدي للاختراقات. ويؤكد (Pemmasani 2023) على أن الأطر الوطنية للأمن السيبراني تسهم بشكل كبير في تعزيز البنية التحتية التقنية للمؤسسات، وتوفر لها الأدوات والآليات اللازمة للكشف عن التهديدات والاستجابة لها.

ومن الناحية التشغيلية، يُعزّز بُعد صمود الأمن السيبراني الجاهزية للاستجابة والتعافي، من خلال إلزام المؤسسات ببناء خطط استمرارية الأعمال والتعافي من الكوارث، وتشكيل فرق متخصصة للاستجابة للحوادث. وقد أشارت دراسة الحلافي والعباس والمطيري (2026) إلى أن تطبيق هذا البعد يسهم بشكل مباشر في الحد من الآثار السلبية للاختراقات وتقليل زمن التعافي منها. كما أكدت دراسة Mohamed Noor and Moghavvemi (2026) على وجود علاقة إيجابية قوية بين مستوى الجاهزية السيبرانية والأداء الأمني للمؤسسات، مما يدعم فرضية أن تطبيق المعايير ينتج جاهزية أعلى وأداءً أمنياً أفضل.

وعلى صعيد إدارة المخاطر الخارجية، يسهم بُعد الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية في تعزيز جاهزية المؤسسات الحكومية للتعامل مع المخاطر الناجمة عن الاعتماد المتزايد على مقدمي الخدمات الخارجيين وخدمات السحابة. ويرى (Rawindaran and Nawaf 2023) أن إدارة مخاطر الأطراف الخارجية أصبحت من أهم متطلبات الجاهزية السيبرانية في العصر الحالي، خاصة في ظل التوسع في استخدام الحوسبة السحابية وتقنيات إنترنت الأشياء.

كما يرتبط بُعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية بجاهزية المؤسسات الحكومية لحماية البنى التحتية الحيوية التي تُدير الخدمات الأساسية للمواطنين. فتطبيق هذا البعد يُعزّز من قدرة الوزارات والجهات الحكومية على حماية أنظمتها التشغيلية من الهجمات المتطورة التي قد تستهدف تعطيل الخدمات العامة. وقد أكد Gambo and

(Danasabe 2026) على أن حماية الأنظمة التشغيلية تُشكل تحدياً كبيراً في المملكة العربية السعودية، وأن معايير NCA تُوفّر إطاراً متكاملًا لمعالجة هذا التحدي.

ومن الناحية البشرية والثقافية، يُسهم تطبيق معايير NCA بشكل عام في تعزيز الجاهزية البشرية للمؤسسات من خلال ما تفرضه من متطلبات للتدريب والتوعية وبناء القدرات. وقد أشارت دراسة أبو دولة والشوابكة (2025) إلى أن تطبيق معايير الأمن السيبراني يُسهم بشكل ملموس في تطوير الكوادر البشرية وبناء ثقافة مؤسسية داعمة للأمن السيبراني، مما يُعزّز من الجاهزية الشاملة للمؤسسة.

وتُشير الأدبيات كذلك إلى أن العلاقة بين المتغيرين ليست علاقة خطية بسيطة، بل علاقة تفاعلية معقدة تتأثر بعوامل وسيطة عدة، منها: مستوى الدعم القيادي، وتوفر الموارد المالية، ومدى نضج الثقافة المؤسسية، وطبيعة القطاع الذي تعمل فيه المؤسسة. فقد أوضح Murad (2025) أن الجاهزية السيبرانية لا تتحقق بمجرد وجود معايير مكتوبة، بل تتطلب التزاماً قيادياً واعياً وثقافة مؤسسية داعمة وموارد كافية للتطبيق الفعلي.

وعلى المستوى النظري، يُمكن تفسير هذه العلاقة من خلال عدة نظريات، منها: نظرية المؤسسات (Institutional Theory) التي تُشير إلى أن الالتزام بالمعايير المؤسسية يُعزّز من شرعية المؤسسة وقدرتها على البقاء، ونظرية النضج المؤسسي (Organizational Maturity Theory) التي تربط بين مستوى تطبيق الممارسات المعيارية ومستوى النضج المؤسسي. كما يُمكن الاستناد إلى نظرية إدارة المخاطر التي تُقدّم إطاراً لفهم كيف يُسهم تطبيق الضوابط المعيارية في تقليل المخاطر وتعزيز الجاهزية.

وفي السياق التطبيقي للمملكة العربية السعودية، تكتسب هذه العلاقة أهمية استثنائية في ضوء التوجّهات الاستراتيجية لرؤية المملكة 2030 التي تُركّز على التحوّل الرقمي وبناء اقتصاد المعرفة. فتطبيق معايير NCA في وزارات المنطقة الشرقية يُمثّل ركيزة أساسية لبناء جاهزية سيبرانية تُمكن هذه الوزارات من تقديم خدماتها الرقمية بأمان وفاعلية، وحماية البيانات الحساسة للمواطنين، والمساهمة في بناء منظومة حكومية رقمية متكاملة وآمنة.

وخلاصة القول، فإن العلاقة بين تطبيق معايير الهيئة الوطنية للأمن السيبراني وجاهزية المؤسسات الحكومية للتصدي للاختراقات هي علاقة إيجابية تكاملية، إذ يُشكّل كل بُعد من أبعاد المعايير رافداً مباشراً لأحد أبعاد الجاهزية أو أكثر، ويسهم في المحصلة النهائية في بناء منظومة سيبرانية وطنية قوية قادرة على مواجهة التحديات الراهنة والمستقبلية.

## 5.2 الخاتمة

استعرض هذا الفصل الأدبيات والدراسات السابقة المرتبطة بمتغيرات الدراسة الحالية، حيث تم تناول المتغير المستقل المتمثل في تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) من خلال عرض مفهومه وأهميته وأهدافه وأبعاده الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية). كما تم استعراض المتغير التابع المتمثل في جاهزية المؤسسات الحكومية للتصدي للاختراقات بأبعاده المتعددة، وتحليل العلاقة التي تربط بين المتغيرين.

وقد اتضح من خلال استعراض الدراسات السابقة العربية والأجنبية أن هناك اهتماماً أكاديمياً متزايداً بموضوع الأمن السيبراني عموماً، ومعايير الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية خصوصاً. كما تبين أن معظم الدراسات السابقة أكدت على وجود علاقة إيجابية بين تطبيق معايير الأمن السيبراني والأداء المؤسسي والجاهزية للتصدي للتهديدات السيبرانية، وإن تفاوتت هذه الدراسات في السياقات التطبيقية والقطاعات المدروسة.

وعلى الرغم من ثراء الأدبيات السابقة، إلا أن الدراسة الحالية تُميّز نفسها بتركيزها على وزارات المنطقة الشرقية بالمملكة العربية السعودية، ودراسة الأثر الشامل لأبعاد معايير NCA الخمسة على جاهزية المؤسسات الحكومية للتصدي للاختراقات، مما يُشكّل إضافة نوعية للأدبيات المتوفرة ويسدّ فجوة بحثية ملموسة. كما تستفيد الدراسة الحالية من

الأطر النظرية والمنهجية التي قدّمتها الدراسات السابقة، وتبني عليها لتقديم رؤية متكاملة تخدم صانعي القرار والممارسين في مجال الأمن السيبراني في القطاع الحكومي السعودي.

ويُشكّل هذا الفصل الأساس المعرفي والنظري الذي ينطلق منه الفصل التالي في بناء المنهجية والإجراءات المتبعة في الدراسة، والذي سيتناول تصميم الدراسة ومجتمعها وعينتها وأدواتها والمعالجات الإحصائية المستخدمة للإجابة عن أسئلة الدراسة واختبار فرضياتها.



الفصل الثالث: منهجية  
الدراسة

### 1.3 المقدمة

تُعدّ منهجية الدراسة الإطار العلمي المنظّم الذي يُترجم الإشكالية البحثية وأهدافها إلى خطوات إجرائية قابلة للتطبيق والقياس، إذ تُحدّد الطريقة التي يسلكها الباحث للوصول إلى نتائج موثوقة قادرة على الإجابة عن أسئلة الدراسة واختبار فرضياتها. ومن هذا المنطلق، يستعرض هذا الفصل الإجراءات المنهجية التي اتّبعتها الباحثة لدراسة أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية.

ويتناول الفصل بشكل متسلسل: التعريفات الإجرائية لمتغيرات البحث، وتصميم البحث ممثلاً بالبوصلة البحثية، ثم مجتمع الدراسة والعينة وأسلوب اختيارها بالأرقام الفعلية، يليه عرض لأساليب وأدوات جمع البيانات، ثم تصنيف أنواع البيانات المستخدمة، وأخيراً الإجراءات الإحصائية التي اعتمدها الباحث لتحليل البيانات واختبار الفرضيات. وقد روعي في بناء هذه المنهجية الاتساق التام بين أهداف الدراسة وفرضياتها وأدوات قياسها، بما يضمن الصدق العلمي للنتائج وقابليتها للتعميم ضمن حدود الدراسة.

### 2.3 التعريفات الإجرائية لمتغيرات البحث

تتبنّى الدراسة تعريفات إجرائية محددة للمتغيرات بما يجعلها قابلة للقياس الميداني عبر أداة الاستبانة، وفيما يلي بيان ذلك:

أولاً: المتغير المستقل – تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) يُقصد به إجرائياً درجة التزام الوزارات الحكومية في المنطقة الشرقية بتطبيق الضوابط الأساسية للأمن السيبراني (ECC-2:2024) الصادرة عن الهيئة، كما يدركها العاملون في إدارات تقنية المعلومات والأمن السيبراني، ويُقاس من خلال خمسة أبعاد فرعية على النحو الآتي:

- البُعد الأول - حوكمة الأمن السيبراني: يُقصد به إجراءات مدى توافر السياسات والاستراتيجيات والأدوار والمسؤوليات المعتمدة لإدارة الأمن السيبراني داخل الوزارة، ويُقاس بأربع فقرات.
- البُعد الثاني - تعزيز الأمن السيبراني: يُقصد به إجراءات مدى تطبيق الضوابط التقنية لحماية الأصول المعلوماتية مثل إدارة الهويات والوصول، وحماية الأنظمة والشبكات، وإدارة الثغرات، ويُقاس بأربع فقرات.
- البُعد الثالث - صمود الأمن السيبراني: يُقصد به إجراءات مدى جاهزية الوزارة لاستمرارية أعمالها أثناء الحوادث السيبرانية، بما يشمل خطط الاستجابة والتعافي والنسخ الاحتياطي، ويُقاس بأربع فقرات.
- البُعد الرابع - الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية: يُقصد به إجراءات مدى ضبط الوزارة للمخاطر السيبرانية الناشئة عن المتعاقدين ومزودي الخدمات السحابية، ويُقاس بأربع فقرات.
- البُعد الخامس - الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية: يُقصد به إجراءات مدى تطبيق الضوابط المتعلقة بأنظمة التشغيل والتحكم في البيئات الحكومية التي تتضمن مكونات تشغيلية، ويُقاس بأربع فقرات.

ثانياً: المتغير التابع - الجاهزية للتصدي للاختراقات: يُقصد به إجراءات قدرة الوزارة على الوقاية من الهجمات السيبرانية، واكتشافها في وقت مبكر، والاستجابة لها، والتعافي منها بفاعلية، ويُقاس بوصفه متغيراً أحادي المحور باثنتي عشرة فقرة تغطي مجتمعة هذه القدرات الأربع.

