

Final Project 2

PMG 497

نموذج المشروع النهائي 2

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

أسم الطالب

معاذ التركي

233000082

المشروع النهائي- 2

كلية الإدارة- جامعة ميدأوشن

إشراف

د. عبدالرحيم نادر

عضو هيئة التدريس- كلية الإدارة- جامعة ميدأوشن

التاريخ- الفصل الدراسي

الشكر والتقدير

الإهداء

مستخلص الدراسة

الهدف:

المنهجية:

النتائج:

التطبيقات والأهمية:

الكلمات المفتاحية:

جدول المحتويات

2	الشكر والتقدير.....
3	الإهداء.....
4	مستخلص الدراسة.....
7	1. الفصل الأول: الإطار العام للدراسة.....
8	1.1. المقدمة:.....
9	1.2. مشكلة الدراسة.....
9	1.2.1. فجوات على المستوى النظري.....
9	1.2.2. فجوات على المستوى التطبيقي.....
9	1.3. أهمية الدراسة.....
9	1.3.1. على المستوى النظري:.....
9	1.3.2. على المستوى التطبيقي:.....
10	1.4. أسئلة الدراسة.....
10	1.5. أهداف الدراسة.....
10	1.6. فرضيات الدراسة.....
10	1.7. نموذج الدراسة.....
11	1.8. الدراسة الميدانية.....
11	1.9. مخطط المشروع.....
12	2. الفصل الثاني: الدراسات السابقة.....
13	2.1. المقدمة:.....
13	2.2. المتغير المستقل.....
13	2.3. المتغير التابع.....
14	2.4. العلاقة بين المتغير المستقل والمتغير التابع.....
14	2.5. الخاتمة.....
15	3. الفصل الثالث: منهجية الدراسة.....

16	3.1. المقدمة
16	3.2. التعريفات الإجرائية لمتغيرات البحث
17	3.3. تصميم البحث
17	3.4. مجتمع البحث وطرق وتقنيات أخذ العينات
18	3.5. طريقة جمع البيانات
18	3.6. أنواع البيانات
18	3.7. إجراءات التحليل الإحصائي
19	3.8. الخاتمة
20	4. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج
21	4.1. المقدمة
21	4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)
21	4.3. اختبارات الصدق والثبات للاستبيانات
22	4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)
22	4.5. اختبار الفرضيات ومناقشة النتائج
22	4.6. الخاتمة
23	5. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات
24	5.1. حدود الدراسة والدراسات المستقبلية
24	5.2. توصيات الدراسة
24	5.3. الخاتمة
25	قائمة المراجع
26	الملاحق

جدول الأشكال

جدول الجداول

1. الفصل الأول: الإطار العام للدراسة

1.1. المقدمة:

تشمل المقدمة الخمس مراحل لكتابة المقدمة

تكتب المقدمة في صورة فقرات فقط

1.2. مشكلة الدراسة

يتم كتابة مقدمة بسيطة في شكل فقرة
يتم تقسيم المشكلة الى فجوات نظرية وعملية

1.2.1. فجوات على المستوى النظري

1.2.2. فجوات على المستوى التطبيقي

ينتهي هذا الجزء بالسؤال الرئيسي

1.3. أهمية الدراسة

1.3.1. على المستوى النظري:

1.3.2. على المستوى التطبيقي:

1.4. أسئلة الدراسة

1.5. أهداف الدراسة

1.6. فرضيات الدراسة

1.7. نموذج الدراسة

1.8. الدراسة الميدانية

1.9. مخطط المشروع

2. الفصل الثاني: الدراسات السابقة

2.1. المقدمة:

2.2. المتغير المستقل

2.3. المتغير التابع

2.4. العلاقة بين المتغير المستقل والمتغير التابع

2.5. الخاتمة

3. الفصل الثالث: منهجية الدراسة

3.1. المقدمة

تُعدّ منهجية الدراسة الإطار العلمي المنظم 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 بالبوصلية 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.

3.2. 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 يُدركها العاملون في إدارات تقنية المعلومات والأمن السيبراني، ويُقاس من خلال خمسة أبعاد فرعية على النحو الآتي:

البُعد الأول - حوكمة الأمن السيبراني: ويُقصد به إجرائياً مدى توافر السياسات والاستراتيجيات والأدوار والمسؤوليات المعتمدة لإدارة الأمن السيبراني داخل الوزارة، ويُقاس بأربع فقرات.