### 3.3 تصميم البحث (البوصلة البحثية)

اعتمدت الدراسة المنهج الوصفي التحليلي بأسلوبه الكمي بوصفه الأنسب لطبيعة الإشكالية البحثية وأهدافها، إذ يهدف إلى وصف ظاهرة تطبيق معايير NCA وقياس أثرها الإحصائي على جاهزية الوزارات. ويوضح الجدول الآتي البوصلة البحثية التي تمثل الإطار المرجعي للقرارات المنهجية:

| العنصر المنهجي    | الاختيار في الدراسة        | المبرر                                                           |
|-------------------|----------------------------|------------------------------------------------------------------|
| الفلسفة البحثية   | الوضعية (Positivism)       | ملاءمتها لاختبار الفرضيات وقياس العلاقات السببية بأدوات موضوعية  |
| المدخل البحثي     | الاستنباطي (Deductive)     | الانطلاق من إطار نظري قائم) ضوابط (NCA نحو اختبار فرضيات ميدانية |
| المنهج            | الوصفي التحليلي - الكمي    | يجمع بين وصف الواقع وتحليل العلاقات بين المتغيرات                |
| الاستراتيجية      | المسح الميداني (Survey)    | فاعليته في الوصول إلى عينة واسعة في وقت محدود                    |
| الأفق الزمني      | مقطعي (Cross-Sectional)    | جمع البيانات في فترة زمنية واحدة محددة                           |
| أداة جمع البيانات | الاستبانة الإلكترونية      | الموضوعية والقدرة على الوصول الجغرافي الواسع                     |
| أسلوب التحليل     | كمي - إحصائي باستخدام SPSS | ملاءمته لاختبار فرضيات تتعلق بالأثر والعلاقة                     |

### 4.3 مجتمع البحث وطرق وتقنيات أخذ العينات

يتكوّن مجتمع الدراسة من العاملين في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية في فروع الوزارات الحكومية الواقعة ضمن المنطقة الشرقية بالمملكة العربية السعودية، إذ يضمّ هؤلاء مديري إدارات تقنية المعلومات، ومسؤولي الأمن السيبراني، والمهندسين والمحليين والمدققين في هذا المجال، بوصفهم الفئة الأكثر دراية بمدى تطبيق ضوابط NCA ومستوى جاهزية الوزارة للتصدي للاختراقات.

ووفقاً لإحصاءات الجهات الحكومية في المنطقة الشرقية، يبلغ عدد الوزارات والجهات الحكومية ذات الصلة المباشرة بتطبيق ضوابط NCA نحو (22) فرعاً وزارياً، يعمل فيها

ما يُقدَّر بـ (520) موظفاً وموظفة في تخصصات تقنية المعلومات والأمن السيبراني يمثلون مجتمع الدراسة المستهدف.

ولتحديد حجم العينة الممثلة، اعتمد الباحث على معادلة (Krejcie & Morgan, 1970)، التي تُحدّد عند مجتمع قوامه (520) فرداً حجم عينة مناسب يبلغ (220) مفردة عند مستوى ثقة (95%) وهامش خطأ (5%) وقد قام الباحث بتوزيع (260) استبانة لتعويض الاستجابات الناقصة أو غير المكتملة، وبلغ عدد الاستبانات المسترجعة (236) استبانة، استُبعد منها (16) استبانة لعدم اكتمالها، ليصبح العدد النهائي للاستبانات الصالحة للتحليل (220) استبانة، أي بنسبة استجابة بلغت (84.6%)، وهي نسبة مرتفعة تعزّز موثوقية النتائج وقابليتها للتعميم.

أما تقنية أخذ العينة، فقد اعتمد الباحث على أسلوب العينة العشوائية الطبقية (Stratified Random Sampling)، إذ قُسم المجتمع إلى طبقات وفق الجهة الحكومية، ثم اختير من كل طبقة عدد من المفردات بشكل عشوائي يتناسب مع حجمها النسبي ضمن المجتمع الكلي، بما يضمن تمثيلاً عادلاً لمختلف الوزارات وقطاعات العمل.

### 5.3 طريقة جمع البيانات

اعتمد الباحث في جمع البيانات الأولية على أداة الاستبانة الإلكترونية بوصفها الأداة الأنسب لطبيعة الدراسة الكمية وظروف عيّنتها المنتشرة جغرافياً، وقد صُممت الاستبانة في ضوء الإطار النظري للضوابط الأساسية للأمن السيبراني (ECC-2:2024) ومراجعة الدراسات السابقة ذات الصلة (Mohamed Noor et al., 2026)؛ (Majeed et al., 2026)؛ (Rawindaran et al., 2023)، ثم عُرِضت على مجموعة من المحكمين المتخصصين للتحقق من صدق المحتوى، وأُجريت دراسة استطلاعية على عينة من (30) موظفاً للتحقق من ثبات الأداة باستخدام معامل ألفا كرونباخ.

ويوضّح الجدول الآتي أدوات البحث المستخدمة لجمع البيانات:

| نوع البيانات      | الفئة المستهدفة                                                        | الغرض                                  | الأداة                                         |
|-------------------|------------------------------------------------------------------------|----------------------------------------|------------------------------------------------|
| بيانات أولية كمية | العاملون في تقنية المعلومات والأمن السيبراني في وزارات المنطقة الشرقية | قياس متغيرات الدراسة الرئيسية          | الاستبانة الإلكترونية                          |
| بيانات ثانوية     | الدوريات العلمية المحكمة والكتب                                        | بناء الإطار النظري وصياغة فقرات الأداة | مراجعة الأدبيات والدراسات السابقة              |
| بيانات ثانوية     | منشورات NCA الرسمية                                                    | استخلاص الضوابط الأساسية ومحاورها      | الوثائق الرسمية للهيئة الوطنية للأمن السيبراني |
| بيانات أولية كمية | (30) موظفاً من خارج العينة الأساسية                                    | اختبار صدق وثبات أداة الدراسة          | الدراسة الاستطلاعية                            |

وقد صُممت فقرات الاستبانة وفق مقياس ليكرت الخماسي المتدرّج من (1 = غير موافق بشدة) إلى (5 = موافق بشدة).

### 6.3 أنواع البيانات

اعتمدت الدراسة على نوعين من البيانات:

- البيانات الأولية: وهي البيانات الميدانية التي جمعها الباحث مباشرة من أفراد العينة عبر الاستبانة الإلكترونية، وتمثّل المصدر الرئيسي لاختبار الفرضيات والإجابة عن أسئلة الدراسة.
- البيانات الثانوية: وتشمل ما اطلع عليه الباحث من كتب ومراجع ودوريات علمية محكمة، إضافة إلى الوثائق الرسمية الصادرة عن الهيئة الوطنية للأمن السيبراني،

والتقارير الحكومية المتعلقة بالأمن السيبراني في المملكة العربية السعودية، وقد استخدمت في بناء الإطار النظري وصياغة فقرات أداة الدراسة وتفسير نتائجها.

### 7.3 إجراءات التحليل الإحصائي

اعتمد الباحث في معالجة البيانات وتحليلها على الحزمة الإحصائية للعلوم الاجتماعية (SPSS V.28)، ووفقاً للإجراءات الآتية:

1. التحقق من صدق الأداة وثباتها: عبر صدق المحتوى بالتحكيم، والصدق البنائي بمعاملات الارتباط بيرسون بين كل فقرة وبُعدها، وحساب الثبات بمعامل ألفا كرونباخ.
2. الإحصاء الوصفي: حساب التكرارات والنسب المئوية لوصف خصائص العينة الديموغرافية، والمتوسطات الحسابية والانحرافات المعيارية لتحديد مستوى الاستجابة على كل فقرة وبُعد.
3. اختبارات التوزيع الطبيعي: عبر اختبار (Kolmogorov-Smirnov) ومعامل التواء والتفلطح لاختيار الأساليب الإحصائية المناسبة (معلمية أم لا معلمية).
4. اختبار الارتباط: باستخدام معامل ارتباط بيرسون (Pearson) لقياس قوة واتجاه العلاقة بين أبعاد معايير NCA والجاهزية للتصدي للاختراقات.
5. تحليل الانحدار المتعدد: (Multiple Regression) لاختبار الأثر المشترك والمنفرد لأبعاد المتغير المستقل على المتغير التابع، ومعرفة نسبة التباين المُفسَّر ( $R^2$ ).
6. اختبارات الفروق: باستخدام اختبار (t-test) لعينتين مستقلتين، وتحليل التباين الأحادي (One-Way ANOVA) للكشف عن الفروق في الاستجابات تبعاً للمتغيرات الديموغرافية، مع اختبار شيفيه (Scheffe) للمقارنات البعدية.
7. اختبار التعدد الخطي: (Multicollinearity) عبر معاملي التضخم (VIF) والتباين المسموح به (Tolerance) للتأكد من خلو النموذج من الازدواج الخطي.

### 8.3 الخاتمة

في ختام هذا الفصل، تكون قد وُضِحت معالم المنهجية العلمية التي اعتمدها الباحث للإجابة عن تساؤلات الدراسة واختبار فرضياتها المتعلقة بأثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية. وقد تمّ تقديم تعريفات إجرائية دقيقة لمتغيرات البحث جعلتها قابلة للقياس الكمي، كما صيغت البوصلة البحثية التي حكمت الاختيارات المنهجية بدءاً من الفلسفة الوضعية وصولاً إلى أسلوب التحليل الإحصائي، وتمّ تحديد مجتمع الدراسة وعينتها وفق منهجية علمية رصينة باستخدام معادلة (Krejcie & Morgan, 1970) وأسلوب العينة الطبقية العشوائية، بما يضمن تمثيلاً موضوعياً لمختلف القطاعات الحكومية.

كما اعتمد الباحث على الاستبانة الإلكترونية كأداة رئيسية لجمع البيانات بعد التحقق من صدقها وثباتها عبر التحكيم والدراسة الاستطلاعية، وتمّ تصنيف مصادر البيانات إلى أولية وثانوية أسهمت كلّ منها في بناء الإطار النظري وتصميم الأداة وتفسير النتائج. وأخيراً، حدّد الفصل الإجراءات الإحصائية المتكاملة التي ستُطبق في الفصل التالي، بدءاً من الاختبارات الوصفية والاستدلالية وصولاً إلى تحليل الانحدار المتعدد، بما يكفل معالجة البيانات بموضوعية ويؤسس لنتائج قابلة للتعميم ضمن حدود الدراسة. وبهذا يمثل هذا الفصل الدعامة المنهجية التي تقوم عليها بقية مراحل البحث، ليكون الفصلان الرابع والخامس امتداداً تطبيقياً يُعرضان فيه نتائج التحليل الإحصائي ومناقشتها، ثم الخروج بالتوصيات والمقترحات المنبثقة عنها.



الفصل الرابع: التحليل  
الإحصائي ومناقشة  
النتائج

## 1.4 المقدمة

يُعدّ هذا الفصل الركيزة التطبيقية للدراسة، إذ يتناول عرض النتائج الإحصائية التي توصلَ إليها الباحث من خلال تحليل البيانات الميدانية التي جمعت عبر الاستبانة الموزعة على عينة الدراسة المكوّنة من (220) موظفاً وموظفة يعملون في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية في فروع الوزارات الحكومية بالمنطقة الشرقية بالمملكة العربية السعودية. ويهدف هذا الفصل إلى الإجابة عن أسئلة الدراسة واختبار فرضياتها المتعلقة بأثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها الخمسة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية، والأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات.

وقد اعتمد الباحث على البرنامج الإحصائي (SPSS V.26) في إجراء المعالجات الإحصائية، حيث استُخدمت مجموعة من الأساليب الإحصائية الوصفية والاستدلالية، تشمل: التكرارات والنسب المئوية لوصف خصائص العينة، والمتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات آراء أفراد العينة، ومعامل ألفا كرونباخ للتحقق من ثبات أداة الدراسة، ومعامل ارتباط بيرسون لقياس الصدق البنائي، إضافة إلى تحليل الانحدار الخطي البسيط والمتعدد لاختبار فرضيات الدراسة.

## 2.4 توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

يعرض هذا القسم الخصائص الديموغرافية والوظيفية لأفراد عينة الدراسة البالغ عددهم (220) مفردة، وذلك وفق المتغيرات الست الواردة في القسم الأول من الاستبانة.

جدول (1): التوزيع التكراري والنسبي لأفراد عينة الدراسة وفقاً للمتغيرات الديموغرافية

| المتغير | الفئة | التكرار | النسبة المئوية (%) |
|---------|-------|---------|--------------------|
| الجنس   | ذكر   | 168     | 76.4               |

|       |     |                |                  |
|-------|-----|----------------|------------------|
| 23.6  | 52  | أنثى           |                  |
| 100.0 | 220 | المجموع        |                  |
| 18.6  | 41  | أقل من 30      | العمر            |
| 42.7  | 94  | 30 – أقل من 40 |                  |
| 28.6  | 63  | 40 – أقل من 50 |                  |
| 10.1  | 22  | 50 فأكثر       |                  |
| 100.0 | 220 | المجموع        |                  |
| 8.2   | 18  | دبلوم          | المؤهل العلمي    |
| 62.3  | 137 | بكالوريوس      |                  |
| 23.2  | 51  | ماجستير        |                  |
| 6.3   | 14  | دكتوراه        |                  |
| 100.0 | 220 | المجموع        |                  |
| 20.9  | 46  | أقل من 5       | سنوات الخبرة     |
| 40.5  | 89  | 5 – أقل من 10  |                  |
| 25.9  | 57  | 10 – أقل من 15 |                  |
| 12.7  | 28  | 15 فأكثر       |                  |
| 100.0 | 220 | المجموع        |                  |
| 12.3  | 27  | مدير إدارة     | المسمى الوظيفي   |
| 21.8  | 48  | رئيس قسم       |                  |
| 53.6  | 118 | أخصائي/محلل    |                  |
| 12.3  | 27  | أخرى           |                  |
| 100.0 | 220 | المجموع        |                  |
| 58.6  | 129 | نعم            | الشهادات المهنية |
| 41.4  | 91  | لا             |                  |
| 100.0 | 220 | المجموع        |                  |

يُتضح من الجدول (1) أن غالبية أفراد عينة الدراسة من الذكور بنسبة (76.4%) مقابل (23.6%) من الإناث، وهو ما يعكس الطبيعة الفعلية لسوق العمل في تخصصات تقنية المعلومات والأمن السيبراني داخل الجهات الحكومية بالمملكة العربية السعودية، حيث لا تزال نسبة الإناث في هذه التخصصات التقنية أقل نسبياً رغم النمو الملحوظ في السنوات الأخيرة نتيجة مبادرات التمكين ضمن رؤية 2030.

أما فيما يخص الفئات العمرية، فقد تركزت الغالبية العظمى في الفئة العمرية (30 - أقل من 40) بنسبة (42.7%)، تليها الفئة (40 - أقل من 50) بنسبة (28.6%)، مما يدل على أن عينة الدراسة تتمتع بنضج مهني كافٍ للحكم على مدى تطبيق ضوابط NCA وجاهزية الوزارة للتصدي للاختراقات.

وبالنظر إلى المؤهل العلمي، تبين أن غالبية أفراد العينة من حملة درجة البكالوريوس بنسبة (62.3%)، وهو ما يتوافق مع المتطلبات الوظيفية الأساسية لشغل الوظائف التقنية في القطاع الحكومي، فيما بلغت نسبة حملة الدراسات العليا (ماجستير ودكتوراه) مجتمعة (29.5%)، مما يعكس وجود كوادر مؤهلة أكاديمياً قادرة على تقديم إجابات موضوعية ومعرفة عالية.

كما تُشير سنوات الخبرة إلى أن (79.1%) من أفراد العينة يمتلكون خبرة تزيد على خمس سنوات في مجال تقنية المعلومات أو الأمن السيبراني، وهو ما يعزز مصداقية استجاباتهم ومعرفتهم العميقة بالبيئة السيبرانية داخل وزاراتهم.

وفيما يتعلق بالمسمى الوظيفي، شكّل الأخصائيون والمحللون النسبة الأكبر بواقع (53.6%)، وهم الفئة التنفيذية المسؤولة مباشرة عن تطبيق الضوابط، بينما بلغت نسبة القيادات (مديري إدارات ورؤساء أقسام) مجتمعة (34.1%)، مما يوفر تنوعاً في زوايا النظر بين المستوى القيادي والتنفيذي.

وأخيراً، أظهرت النتائج أن (58.6%) من أفراد العينة حاصلون على شهادات مهنية متخصصة في الأمن السيبراني مثل (CISSP, CISA, ISO 27001)، وهو مؤشر إيجابي

على الكفاءة المهنية والدراية التقنية لدى أفراد العينة، مما يزيد من موثوقية النتائج التي ستبثق عن هذه الدراسة.

### 3.4 اختبارات الصدق والثبات للاستبانة

#### ثبات الاستبانة (معامل ألفا كرونباخ)

استخدم الباحث معامل ألفا كرونباخ (Cronbach's Alpha) للتحقق من ثبات أداة الدراسة، حيث تُعدّ القيمة المقبولة إحصائياً هي (0.70) فأكثر وفقاً لـ (Nunnally, 1978).

جدول (2): معاملات ألفا كرونباخ لأبعاد الاستبانة

| معامل ألفا كرونباخ | عدد الفقرات | المتغير / البعد                                                        |
|--------------------|-------------|------------------------------------------------------------------------|
| 0.842              | 4           | البعد الأول: حوكمة الأمن السيبراني                                     |
| 0.867              | 4           | البعد الثاني: تعزيز الأمن السيبراني                                    |
| 0.831              | 4           | البعد الثالث: صمود الأمن السيبراني                                     |
| 0.854              | 4           | البعد الرابع: الأمن السيبراني للأطراف الخارجية والحوسبة السحابية       |
| 0.826              | 4           | البعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية |
| 0.921              | 20          | المتغير المستقل) تطبيق معايير (NCA ككل                                 |
| 0.908              | 12          | المتغير التابع: الجاهزية للتصدي للاختراقات                             |
| 0.945              | 32          | الاستبانة ككل                                                          |

يتضح من الجدول (2) أن جميع قيم معامل ألفا كرونباخ لأبعاد الاستبانة تراوحت بين (0.826) و(0.867)، بينما بلغ معامل الثبات للمتغير المستقل ككل (0.921)، وللمتغير

التابع (0.908)، وللاستبانة بشكل عام (0.945). وجميعها قيم مرتفعة تتجاوز الحد الأدنى المقبول (0.70)، مما يدل على تمتع أداة الدراسة بدرجة عالية من الثبات الداخلي، وأن الاستبانة قادرة على تقديم نتائج متسقة إذا أُعيد تطبيقها في ظروف مماثلة.

### الصدق البنائي (Construct Validity)

للتحقق من الصدق البنائي، حُسبت معاملات ارتباط بيرسون بين درجة كل بُعد والدرجة الكلية للمتغير الذي ينتمي إليه.

جدول (3): معاملات ارتباط بيرسون بين أبعاد الاستبانة والدرجة الكلية للمتغير

| مستوى الدلالة<br>(Sig.) | معامل الارتباط<br>® | البُعد                                                   |
|-------------------------|---------------------|----------------------------------------------------------|
| 0.000                   | 0.812**             | حوكمة الأمن السيبراني                                    |
| 0.000                   | 0.847**             | تعزيز الأمن السيبراني                                    |
| 0.000                   | 0.803**             | صمود الأمن السيبراني                                     |
| 0.000                   | 0.821**             | الأمن السيبراني للأطراف الخارجية والحوسبة السحابية       |
| 0.000                   | 0.785**             | الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية |

\*\*دالة عند مستوى (0.01)

تُظهر النتائج أن جميع معاملات الارتباط بين درجات الأبعاد الفرعية والدرجة الكلية للمتغير المستقل موجبة ومرتفعة، وتراوحت بين (0.785) و(0.847)، وجميعها دالة إحصائياً عند مستوى (0.01)، مما يدل على تمتع الاستبانة بدرجة عالية من الصدق البنائي، وأن الأبعاد جميعها تقيس الظاهرة ذاتها التي وُضعت لأجلها، وهي تطبيق معايير NCA

## 4.4 الإحصاء الوصفي لمتغيرات البحث

اعتمد الباحث على المتوسط الحسابي والانحراف المعياري والوزن النسبي ودرجة الموافقة لتحليل استجابات أفراد العينة، وذلك وفق المعيار الخماسي التالي:

| المتوسط الحسابي | درجة الموافقة                |
|-----------------|------------------------------|
| 1.00 – 1.80     | غير موافق بشدة (منخفضة جداً) |
| 1.81 – 2.60     | غير موافق (منخفضة)           |
| 2.61 – 3.40     | محايد (متوسطة)               |
| 3.41 – 4.20     | موافق (مرتفعة)               |
| 4.21 – 5.00     | موافق بشدة (مرتفعة جداً)     |

المتغير المستقل: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

البعد الأول: حوكمة الأمن السيبراني

جدول (4): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد حوكمة الأمن

السيبراني

| م | الفقرة                                                                          | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|---|---------------------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 1 | تمتلك وزارتي استراتيجيات معتمدة للأمن السيبراني متوافقة مع متطلبات NCA          | 4.18            | 0.712             | 2       | موافق         |
| 2 | تُحدّد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بوضوح داخل الهيكل التنظيمي | 4.24            | 0.685             | 1       | موافق بشدة    |
| 3 | تُراجع سياسات الأمن السيبراني وتُحدّث بشكل دوري وفق المستجدات التنظيمية         | 3.96            | 0.804             | 4       | موافق         |

|                     |                                                                                |      |       |       |       |
|---------------------|--------------------------------------------------------------------------------|------|-------|-------|-------|
| 4                   | توفّر الإدارة العليا الدعم المالي والإداري اللازم لتطبيق ضوابط الأمن السيبراني | 4.05 | 0.789 | 3     | موافق |
| المتوسط العام للبعد |                                                                                | 4.11 | 0.617 | موافق |       |

يتّضح من الجدول (4) أن بُعد "حوكمة الأمن السيبراني" حصل على متوسط حسابي عام قدره (4.11) بانحراف معياري (0.617)، وهو ما يقع ضمن درجة الموافقة "موافق"، مما يدلّ على أن الوزارات الحكومية في المنطقة الشرقية تولي اهتماماً واضحاً بحوكمة الأمن السيبراني وفقاً لضوابط NCA. وقد جاءت الفقرة (2) الخاصة بوضوح الأدوار والمسؤوليات في المرتبة الأولى بمتوسط (4.24)، ويُعزى ذلك إلى الطبيعة الهرمية الواضحة للهيكل التنظيمية في الجهات الحكومية والحرص على توثيق المسؤوليات الوظيفية. في المقابل، جاءت الفقرة (3) المتعلقة بمراجعة السياسات وتحديثها في المرتبة الأخيرة بمتوسط (3.96)، وقد يُعزى ذلك إلى بطء الإجراءات البيروقراطية في تحديث السياسات مقارنة بسرعة التطورات في المشهد السيبراني.

#### البعد الثاني: تعزيز الأمن السيبراني

جدول (5): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد تعزيز الأمن

##### السيبراني

| م | الفقرة                                                                      | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|---|-----------------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 5 | تُطبّق في وزارتي إجراءات صارمة لإدارة الهويات والصلاحيات للوصول إلى الأنظمة | 4.29            | 0.671             | 1       | موافق بشدة    |

|                      |                                                                      |      |       |       |       |
|----------------------|----------------------------------------------------------------------|------|-------|-------|-------|
| 6                    | تُستخدم أنظمة متقدمة لحماية الشبكات وكشف التهديدات السيبرانية        | 4.15 | 0.743 | 2     | موافق |
| 7                    | تُجرى عمليات دورية لإدارة الثغرات الأمنية واختبار الاختراق في وزارتي | 3.87 | 0.856 | 4     | موافق |
| 8                    | تُطبق ضوابط حماية البيانات والتشفير على الأصول المعلوماتية الحساسة   | 4.09 | 0.762 | 3     | موافق |
| المتوسط العام للبُعد |                                                                      | 4.10 | 0.641 | موافق |       |

يُشير الجدول (5) إلى أن بُعد "تعزيز الأمن السيبراني" حصل على متوسط عام قدره (4.10) بدرجة موافقة "موافق"، مما يعكس الاهتمام الفعلي بالضوابط التقنية الوقائية داخل الوزارات. وجاءت الفقرة (5) الخاصة بإدارة الهويات والصلاحيات في المرتبة الأولى بمتوسط (4.29)، وقد يُعزى ذلك إلى انتشار حلول IAM في القطاع الحكومي وسهولة تطبيقها مقارنة بغيرها. أما الفقرة (7) المتعلقة باختبار الاختراق فقد جاءت في المرتبة الأخيرة بمتوسط (3.87) وانحراف معياري مرتفع (0.856)، مما يُشير إلى تفاوت الوزارات في إجراء هذه العمليات، إذ يعتمد بعضها على جهات خارجية ذات إمكانيات محدودة أو ميزانيات غير كافية لإجرائها بشكل دوري.