البُعد الثاني - تعزيز الأمن السيبراني: ويُقصد به إجرائياً مدى تطبيق الضوابط التقنية لحماية الأصول المعلوماتية مثل إدارة الهويات والوصول، وحماية الأنظمة والشبكات، وإدارة الثغرات، ويُقاس بأربع فقرات.

البُعد الثالث – صمود الأمن السيبراني: ويُقصد 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: ويُقصد 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: ويُقصد به إجراءات مدى تطبيق الضوابط المتعلقة بأنظمة التشغيل والتحكم في البيانات 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

3.4. 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 والمحليلين 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 يُقدّر 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.

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.

3.5. طريقة جمع البيانات

اعتمد الباحث في جمع البيانات الأولية على أداة الاستبانة الإلكترونية بوصفها الأداة الأنسب لطبيعة الدراسة الكمية ولظروف عيّنتها المنتشرة جغرافياً، وقد صُمّمت 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 عُرضت على مجموعة من المحكمين المتخصصين للتحقق من صدق المحتوى، وأُجريت دراسة استطلاعية على عيّنة من (30) موظفاً للتحقق من ثبات الأداة باستخدام معامل ألفا كرونباخ.

ويوضّح الجدول الآتي أدوات البحث المستخدمة لجمع البيانات:

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

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

3.6. أنواع البيانات

اعتمدت الدراسة على نوعين من البيانات:

البيانات الأولية: وهي البيانات الميدانية التي جمعها الباحث مباشرة من أفراد العينة عبر الاستبانة الإلكترونية، وتُمثل 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 استُخدمت في بناء الإطار النظري وصياغة فقرات أداة الدراسة وتفسير نتائجها.

3.7. 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 وبُعده.
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 خلوّ النموذج من الازدواج الخطي.

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 بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تمتلك وزارتي استراتيجية 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 بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5	تُطبّق في وزارتي إجراءات صارمة لإدارة الهويات والصلاحيات للوصول إلى الأنظمة.					
6	تُستخدم أنظمة متقدمة لحماية الشبكات وكشف التهديدات السيبرانية.					

					7 تُجرى عمليات دورية لإدارة الثغرات الأمنية واختبار الاختراق في وزارتي.
					8 تُطبّق ضوابط حماية البيانات والتشفير على الأصول المعلوماتية الحساسة.

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	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 بشدة	محايد	غير موافق	غير موافق بشدة
17	تُطبّق في وزارتي ضوابط متخصصة لحماية أنظمة التقنية التشغيلية. (OT)					
18	تُفصل شبكات التقنية التشغيلية عن شبكات تقنية المعلومات بشكل آمن.					
19	تُجرى عمليات رصد مستمرة للأنشطة غير المعتادة في أنظمة التحكم.					
20	يُدرّب العاملون على الأنظمة التشغيلية على متطلبات الأمن السيبراني.					

ثانياً: الجاهزية للتصدي للاختراقات

م	الفقرة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تمتلك وزارتي قدرات وقائية فعّالة تحول دون وقوع الاختراقات السيبرانية.					
2	تتوفر أدوات متقدمة لاكتشاف الهجمات السيبرانية في مراحلها الأولى.					
3	يستجيب فريق الأمن السيبراني لدينا للحوادث في زمن قياسي.					
4	تمتلك وزارتي خطة واضحة ومُختبّرة 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	تُوثّق 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.
					11	تُراجَع مؤشرات الأداء الخاصة بالجاهزية السيبرانية بصورة دورية.
					12	تستطيع وزارتي استئناف خدماتها الرقمية بسرعة بعد أي حادث سيبراني.

شاكرين لكم حسن تعاونكم

3.2. الخاتمة

4. الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

4.1. المقدمة

4.2. توصيف عينة الدراسة (الإحصائيات الوصفية لعينة البحث)

4.3. اختبارات الصدق والثبات للاستبيانات

4.4. الإحصاء الوصفي لمتغيرات البحث (الإجابة على أسئلة البحث)

4.5. اختبار الفرضيات ومناقشة النتائج

4.6. الخاتمة

5. الفصل الخامس: حدود البحث والتوصيات والاستنتاجات

5.1. حدود الدراسة والدراسات المستقبلية:

5.2. توصيات الدراسة:

5.3. الخاتمة:

قائمة المراجع

الملاحق