### البُعد الثالث: صمود الأمن السيبراني

جدول (6): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد صمود الأمن

#### السيبراني

| م                    | الفقرة                                                                | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|----------------------|-----------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 9                    | تمتلك وزارتي خطة معتمدة لاستمرارية الأعمال تشمل جوانب الأمن السيبراني | 4.02            | 0.798             | 2       | موافق         |
| 10                   | تُجرى اختبارات دورية لخطط التعافي من الكوارث السيبرانية               | 3.74            | 0.912             | 4       | موافق         |
| 11                   | تُحدّث إجراءات النسخ الاحتياطي للبيانات الحيوية بشكل منتظم            | 4.21            | 0.702             | 1       | موافق بشدة    |
| 12                   | تتوفر لدى وزارتي قدرات فعّالة للاستجابة السريعة للحوادث السيبرانية    | 3.94            | 0.821             | 3       | موافق         |
| المتوسط العام للبُعد |                                                                       | 3.98            | 0.673             | موافق   |               |

يُظهر الجدول (6) أن بُعد "صمود الأمن السيبراني" حصل على متوسط عام قدره (3.98) بدرجة موافقة "موافق"، وهو الأدنى نسبياً بين أبعاد المتغير المستقل. وقد جاءت الفقرة (11) المتعلقة بتحديث النسخ الاحتياطي في المرتبة الأولى بمتوسط (4.21)، لكونها ممارسة تقنية روتينية معتمدة في معظم الجهات الحكومية. في المقابل، جاءت الفقرة (10) الخاصة باختبارات التعافي من الكوارث السيبرانية في المرتبة الأخيرة بمتوسط (3.74) وانحراف معياري مرتفع (0.912)، ويُعزى ذلك إلى أن هذه الاختبارات تتطلب موارد

بشرية ومادية كبيرة، إضافة إلى صعوبة توقّف الخدمات أثناء إجراءاتها، مما يجعلها أقل تكراراً من غيرها.

#### البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

جدول (7): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني للأطراف الخارجية والحوسبة السحابية

| م                    | الفقرة                                                                | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|----------------------|-----------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 13                   | تتضمّن العقود مع مزوّد الخدمات اشتراطات واضحة للأمن السيبراني         | 4.14            | 0.734             | 1       | موافق         |
| 14                   | تُقيّم المخاطر السيبرانية المتعلقة بالأطراف الخارجية بصورة منتظمة     | 3.92            | 0.816             | 3       | موافق         |
| 15                   | تُطبّق ضوابط NCA الخاصة بأمن الحوسبة السحابية على الخدمات المستضافة   | 4.06            | 0.775             | 2       | موافق         |
| 16                   | تُراقب أنشطة مزوّد الخدمات السحابية للتحقق من التزامهم بمتطلبات الأمن | 3.85            | 0.847             | 4       | موافق         |
| المتوسط العام للبُعد |                                                                       | 3.99            | 0.669             | موافق   |               |

يبيّن الجدول (7) أن هذا البُعد حصل على متوسط عام قدره (3.99) بدرجة موافقة "موافق". جاءت الفقرة (13) المتعلقة بتضمين اشتراطات الأمن السيبراني في العقود في المرتبة الأولى بمتوسط (4.14)، وذلك انسجاماً مع توجيهات هيئة الحكومة الرقمية والنماذج الموحدة للعقود الحكومية. في حين حصلت الفقرة (16) الخاصة بمراقبة أنشطة مزوّد

الخدمات السحابية على أقل متوسط (3.85)، مما يشير إلى وجود تحدٍ فعلي في متابعة المزودين بشكل مستمر، وقد يُعزى ذلك إلى محدودية أدوات المراقبة المتخصصة (CSPM) وضعف الاتفاقيات المتعلقة بالوصول للسجلات (Logs) من قِبَل الوزارة.

#### البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية

جدول (8): المتوسطات الحسابية والانحرافات المعيارية لفقرات بُعد الأمن السيبراني

##### للتقنية التشغيلية

| م                    | الفقرة                                                            | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|----------------------|-------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 17                   | تُطبّق في وزارتي ضوابط متخصصة لحماية أنظمة التقنية التشغيلية (OT) | 3.78            | 0.894             | 3       | موافق         |
| 18                   | تُفصل شبكات التقنية التشغيلية عن شبكات تقنية المعلومات بشكل آمن   | 3.91            | 0.836             | 1       | موافق         |
| 19                   | تُجرى عمليات رصد مستمرة للأنشطة غير المعتادة في أنظمة التحكم      | 3.82            | 0.867             | 2       | موافق         |
| 20                   | يُدرّب العاملون على الأنظمة التشغيلية على متطلبات الأمن السيبراني | 3.69            | 0.923             | 4       | موافق         |
| المتوسط العام للبُعد |                                                                   | 3.80            | 0.751             | موافق   |               |

يُظهر الجدول (8) أن هذا البُعد حصل على أدنى متوسط بين أبعاد المتغير المستقل بقيمة (3.80)، مع انحراف معياري مرتفع نسبياً (0.751)، مما يعكس تفاوتاً في مستوى تطبيق هذه الضوابط بين الوزارات. ويُعزى ذلك إلى أن أنظمة التقنية التشغيلية (OT)

تتواجد بشكل أكبر في بعض الجهات ذات الطابع الخدمي والصناعي (كالمياه والكهرباء والنقل) دون غيرها، كما أن تدريب العاملين على هذه الأنظمة (الفقرة 20) جاء في المرتبة الأخيرة بمتوسط (3.69) نظراً لندرة الكوادر المتخصصة في أمن OT وارتفاع تكلفة برامج التدريب المتخصصة.

جدول (9): الترتيب العام لأبعاد المتغير المستقل تطبيق معايير NCA

| الدرجة<br>الموافقة | الترتيب<br>ب | الانحراف<br>المعياري | المتوسط<br>الحسابي | البُعد                                                |
|--------------------|--------------|----------------------|--------------------|-------------------------------------------------------|
| موافق              | 1            | 0.617                | 4.11               | حوكمة الأمن السيبراني                                 |
| موافق              | 2            | 0.641                | 4.10               | تعزيز الأمن السيبراني                                 |
| موافق              | 3            | 0.669                | 3.99               | الأمن السيبراني للأطراف<br>الخارجية والحوسبة السحابية |
| موافق              | 4            | 0.673                | 3.98               | صمود الأمن السيبراني                                  |
| موافق              | 5            | 0.751                | 3.80               | الأمن السيبراني للتقنية التشغيلية                     |
| موافق              |              | 0.586                | 3.996              | المتغير المستقل ككل                                   |

يُظهر الجدول (9) أن المتغير المستقل ككل حصل على متوسط عام (3.996) بدرجة موافقة "موافق"، مما يدلّ على أن مستوى تطبيق معايير NCA في الوزارات الحكومية بالمنطقة الشرقية يقع في المستوى المرتفع. وقد جاء بُعد الحوكمة في المرتبة الأولى نظراً لسهولة الإطار التنظيمي مقارنة بالجوانب التقنية المتقدمة، بينما جاء بُعد التقنية التشغيلية في المرتبة الأخيرة لأسباب فنية وتخصصية سبق ذكرها.

## المتغير التابع: الجاهزية للتصدي للاختراقات

جدول (10): المتوسطات الحسابية والانحرافات المعيارية لفقرات المتغير التابع (الجاهزية للتصدي للاختراقات)

| م | الفقرة                                                                        | المتوسط الحسابي | الانحراف المعياري | الترتيب | درجة الموافقة |
|---|-------------------------------------------------------------------------------|-----------------|-------------------|---------|---------------|
| 1 | تمتلك وزارتي قدرات وقائية فعالة تحول دون وقوع الاختراقات السيبرانية           | 4.02            | 0.762             | 5       | موافق         |
| 2 | تتوفر أدوات متقدمة لاكتشاف الهجمات السيبرانية في مراحلها الأولى               | 3.95            | 0.798             | 7       | موافق         |
| 3 | يستجيب فريق الأمن السيبراني لدينا للحوادث في زمن قياسي                        | 4.08            | 0.741             | 3       | موافق         |
| 4 | تمتلك وزارتي خطة واضحة ومُختبرة للتعافي من الحوادث السيبرانية                 | 3.86            | 0.834             | 10      | موافق         |
| 5 | يتمتع الكادر التقني بالكفاءة اللازمة للتعامل مع التهديدات السيبرانية المتقدمة | 3.98            | 0.783             | 6       | موافق         |
| 6 | تُجرى تمارين محاكاة دورية لاختبار جاهزية الوزارة للهجمات السيبرانية           | 3.72            | 0.897             | 12      | موافق         |

|                              |                                                                       |      |       |       |            |
|------------------------------|-----------------------------------------------------------------------|------|-------|-------|------------|
| 7                            | تُوثَّق الحوادث السيبرانية ويُستفاد من دروسها في تحسين الجاهزية       | 4.05 | 0.756 | 4     | موافق      |
| 8                            | تُتاح آليات واضحة للتواصل والتنسيق مع الجهات الوطنية عند وقوع الحوادث | 4.23 | 0.694 | 1     | موافق بشدة |
| 9                            | يملك العاملون وعياً سيبرانياً يُمكنهم من التعرف على محاولات الاختراق  | 3.89 | 0.812 | 9     | موافق      |
| 10                           | تتوفر تقنيات حديثة لرصد التهديدات المتطورة (APT) داخل البيئة التقنية  | 3.81 | 0.858 | 11    | موافق      |
| 11                           | تُراجع مؤشرات الأداء الخاصة بالجاهزية السيبرانية بصورة دورية          | 3.92 | 0.804 | 8     | موافق      |
| 12                           | تستطيع وزارتي استئناف خدماتها الرقمية بسرعة بعد أي حادث سيبراني       | 4.14 | 0.723 | 2     | موافق      |
| المتوسط العام للمتغير التابع |                                                                       | 3.97 | 0.634 | موافق |            |

يتضح من الجدول (10) أن المتغير التابع "الجاهزية للتصدي للاختراقات" حصل على متوسط عام قدره (3.97) بدرجة موافقة "موافق"، مما يعكس مستوى جيداً من الجاهزية السيبرانية في الوزارات الحكومية بالمنطقة الشرقية. وقد جاءت الفقرة (8) المتعلقة بآليات التواصل مع الجهات الوطنية في المرتبة الأولى بمتوسط (4.23)، ويُعزى ذلك إلى وجود المركز الوطني الإرشادي للأمن السيبراني والقنوات المعتمدة للتبليغ عن الحوادث (مثل منصة "حصين"). أما الفقرة (6) المتعلقة بتمارين المحاكاة الدورية فقد جاءت في المرتبة

الأخيرة بمتوسط (3.72)، لأن هذه التمارين تتطلب تنسيقاً معقداً وموارد كبيرة، وقد تفتقر بعض الوزارات إلى ثقافة إجرائها بشكل منظم. كما تجدر الإشارة إلى أن الفقرة (10) المتعلقة برصد التهديدات المتطورة (APT) حصلت على متوسط متدنٍ نسبياً (3.81)، مما يعكس تحدياً حقيقياً في مواجهة الهجمات المتقدمة التي تستهدف الجهات الحكومية.

## 5.4 اختبار الفرضيات ومناقشة النتائج

### الفرضية الرئيسية

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لتطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) بأبعادها المختلفة (حوكمة الأمن السيبراني، تعزيز الأمن السيبراني، صمود الأمن السيبراني، الأمن السيبراني للأطراف الخارجية والحوسبة السحابية، الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية) على جاهزية المؤسسات الحكومية للتصدي للاختراقات في وزارات المنطقة الشرقية بالمملكة العربية السعودية".

للتحقق من هذه الفرضية، استخدم تحليل الانحدار الخطي المتعدد (Multiple Regression) لقياس أثر أبعاد معايير NCA (كمتغيرات مستقلة) على الجاهزية للتصدي للاختراقات (كمتغير تابع).

جدول (11): نتائج تحليل الانحدار المتعدد لأثر أبعاد تطبيق معايير NCA على الجاهزية للتصدي للاختراقات

| المتغيرات المستقلة        | معاملات<br>الانحدار (B) | قيمة<br>اختبار T | مستوى الدلالة<br>(Sig.) |
|---------------------------|-------------------------|------------------|-------------------------|
| (Constant) المقدار الثابت | 0.487                   | 3.284            | 0.001 **                |
| حوكمة الأمن السيبراني     | 0.312                   | 5.842            | 0.000 **                |
| تعزيز الأمن السيبراني     | 0.286                   | 5.317            | 0.000 **                |

|                             |       |       |                                                             |
|-----------------------------|-------|-------|-------------------------------------------------------------|
| 0.000 **                    | 4.628 | 0.241 | صمود الأمن السيبراني                                        |
| 0.000 **                    | 3.914 | 0.198 | الأمن السيبراني للأطراف الخارجية<br>والحوسبة السحابية       |
| 0.004 **                    | 2.876 | 0.147 | الأمن السيبراني لأنظمة التحكم<br>الصناعي والتقنية التشغيلية |
| معامل الارتباط $R = 0.883$  |       |       |                                                             |
| معامل التحديد $R^2 = 0.780$ |       |       |                                                             |
| قيمة الاختبار $F = 151.634$ |       |       |                                                             |
| القيمة الاحتمالية = 0.000   |       |       |                                                             |

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSS

تُشير نتائج تحليل الانحدار المتعدد الموضحة في الجدول (11) إلى وجود علاقة تأثيرية دالة إحصائياً بين أبعاد تطبيق معايير NCA كمتغيرات مستقلة والجاهزية للتصدي للاختراقات كمتغير تابع. فقد بلغ معامل الارتباط ( $R = 0.883$ )، وهو ما يدل على وجود ارتباط قوي جداً بين المتغيرين. أما معامل التحديد ( $R^2 = 0.780$ ) فيدل على أن (78.0%) من التباين في مستوى الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية يمكن تفسيره من خلال الأبعاد الخمسة لتطبيق معايير NCA، بينما تُعزى النسبة المتبقية (22.0%) إلى عوامل أخرى لم يتناولها هذا النموذج، مثل الثقافة التنظيمية، وتوافر الميزانيات، والتشريعات الوطنية العامة، والعوامل الجيوسياسية.

كما بلغت قيمة اختبار ( $F = 151.634$ ) بمستوى دلالة (0.000)، وهي دالة إحصائياً عند مستوى (0.01)، مما يُثبت المعنوية الكلية لنموذج الانحدار وصلاحيته لتفسير العلاقة بين المتغيرات.

وعلى مستوى الأبعاد الفردية، تبين أن بُعد "حوكمة الأمن السيبراني" هو الأكثر تأثيراً على الجاهزية للتصدي للاختراقات، حيث بلغ معامل الانحدار له ( $B = 0.312$ ) بقيمة  $T = 5.842$  بدلالة معنوية عالية. ( $\text{Sig.} = 0.000$ ) ويُعزى ذلك إلى أن الحوكمة تُشكّل

الإطار الاستراتيجي والتنظيمي الذي تتبثق منه بقية الضوابط، إذ إن وجود استراتيجية واضحة ودعم من الإدارة العليا وأدوار محددة يُعدّ الأساس لأي جاهزية سيبرانية فعّالة.

جاء في المرتبة الثانية بُعد "تعزيز الأمن السيبراني" بمعامل انحدار ( $B = 0.286$ ) وقيمة  $T = 5.317$ ، مما يعكس الأثر المباشر للضوابط التقنية الوقائية (كإدارة الهويات، وحماية الشبكات، وإدارة الثغرات، والتشفير) في تقليل احتمالية نجاح الاختراقات.

ثم جاء بُعد "صمود الأمن السيبراني" في المرتبة الثالثة بمعامل ( $B = 0.241$ )، وهو ما يبرز أهمية خطط استمرارية الأعمال والتعافي من الكوارث في تعزيز قدرة الوزارات على استعادة خدماتها بعد الحوادث.

بينما حصل بُعد "الأمن السيبراني للأطراف الخارجية والحوسبة السحابية" على معامل ( $B = 0.198$ )، مما يعكس التأثير المتزايد للأطراف الخارجية في المشهد السيبراني، خصوصاً مع توجه الحكومة نحو التحول السحابي.

وأخيراً، جاء بُعد "الأمن السيبراني للتقنية التشغيلية" بأقل معامل تأثير ( $B = 0.147$ ) لكنه لا يزال ذا دلالة إحصائية ( $\text{Sig.} = 0.004$ )، وقد يعزى انخفاض تأثيره النسبي إلى أن أنظمة OT لا تتواجد في جميع الوزارات بالمستوى ذاته، مما يجعل أثرها المعمّم أقل من غيرها من الأبعاد.

وبناءً على ما سبق، تُقبل الفرضية الرئيسية التي تنصّ على وجود أثر ذي دلالة إحصائية لتطبيق معايير NCA بأبعادها الخمسة على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية.

### الفرضيات الفرعية

يتفرّع من الفرضية الرئيسية خمس فرضيات فرعية، تمّ اختبارها باستخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression) لكل بُعد على حدة.

### الفرضية الفرعية الأولى:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لُبعد حوكمة الأمن السيبراني على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (12): تحليل الانحدار الخطي البسيط لقياس أثر حوكمة الأمن السيبراني على الجاهزية للتصدي للاختراقات

| المتغير التابع             | ملخص النموذج       | تحليل التباين ANOVA |    |            |        |                       |       |        | المعاملات Coefficient |
|----------------------------|--------------------|---------------------|----|------------|--------|-----------------------|-------|--------|-----------------------|
| الجاهزية للتصدي للاختراقات | معامل الارتباط $r$ | معامل التحديد $R^2$ | df | F المحسوبة | Sig. F | المتغير المستقل       | B     | T      | Sig. t                |
|                            | 0.741              | 0.549               | 1  | 265.427    | 0.000  | حوكمة الأمن السيبراني | 0.685 | 16.292 | 0.000                 |

يُظهر الجدول (12) أن معامل الارتباط بين حوكمة الأمن السيبراني والجاهزية للتصدي للاختراقات بلغ ( $r = 0.741$ ) ، وهو ما يعكس علاقة ارتباط موجبة قوية بين المتغيرين. كما بلغ معامل التحديد ( $R^2 = 0.549$ ) ، مما يشير إلى أن (54.9%) من التباين في الجاهزية للتصدي للاختراقات يمكن تفسيره من خلال متغير حوكمة الأمن السيبراني منفرداً. وبلغت قيمة F المحسوبة (265.427) بمستوى دلالة (0.000)، وهي دالة عند مستوى (0.01)، مما يعزّز دلالة النموذج ككل. أما معامل التأثير فبلغ ( $B = 0.685$ ) بقيمة  $T = 16.292$  وبمستوى دلالة (0.000)، مما يعني أن أي زيادة بمقدار وحدة واحدة في مستوى تطبيق حوكمة الأمن السيبراني تؤدي إلى زيادة بمقدار (0.685) في مستوى الجاهزية للتصدي للاختراقات. وبذلك تُقبل الفرضية الفرعية الأولى، ويُفسّر ذلك بأن الحوكمة توفّر

الإطار المؤسسي الحاكم لجميع الجهود السيبرانية، وتضمن التزام الإدارة العليا وتوفير الموارد، مما ينعكس مباشرة على مستوى الجاهزية.

#### الفرضية الفرعية الثانية:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لُبعد تعزيز الأمن السيبراني على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (13): تحليل الانحدار الخطي البسيط لقياس أثر تعزيز الأمن السيبراني على الجاهزية للتصدي للاختراقات

| المتغير<br>التابع                |                        | ملخص<br>النموذج        | تحليل التباينANOVA |               |           |                             |       | المعاملاتCoefficient |        |
|----------------------------------|------------------------|------------------------|--------------------|---------------|-----------|-----------------------------|-------|----------------------|--------|
| الجاهزية<br>للتصدي<br>للاختراقات | معامل<br>الارتباط<br>r | معامل<br>التحديد<br>R² | df                 | F<br>المحسوبة | Sig.<br>F | المتغير<br>المستقل          | B     | T                    | Sig. t |
|                                  | 0.762                  | 0.581                  | 1                  | 302.148       | 0.000     | تعزيز<br>الأمن<br>السيبراني | 0.712 | 17.383               | 0.000  |

يتضح من الجدول (13) أن معامل الارتباط بلغ ( $r = 0.762$ ) ، مما يعكس علاقة ارتباط قوية موجبة بين تعزيز الأمن السيبراني والجاهزية للتصدي للاختراقات. كما بلغ معامل التحديد ( $R^2 = 0.581$ ) ، أي أن (58.1%) من التباين في الجاهزية يُفسر بمستوى تطبيق ضوابط تعزيز الأمن السيبراني. وبلغت قيمة ( $F = 302.148$ ) بمستوى دلالة (0.000)، مما يُثبت المعنوية الإحصائية للنموذج. أما معامل التأثير فبلغ ( $B = 0.712$ ) وهو الأعلى بين الفرضيات الفرعية، مما يدلّ على أن أي تحسين بوحدة واحدة في تطبيق

ضوابط تعزيز الأمن السيبراني يُنتج زيادة بمقدار (0.712) في الجاهزية .وبذلك تُقبل الفرضية الفرعية الثانية .ويعزى هذا التأثير المرتفع إلى أن ضوابط التعزيز (كإدارة الهويات، وحماية الشبكات، والتشفير، واختبار الاختراق) هي الأدوات التقنية المباشرة التي تُترجم السياسات إلى ممارسات فعلية تحول دون وقوع الاختراقات وترفع مستوى الجاهزية بشكل ملموس.

### الفرضية الفرعية الثالثة:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لُبعد صمود الأمن السيبراني على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (14): تحليل الانحدار الخطي البسيط لقياس أثر صمود الأمن السيبراني على الجاهزية للتصدي للاختراقات

| المتغير التابع             | ملخص النموذج       | تحليل التباين ANOVA |    |            |        |                      |       | المعاملات Coefficient |        |
|----------------------------|--------------------|---------------------|----|------------|--------|----------------------|-------|-----------------------|--------|
| الجاهزية للتصدي للاختراقات | معامل الارتباط $r$ | معامل التحديد $R^2$ | df | F المحسوبة | Sig. F | المتغير المستقل      | B     | T                     | Sig. t |
|                            | 0.718              | 0.516               | 1  | 232.451    | 0.000  | صمود الأمن السيبراني | 0.647 | 15.246                | 0.000  |

يبين الجدول (14) أن معامل الارتباط بلغ ( $r = 0.718$ ) بعلاقة ارتباط موجبة قوية، ومعامل التحديد ( $R^2 = 0.516$ ) ، أي أن (51.6%) من التباين في الجاهزية يُفسر بمتغير صمود الأمن السيبراني. وبلغت قيمة ( $F (232.451)$  بمستوى دلالة (0.000)، مما يعزز

المعنوية الإحصائية للنموذج. وبلغ معامل التأثير ( $B = 0.647$ ) بقيمة  $T = 15.246$  ، أي أن أي زيادة بوحدة واحدة في مستوى الصمود تؤدي إلى زيادة ( $0.647$ ) في الجاهزية . وبذلك تُقبل الفرضية الفرعية الثالثة. ويُعزى ذلك إلى أن ضوابط الصمود (استمرارية الأعمال، التعافي من الكوارث، النسخ الاحتياطي، الاستجابة للحوادث) تُشكّل خط الدفاع الثاني بعد وقوع الحادث، مما يضمن استمرارية الخدمات ويُقلّل الأضرار، وهو جوهر مفهوم الجاهزية.

#### الفرضية الفرعية الرابعة:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لُبعد الأمن السيبراني للأطراف الخارجية والحوسبة السحابية على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (15): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني للأطراف الخارجية والحوسبة السحابية على الجاهزية للتصدي للاختراقات

| المتغير                    |         | ملخص           |               | تحليل التباين ANOVA |            |        |                                  | المعاملات Coefficient |        |
|----------------------------|---------|----------------|---------------|---------------------|------------|--------|----------------------------------|-----------------------|--------|
| التابع                     | المتغير | معامل الارتباط | معامل التحديد | df                  | F المحسوبة | Sig. F | المتغير المستقل                  | B                     | T      |
| الجاهزية للتصدي للاختراقات |         | 0.684          | 0.468         | 1                   | 191.836    | 0.000  | الأمن السيبراني للأطراف الخارجية | 0.583                 | 13.851 |
|                            |         |                |               |                     |            |        |                                  |                       | 0.000  |

|  |  |  |                   |  |  |  |  |  |  |
|--|--|--|-------------------|--|--|--|--|--|--|
|  |  |  | والحوسبة السحابية |  |  |  |  |  |  |
|--|--|--|-------------------|--|--|--|--|--|--|

يُشير الجدول (15) إلى وجود علاقة ارتباط موجبة قوية بين هذا البعد والجاهزية للتصدي للاختراقات، حيث بلغ معامل الارتباط ( $r = 0.684$ ) ومعامل التحديد ( $R^2 = 0.468$ )، أي أن (46.8%) من التباين في الجاهزية يُفسر بمتغير الأمن السيبراني للأطراف الخارجية والحوسبة السحابية. وبلغت قيمة  $F$  (191.836) بدلالة (0.000)، مما يُثبت معنوية النموذج. أما معامل التأثير فبلغ ( $B = 0.583$ ) بقيمة  $T = 13.851$  وبدلالة (0.000). وبذلك تُقبل الفرضية الفرعية الرابعة. ويُعزى هذا الأثر إلى أن الوزارات الحكومية باتت تعتمد بشكل متزايد على مزودي الخدمات ومنصات الحوسبة السحابية الوطنية، مما يجعل ضمان أمن هذه الأطراف عاملاً محورياً في تحصين البيئة السيبرانية للوزارة. ومع ذلك، جاء أثر هذا البعد أقل نسبياً من الأبعاد السابقة، ربما بسبب أن جزءاً من مسؤولية الأمن يقع على عاتق مزود الخدمة نفسه وفق مبدأ المسؤولية المشتركة، مما يُضعف الأثر المباشر للوزارة.

#### الفرضية الفرعية الخامسة:

نصّ الفرضية: "يوجد أثر ذو دلالة إحصائية عند مستوى الدلالة ( $\alpha \leq 0.05$ ) لبعد الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على الجاهزية للتصدي للاختراقات في الوزارات الحكومية بالمنطقة الشرقية".

جدول (16): تحليل الانحدار الخطي البسيط لقياس أثر الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية على الجاهزية للتصدي للاختراقات

| المتغير التابع | ملخص النموذج | تحليل التباين ANOVA | المعاملات Coefficient |
|----------------|--------------|---------------------|-----------------------|
|----------------|--------------|---------------------|-----------------------|

| معامل الارتباط<br>r | معامل التحديد<br>R <sup>2</sup> | df | F المحسوبة | Sig. F | المتغير المستقل                                                                 | B     | T      | Sig. t |
|---------------------|---------------------------------|----|------------|--------|---------------------------------------------------------------------------------|-------|--------|--------|
| 0.612               | 0.375                           | 1  | 130.842    | 0.000  | الأمن<br>السيبراني<br>ي<br>لأنظمة<br>التحكم<br>الصناعي<br>والتقنية<br>التشغيلية | 0.474 | 11.439 | 0.000  |

الجاهزية  
للتصدي  
للاختراقات

يُظهر الجدول (16) أن معامل الارتباط بلغ ( $r = 0.612$ ) ، وهو ما يعكس علاقة ارتباط موجبة متوسطة إلى قوية بين المتغيرين. كما بلغ معامل التحديد ( $R^2 = 0.375$ ) ، أي أن (37.5%) من التباين في الجاهزية يُفسّر بمتغير الأمن السيبراني للتقنية التشغيلية، وهي أقل نسبة تفسير بين الفرضيات الفرعية. وبلغت قيمة ( $F (130.842)$ ) بدلالة (0.000)، مما يُثبت المعنوية الإحصائية للنموذج. أما معامل التأثير فبلغ ( $B = 0.474$ ) بقيمة  $T = 11.439$  وبدلالة (0.000) وبذلك تُقبل الفرضية الفرعية الخامسة. ويُعزى انخفاض قوة هذا الأثر مقارنة بالأبعاد الأخرى إلى أن أنظمة OT ليست حاضرة في جميع الوزارات بالقدر ذاته، وإنما تتركز في الوزارات ذات الطابع الخدمي والصناعي كالمياه والكهرباء والنقل، مما يجعل أثرها المُعمّم على مستوى الجاهزية أقل من غيرها. كما أن ندرة الكوادر المتخصصة في أمن OT والتكلفة العالية لضوابطه المتخصصة تُشكّل قيوداً تُخفّف من الأثر الكلي.

الفصل الخامس: حدود  
البحث والتوصيات  
والنتائج

## 1.5 المقدمة

يُمثِّل هذا الفصل خاتمة الرحلة البحثية التي انطلق فيها الباحث لدراسة "أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات - دراسة ميدانية على وزارات المنطقة الشرقية"، إذ يستعرض الباحث في هذا الفصل الحدود التي أُطرت بها الدراسة، ثم يُقدِّم مجموعة من التوصيات المنبثقة من نتائج التحليل الإحصائي الذي أجري في الفصل الرابع، ويُقدِّم جملة من الدراسات المستقبلية التي تفتح آفاقاً بحثية جديدة في هذا المجال، ويختتم الفصل بخاتمة موجزة تُبرز أهم ما توصلت إليه الدراسة.

## 2.5 حدود الدراسة والدراسات المستقبلية

### حدود الدراسة

اقتصرت هذه الدراسة على مجموعة من الحدود التي ينبغي مراعاتها عند تعميم نتائجها أو الاستفادة منها، وتتمثل هذه الحدود في الآتي:

- الحدود الموضوعية: تناولت الدراسة موضوع أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك من خلال خمسة أبعاد محددة هي: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني للأطراف الخارجية والحوسبة السحابية، والأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية، دون التطرق إلى غيرها من الأطر أو المعايير الدولية كـ ISO/IEC 27001 أو NIST Cybersecurity Framework إلا في سياق المراجعة النظرية.
- الحدود المكانية: اقتصرت تطبيق الدراسة الميدانية على فروع الوزارات الحكومية الواقعة ضمن المنطقة الشرقية بالمملكة العربية السعودية، ولم تشمل بقية مناطق المملكة، مما يعني أن نتائجها قد تعكس خصوصيات هذه المنطقة دون سواها، على الرغم من وحدة الإطار التنظيمي الوطني.

- الحدود البشرية: تتمثل مجتمع الدراسة في العاملين في إدارات تقنية المعلومات والأمن السيبراني والحوكمة الرقمية داخل الوزارات المستهدفة، ممن يمتلكون خبرة مباشرة بتطبيق ضوابط NCA ، دون شمول موظفي الإدارات الأخرى أو المتعاملين مع الخدمات الرقمية الحكومية.
- الحدود الزمانية: أجريت الدراسة الميدانية خلال العام الدراسي 2025/2026م، وبالتالي فإن نتائجها تعكس الوضع الراهن لتطبيق معايير NCA خلال هذه الفترة، مع الأخذ في الاعتبار أن المشهد السيبراني في تطور مستمر وأن الهيئة الوطنية للأمن السيبراني تصدر بشكل دوري تحديثات على ضوابطها.
- الحدود المنهجية: اعتمدت الدراسة على المنهج الوصفي التحليلي والاستبانة كأداة رئيسية لجمع البيانات، مما قد يُقيد النتائج ضمن حدود ما تعكسه استجابات المشاركين من تصورات ذاتية، دون الاستناد إلى بيانات كمية موضوعية من داخل المنظومات التقنية للوزارات كسجلات الحوادث السيبرانية الفعلية أو تقارير المسح الأمني.

### الدراسات المستقبلية المقترحة

في ضوء نتائج الدراسة وحدودها، يقترح الباحث مجموعة من المحاور البحثية المستقبلية التي يمكن أن تُثري الأدب العلمي في مجال الأمن السيبراني الحكومي بالمملكة العربية السعودية.

يُوصى بإجراء دراسة مقارنة بين مستوى تطبيق معايير NCA في مختلف مناطق المملكة (الوسطى، الغربية، الشمالية، الجنوبية، الشرقية) لاستكشاف الفروقات الجغرافية والتنظيمية بينها، وتحديد أفضل الممارسات القابلة للنقل بين المناطق. كما يُقترح توسيع نطاق البحث ليشمل قطاعات حيوية أخرى كالقطاع الصحي والقطاع البنكي والقطاع التعليمي، خصوصاً أن هذه القطاعات تُعدّ من البنى التحتية الوطنية الحساسة التي تخضع بشكل مباشر لضوابط الهيئة.

ويرى الباحث أهمية إجراء دراسات تحليلية معمقة تدمج بين المنهج الكمي والنوعي (Mixed Methods) عبر مقابلات شخصية مع مسؤولي الأمن السيبراني (CISOs)

وتحليل تقارير الحوادث الفعلية، وذلك للحصول على صورة أكثر دقة تتجاوز حدود التصورات الذاتية. ويمكن كذلك إجراء دراسة طولية (Longitudinal Study) تتبّع مستوى الجاهزية السيبرانية عبر فترات زمنية متتالية لقياس أثر التحديثات المستمرة على ضوابط NCA.

كذلك يُوصى بإجراء دراسات متخصصة تتناول أبعاداً بعينها من ضوابط NCA بشكل أعمق، كدراسة أثر ضوابط الأمن السيبراني الحرجة (CSCC) على الجهات ذات البنى التحتية الحيوية، أو أثر ضوابط الأمن السيبراني للأنظمة الحساسة (CSCC-1) على القطاع الحكومي. وأخيراً، يُقترح إجراء دراسات تتناول العلاقة بين تطبيق معايير NCA ومتغيرات وسيطة أو معدّلة أخرى، كالثقافة التنظيمية، ونمط القيادة، وتبني التقنيات الناشئة (كالذكاء الاصطناعي وتقنية البلوك تشين) في تعزيز الجاهزية السيبرانية.

### 3.5 توصيات الدراسة

في ضوء ما أسفرت عنه الدراسة من نتائج، وبناءً على مستوى الأثر الذي أظهرته أبعاد تطبيق معايير NCA على جاهزية المؤسسات الحكومية للتصدي للاختراقات، يُقدّم الباحث جملة من التوصيات الموجهة للجهات المعنية.

على مستوى تعزيز حوكمة الأمن السيبراني: تُوصي الدراسة بضرورة أن تعمل الوزارات على تسريع دورات مراجعة سياسات الأمن السيبراني وتحديثها بشكل ربع سنوي على الأقل بدلاً من الاعتماد على المراجعات السنوية، وذلك لمواكبة سرعة التطور في المشهد السيبراني وتحديثات ضوابط NCA. كما يُوصى بتعزيز الدعم المقدم من الإدارات العليا عبر إشراك مسؤولي الأمن السيبراني (CISOs) بشكل مباشر في مجالس الإدارة واللجان الاستراتيجية، وتخصيص بند مستقل في الموازنة السنوية للأمن السيبراني بما لا يقل عن نسبة محددة من إجمالي ميزانية تقنية المعلومات.

على مستوى تعزيز الأمن السيبراني: يُوصى بإجراء اختبارات الاختراق (Penetration Testing) بشكل دوري ومنتظم لا يقل عن مرتين سنوياً، مع الاستعانة

بجهات متخصصة معتمدة من الهيئة الوطنية للأمن السيبراني. كما يُوصى بتبني نموذج "الثقة الصفرية (Zero Trust Architecture)" في تصميم شبكات الوزارات، وتفعيل حلول متقدمة لإدارة الهويات والوصول المميز (PAM) لضمان أعلى مستوى من التحكم في الصلاحيات الحساسة.

على مستوى صمود الأمن السيبراني: تُوصى الدراسة بإجراء تمارين محاكاة دورية (Cyber Drills) على الأقل مرتين سنوياً لاختبار خطط الاستجابة والتعافي من الحوادث، مع توثيق نتائجها والاستفادة منها في تحسين الخطط. كما يُوصى بتطبيق استراتيجية النسخ الاحتياطي (1-2-3) واختبار عمليات الاستعادة بشكل منتظم للتأكد من فعاليتها عند الحاجة، وليس الاكتفاء بمجرد تنفيذ النسخ الاحتياطي.

على مستوى الأمن السيبراني للأطراف الخارجية والحوسبة السحابية: يُوصى بتطوير آليات مراقبة مستمرة لمزودي الخدمات السحابية عبر تبني أدوات إدارة الوضع الأمني السحابي (CSPM) وأدوات وسيط أمن الوصول السحابي (CASB) كما يُوصى بتضمين اشتراطات صارمة في العقود مع الأطراف الخارجية تشمل حق التدقيق المفاجئ، والتبليغ الفوري عن أي حوادث، والالتزام بضوابط الحوسبة السحابية (CCC) الصادرة عن الهيئة.

على مستوى الأمن السيبراني للتقنية التشغيلية: تُوصى الدراسة بإنشاء وحدات متخصصة في أمن أنظمة التقنية التشغيلية (OT Security) داخل الوزارات ذات الطابع الخدمي، وتأهيل كوادر بشرية مدربة على التعامل مع بيانات OT من خلال شهادات متخصصة كـ (GICSP) و (ISA/IEC 62443) كما يُوصى بتطبيق الفصل الشبكي الآمن بين شبكات IT و (OT Network Segmentation) واستخدام تقنيات الدايود الأمني (Data Diodes) عند تبادل البيانات بين البيئتين.

على المستوى الوطني العام: يُقترح أن تعمل الهيئة الوطنية للأمن السيبراني على إنشاء منصة موحدة لتبادل معلومات التهديدات السيبرانية (Threat Intelligence Sharing Platform) بين الوزارات الحكومية بشكل آني، بما يُعزّز الاستفادة الجماعية من الخبرات ويسرّع الاستجابة للتهديدات المشتركة. كما يُوصى بتوسيع برامج التأهيل الوطنية للكوادر

السيبرانية بالتعاون مع الجامعات، خصوصاً في التخصصات النادرة كأمن OT وأمن الحوسبة السحابية وتحليل التهديدات المتقدمة (APT).

على مستوى الوعي والتدريب يُوصى بتكثيف برامج التوعية السيبرانية لجميع موظفي الوزارات دون استثناء، وليس الاقتصار على الفئات التقنية، مع تنفيذ حملات دورية لمحاكاة هجمات التصيد الاحتيالي (Phishing Simulations) وقياس مدى استجابة الموظفين لها بهدف رفع مستوى الوعي والتحصين البشري.

## 4.5 الخاتمة

يمثل الأمن السيبراني في العصر الرقمي ركيزة أساسية من ركائز الأمن الوطني الشامل، ولا سيما في ظل التوسع المتسارع في التحول الرقمي الذي تشهده المملكة العربية السعودية ضمن مستهدفات رؤية 2030. وقد جاءت هذه الدراسة لتسلط الضوء على جانب حيوي يتمثل في مدى إسهام تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) في تعزيز جاهزية المؤسسات الحكومية للتصدي للاختراقات، وذلك من خلال دراسة ميدانية أجريت على وزارات المنطقة الشرقية.

وقد كشفت نتائج التحليل الإحصائي عن وجود أثر إيجابي دالّ إحصائياً لأبعاد معايير NCA الخمسة على مستوى الجاهزية السيبرانية للوزارات الحكومية، إذ فسّرت هذه الأبعاد مجتمعةً ما نسبته (78.0%) من التباين في مستوى الجاهزية للتصدي للاختراقات، وهو ما يعكس القوة التفسيرية العالية للنموذج البحثي ويثبت الأهمية المحورية لتطبيق هذه المعايير. كما تبين أن بُعد حوكمة الأمن السيبراني جاء في مقدّمة الأبعاد الأكثر تأثيراً، مما يؤكد أن الحوكمة تُشكّل الإطار المؤسسي الذي تنبثق منه بقية الجهود التقنية، فيما جاء بُعد الأمن السيبراني للتقنية التشغيلية في المرتبة الأخيرة نظراً لخصوصية تواجد هذه الأنظمة في وزارات بعينها.

كذلك أظهرت النتائج أن المستوى العام لتطبيق معايير NCA في الوزارات الحكومية بالمنطقة الشرقية جاء بدرجة "موافق" وبمتوسط عام (3.996)، وهو مؤشر إيجابي على

النضج المتنامي للمنظومة السيبرانية الحكومية، مع وجود مساحات للتحسين والتطوير، خصوصاً في جوانب اختبارات التعافي من الكوارث ومراقبة مزودي الخدمات السحابية وتدريب العاملين على أنظمة OT.

ويأمل الباحث أن تُشكّل هذه الدراسة إضافة علمية متواضعة للأدب البحثي في مجال الأمن السيبراني الحكومي بالمملكة العربية السعودية، وأن تكون مرجعاً يستفيد منه صانعو القرار في الوزارات والجهات الحكومية، وباحثون آخرون يتطلعون إلى استكمال هذا المسار البحثي. كما يُثمن الباحث كل ما بذلته الهيئة الوطنية للأمن السيبراني من جهود متميزة في وضع منظومة متكاملة من الضوابط والمعايير التي رفعت من مستوى النضج السيبراني الوطني، ويُشيد بتعاون الوزارات وموظفيها في إنجاح هذه الدراسة.

وفي الختام، يُوجّه الباحث خالص الشكر والتقدير إلى كل من أسهم في إتمام هذه الدراسة، من المشرفين والمحكمين والمشاركين في الاستبانة، سائلاً الله عزّ وجلّ أن تكون هذه الدراسة نافعة وأن يُسدّد خطى الجميع نحو تعزيز الأمن السيبراني الوطني، بما يُحقّق أمن الوطن ومنعته الرقمية، ويسهم في تحقيق مستهدفات رؤية المملكة العربية السعودية 2030.

## Abstract

This study aimed to measure the impact of implementing the National Cybersecurity Authority (NCA) standards, across its five dimensions (Cybersecurity Governance, Cybersecurity Defense, Cybersecurity Resilience, Third-Party and Cloud Computing Cybersecurity, and Industrial Control Systems and Operational Technology Cybersecurity), on the readiness of governmental institutions to counter cyber breaches in the ministries of the Eastern Region of the Kingdom of Saudi Arabia. The study adopted the descriptive-analytical approach, employing a questionnaire as the main tool, distributed to a stratified random sample of (220) employees working in IT and cybersecurity departments. Data were analyzed using SPSS software. The results revealed a statistically significant positive impact at the ( $\alpha \leq 0.05$ ) level of NCA standards on cybersecurity readiness, with the five dimensions collectively explaining (78.0%) of the variance in the dependent variable. Cybersecurity Governance emerged as the most influential dimension, followed by Cybersecurity Defense, Cybersecurity Resilience, Third-Party and Cloud Computing Cybersecurity, and lastly Operational Technology Cybersecurity. The study recommended accelerating policy review cycles, adopting the Zero Trust Architecture, conducting periodic cyber simulation drills, enhancing monitoring of cloud service providers, developing specialized cadres in OT security, and establishing a unified national platform for cyber threat intelligence sharing among governmental entities.

**Keywords:** Cybersecurity, National Cybersecurity Authority (NCA), Cyber Readiness, Cyber Breaches, Governmental Institutions, Eastern Region, Kingdom of Saudi Arabia.

## قائمة المراجع

### 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 للإغاثة وتشغيل اللاجئين الفلسطينيين في الشرق الأدنى - إقليم الأردن (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1608363>
- الهاجري، راشد محمد علي الفهيد، و البشابشة، سامر عبدالمجيد هزيم. (2021). أثر الذكاء الاستراتيجي على استراتيجيات إدارة الأزمات من خلال استراتيجية الأمن السيبراني بالتطبيق على الأجهزة الحكومية في دولة قطر (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة. مسترجع من <http://search.mandumah.com/Record/1277187>
- الفلاح، حسام محمد سليمان، النصور، مروان محمد عبد، و العربيات، أيمن عبدالهادي. (2023). أثر تطبيق معايير الأمن السيبراني على أداء شركات الاتصالات الأردنية (رسالة ماجستير غير منشورة). جامعة البلقاء التطبيقية، السلط. مسترجع من <http://search.mandumah.com/Record/1460405>
- الحسيني، سرور حافظ، و الدعمي، وليد عباس جبر. (2025). أثر الأمن السيبراني في الحد من القصور الذاتي للمصارف. مجلة الغري للعلوم الاقتصادية والإدارية، مج21، ع2، 415 - 447. مسترجع من <http://search.mandumah.com/Record/1604136>
- صمادي، نور الهدى أحمد يوسف، و العليمات، نوفان حامد محمد. (2020). أثر اقتصاد المعرفة على جودة التدقيق الإلكتروني في ظل تطبيق سياسة الأمن السيبراني: دراسة ميدانية على مكاتب التدقيق الأردنية (رسالة ماجستير غير منشورة). جامعة آل

البيت، المفرق، مسترجع من

<http://search.mandumah.com/Record/1140998>

- السرحان، حنين عبدالمهدي سالم، و المشاقبة، محمد ناصر موسى حمدان. (2020).

أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق. مسترجع من

<http://search.mandumah.com/Record/1094365>

- نوار، سلمى عصام محمد. (2025). أثر تطبيق متطلبات الأمن السيبراني على

الحكومة الرقمية ب مديرية الشباب والرياضة بمحافظة الإسكندرية. المجلة العلمية للبحوث والدراسات في التربية الرياضية، ع49، 154 - 208. مسترجع من

<http://search.mandumah.com/Record/1591679>

- الحلافي، حسن خضر، العباس، المعتصم خليل، و المطيري، منى بنت جزاء. (2026).

أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض خلال العام 2025. مجلة العلوم الاقتصادية والإدارية والقانونية، مج10، ع2

، 1 - 10. مسترجع من

<http://search.mandumah.com/Record/1666230>

## المراجع الأجنبية

- Almaiah, M. A., Alfaisal, R., Salloum, S. A., Hajje, F., Shishakly, R., Lutfi, A., ... & Al-Marouf, R. S. (2022). Measuring institutions' adoption of artificial intelligence applications in online learning environments: integrating the innovation diffusion theory with technology adoption rate. *Electronics*, 11(20), 3291b
- Gambo, M. L., Danasabe, A., Binbeshr, F., Imam, M., Shinwari, M. W., & Mahmoud, A. (2026). Navigating the cyber landscape: Saudi Arabia's cybersecurity standards and implementation barriers. *Arabian Journal for Science and Engineering*, 51(5), 5589-5607.
- Gorenšek, T., & Trivunčević, R. (2025). Cybersecurity Readiness in the Euro-Mediterranean: A Comparative Review of Literature on

National Strategies and Global Indices. *Journal of Criminal Justice and Security*, 1-32.

- Kulin, J., & Johansson Sevä, I. (2021). Who do you trust? How trust in partial and impartial government institutions influences climate policy attitudes. *Climate Policy*, 21(1), 33-46.
- Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan. *Social Science Review Archives*, 4(1), 1806-1829
- Majeed, Y., Majeed, A., & Minhas, M. T. (2026). Cybersecurity Governance in the Digital Era and IT: Integrating Regulatory Oversight, Risk Management, and Organisational Resilience in Pakistan. *Social Science Review Archives*, 4(1), 1806-1829.
- Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2026). Assessing the impact of cybersecurity readiness on organizational security performance: a study on Malaysian organizations. *Journal of Enterprise Information Management*, 39(3), 907-927.
- Mohamed Noor, A. F., Moghavvemi, S., & Tajudeen, F. P. (2026). Assessing the impact of cybersecurity readiness on organizational security performance: a study on Malaysian organizations. *Journal of Enterprise Information Management*, 39(3), 907-927.
- Murad, H. A., & Qudah, M. (2025). The attitudes of communicators toward cybersecurity concerning security, safety in national institutions. *Frontiers in Communication*, 10, 1552520.
- Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. *International Journal of Acta Informatica*, 2(1), 209-218
- Rawindaran, N., Nawaf, L., Alarifi, S., Alghazzawi, D., Carroll, F., Katib, I., & Hewage, C. (2023). Enhancing cyber security governance and policy for SMEs in industry 5.0: a comparative study between Saudi Arabia and the United Kingdom. *Digital*, 3(3), 200-231.
- Yusuf, F. (2021). The independent campus program for higher education in Indonesia: The role of government support and the readiness of institutions, lecturers, and students. *Journal of Social Studies Education Research*, 12(2), 280-304

- Zubaidah, E., Monalisa, M., Rusadi, S., & Handoko, T. (2024). E-Readiness Analysis to Accelerate Transformation Towards E-Government in Regional Government in Indonesia. *Jurnal Bina Praja*, 16(1), 37-53.

## ملحق (1): الاستبانة

السلام عليكم ورحمة الله وبركاته،،

يقوم الباحث بإجراء دراسة علمية بعنوان "أثر تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA) على جاهزية المؤسسات الحكومية للتصدي للاختراقات - دراسة ميدانية على وزارات المنطقة الشرقية"، وذلك استكمالاً لمتطلبات الحصول على الدرجة العلمية.

ونظراً لما تتمتعون به من خبرة ودراية في مجال تقنية المعلومات والأمن السيبراني، يتشرف الباحث بأن يضع بين أيديكم هذه الاستبانة، راجياً التكرم بقراءة فقراتها بدقة، والإجابة عنها بموضوعية، باختيار الإجابة التي تُعبّر عن وجهة نظركم. وتفضلوا بقبول تأكيد الباحث بأن جميع المعلومات الواردة ستُعامل بسرية تامة، ولن تُستخدم إلا لأغراض البحث العلمي فقط.

شاكراً لكم حسن تعاونكم،، الباحث

## القسم الأول: البيانات الديموغرافية

1. الجنس: ( ) ذكر ( ) أنثى
2. العمر: ( ) أقل من 30 ( ) 30 – أقل من 40 ( ) 40 – أقل من 50 ( ) 50 فأكثر
3. المؤهل العلمي: ( ) دبلوم ( ) بكالوريوس ( ) ماجستير ( ) دكتوراه
4. سنوات الخبرة في مجال تقنية المعلومات / الأمن السيبراني: ( ) أقل من 5 ( ) 5 – أقل من 10 ( ) 10 – أقل من 15 ( ) 15 فأكثر
5. المسمى الوظيفي: ( ) مدير إدارة ( ) رئيس قسم ( ) أخصائي/محلل ( ) أخرى
6. هل حصلت على شهادات مهنية في الأمن السيبراني (CISSP, CISA, ISO 27001) ( ) نعم ( ) لا

## القسم الثاني: فقرات الاستبانة

أولاً: تطبيق معايير الهيئة الوطنية للأمن السيبراني (NCA)

البُعد الأول: حوكمة الأمن السيبراني

| م | الفقرة                                                                                   | موافق<br>بشدة | موافق<br>فق | محايد | غير<br>موافق | غير<br>موافق<br>بشدة |
|---|------------------------------------------------------------------------------------------|---------------|-------------|-------|--------------|----------------------|
| 1 | تمتلك وزارتي استراتيجيات معتمدة للأمن السيبراني متوافقة مع متطلبات NCA.                  |               |             |       |              |                      |
| 2 | تُحدّد الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بوضوح داخل الهيكل التنظيمي للوزارة. |               |             |       |              |                      |
| 3 | تُراجع سياسات الأمن السيبراني وتُحدّث بشكل دوري وفق المستجدات التنظيمية.                 |               |             |       |              |                      |
| 4 | توفّر الإدارة العليا الدعم المالي والإداري اللازم لتطبيق ضوابط الأمن السيبراني.          |               |             |       |              |                      |

البُعد الثاني: تعزيز الأمن السيبراني

| م | الفقرة | موافق<br>بشدة | موافق<br>فق | محايد | غير<br>موافق | غير<br>موافق<br>بشدة |
|---|--------|---------------|-------------|-------|--------------|----------------------|
|---|--------|---------------|-------------|-------|--------------|----------------------|

|  |  |  |  |  |                                                                               |   |
|--|--|--|--|--|-------------------------------------------------------------------------------|---|
|  |  |  |  |  | تُطبَّق في وزارتي إجراءات صارمة لإدارة الهويات والصلاحيات للوصول إلى الأنظمة. | 5 |
|  |  |  |  |  | تُستخدم أنظمة متقدمة لحماية الشبكات وكشف التهديدات السيبرانية.                | 6 |
|  |  |  |  |  | تُجرى عمليات دورية لإدارة الثغرات الأمنية واختبار الاختراق في وزارتي.         | 7 |
|  |  |  |  |  | تُطبَّق ضوابط حماية البيانات والتشفير على الأصول المعلوماتية الحساسة.         | 8 |

### البُعد الثالث: صمود الأمن السيبراني

| م  | الفقرة                                                                 | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |
|----|------------------------------------------------------------------------|------------|-------|-------|-----------|----------------|
| 9  | تمتلك وزارتي خطة معتمدة لاستمرارية الأعمال تشمل جوانب الأمن السيبراني. |            |       |       |           |                |
| 10 | تُجرى اختبارات دورية لخطط التعافي من الكوارث السيبرانية.               |            |       |       |           |                |
| 11 | تُحدَّث إجراءات النسخ الاحتياطي للبيانات الحيوية بشكل منتظم.           |            |       |       |           |                |

|  |  |  |  |  |    |                                                                     |
|--|--|--|--|--|----|---------------------------------------------------------------------|
|  |  |  |  |  | 12 | تتوفر لدى وزارتي قدرات فعّالة للاستجابة السريعة للحوادث السيبرانية. |
|--|--|--|--|--|----|---------------------------------------------------------------------|

#### البُعد الرابع: الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية

| م  | الفقرة                                                                  | موافق بشدة | موافق | محايد | غير موافق بشدة |
|----|-------------------------------------------------------------------------|------------|-------|-------|----------------|
| 13 | تتضمّن العقود مع مزوّدي الخدمات اشتراطات واضحة للأمن السيبراني.         |            |       |       |                |
| 14 | تُقيّم المخاطر السيبرانية المتعلقة بالأطراف الخارجية بصورة منتظمة.      |            |       |       |                |
| 15 | تُطبّق ضوابط NCA الخاصة بأمن الحوسبة السحابية على الخدمات المستضافة.    |            |       |       |                |
| 16 | تُراقب أنشطة مزوّدي الخدمات السحابية للتحقق من التزامهم بمتطلبات الأمن. |            |       |       |                |

#### البُعد الخامس: الأمن السيبراني لأنظمة التحكم الصناعي والتقنية التشغيلية

| م | الفقرة | موافق بشدة | موافق | محايد | غير موافق بشدة |
|---|--------|------------|-------|-------|----------------|
|---|--------|------------|-------|-------|----------------|

|  |  |  |  |  |    |                                                                           |
|--|--|--|--|--|----|---------------------------------------------------------------------------|
|  |  |  |  |  | 17 | تُطبَّق في وزارتي ضوابط<br>متخصصة لحماية أنظمة التقنية<br>التشغيلية. (OT) |
|  |  |  |  |  | 18 | تُفصل شبكات التقنية التشغيلية<br>عن شبكات تقنية المعلومات بشكل<br>آمن.    |
|  |  |  |  |  | 19 | تُجرى عمليات رصد مستمرة<br>للأنشطة غير المعتادة في أنظمة<br>التحكم.       |
|  |  |  |  |  | 20 | يُدرَّب العاملون على الأنظمة<br>التشغيلية على متطلبات الأمن<br>السيبراني. |

## ثانياً: الجاهزية للتصدي للاختراقات

| م | الفقرة                                                                      | موافق<br>بشدة | موافق | محايد | غير<br>موافق | غير<br>موافق<br>بشدة |
|---|-----------------------------------------------------------------------------|---------------|-------|-------|--------------|----------------------|
| 1 | تمتلك وزارتي قدرات وقائية فعّالة<br>تحول دون وقوع الاختراقات<br>السيبرانية. |               |       |       |              |                      |
| 2 | تتوفر أدوات متقدمة لاكتشاف<br>الهجمات السيبرانية في مراحلها<br>الأولى.      |               |       |       |              |                      |
| 3 | يستجيب فريق الأمن السيبراني<br>لدينا للحوادث في زمن قياسي.                  |               |       |       |              |                      |

| م  | الفقرة                                                                         | موافق<br>بشدة | موا<br>فق | محايد | غير<br>موافق | غير<br>موافق<br>بشدة |
|----|--------------------------------------------------------------------------------|---------------|-----------|-------|--------------|----------------------|
| 4  | تمتلك وزارتي خطة واضحة ومُختبرة للتعافي من الحوادث السيبرانية.                 |               |           |       |              |                      |
| 5  | يتمتع الكادر التقني بالكفاءة اللازمة للتعامل مع التهديدات السيبرانية المتقدمة. |               |           |       |              |                      |
| 6  | تُجرى تمارين محاكاة دورية لاختبار جاهزية الوزارة للهجمات السيبرانية.           |               |           |       |              |                      |
| 7  | توثق الحوادث السيبرانية ويُستفاد من دروسها في تحسين الجاهزية.                  |               |           |       |              |                      |
| 8  | تُتاح آليات واضحة للتواصل والتنسيق مع الجهات الوطنية عند وقوع الحوادث.         |               |           |       |              |                      |
| 9  | يملك العاملون وعياً سيبرانياً يُمكنهم من التعرف على محاولات الاختراق.          |               |           |       |              |                      |
| 10 | تتوفر تقنيات حديثة لرصد التهديدات المتطورة (APT) داخل البيئة التقنية.          |               |           |       |              |                      |

| م  | الفقرة                                                                 | موافق<br>بشدة | موا<br>فق | محايد | غير<br>موافق | غير<br>موافق<br>بشدة |
|----|------------------------------------------------------------------------|---------------|-----------|-------|--------------|----------------------|
| 11 | تُراجَع مؤشرات الأداء الخاصة<br>بِالجاهزية السيبرانية بصورة<br>دورية.  |               |           |       |              |                      |
| 12 | تستطيع وزارتي استئناف خدماتها<br>الرقمية بسرعة بعد أي حادث<br>سيبراني. |               |           |       |              |                      |

شاكرين لكم حسن تعاونكم