

أثرتبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية
السعودية

إعداد الطالب/

ياسر حسن الصفدي

الرقم الجامعي/

243000055

إشراف/

د. أحمد راجح

العام الدراسي

2025



إهداء

إلى من رحل عن الدنيا قبل أن يشهد هذه اللحظة...

إلى روح والدي الحبيب رحمه الله، الذي علّمني أن العلم زاد، وأن العمل عبادة، وأن الكلمة أمانة...

غاب حضوره عن عيني، لكن أثره في قلبي وعقلي باقٍ ما حييت.

اللهم اجعل هذا العمل صدقةً جاريةً له، وأنر قبره بضياء لا ينطفئ.

إلى أُمي الغالية، التي كانت دعواتها سرّ قوتي، ودموعها زادي في الطريق...

إلى إخوتي وأبنائي، الذين أحاطوني بحبهم، ومنحوني ما يعجز عنه الشكر والامتنان...

إلى كل من أضاء لي شمعة في درب العلم، أو مدّ يده لي في لحظة احتجت فيها للسند...

أهديكم ثمرة عمري، وقطاف سنوات من السعي والصبر، وفاءً وحبًا وعرفانًا.

شكر وتقدير

الحمد لله الذي بنعمته تتم الصالحات، وبفضله وكرمه أنجزت هذا العمل المتواضع.

أتقدم بخالص الشكر وعظيم الامتنان إلى أستاذي ومشرفي الأكاديمي د. أحمد راجح على دعمه وتوجيهاته القيّمة، وصبره الكبير خلال جميع مراحل إعداد هذه الرسالة، فقد كان نعم الموجه والنصح.

كما أشكر جميع أعضاء هيئة التدريس في الجامعة على ما قدّموه من علم ومعرفة، وزملائي الباحثين على تعاونهم وروحهم الطيبة.

إلى روح والدي الحبيب رحمه الله، الذي غرس في نفسي حب العلم والعمل الجاد، فكان حافزاً لي في مسيرتي العلمية، وأدعو الله أن يجعل هذا العمل صدقةً جارية له.

كما أخص بالشكر والدتي العزيزة على دعمها الدائم ودعواتها الصادقة، وإخوتي وأبنائي على مساندتهم وتشجيعهم المستمر.

وأخيراً، شكري موصول لكل من قدّم لي يد العون، أو كلمة مشجعة، أو نصيحة مخلصة، جعلت من هذا الإنجاز ممكناً.

فهرس المحتويات

3	إهداء.....
4	شكر وتقدير
6	قائمة الجداول
7	فهرس الأشكال.....
9	المستخلص.....
10	الفصل الأول.....
11	المقدمة.....
13	مشكلة الدراسة
14	تساؤلات الدراسة.....
14	أهمية الدراسة
15	أهداف الدراسة.....
16	فرضيات الدراسة
17	النظرية العلمية المتبعة لإعداد البحث
20	الفصل الثاني.....
20	الدراسات السابقة.....
21	المقدمة.....
23	المتغير التابع والمستقل
25	الدراسات السابقة.....
32	الإطار النظري للدراسة
35	الفصل الثالث.....
35	منهجية الدراسة
36	المقدمة.....
37	المنهجية وطرق البحث
38	أدوات الدراسة
40	مجتمع البحث

41	خطوات جمع البيانات
43	حدود البحث
44	الفصل الرابع
44	نتائج الدراسة
45	المقدمة
47	تحليل البيانات
79	المناقشة
79	الخاتمة
82	التوصيات
83	المراجع
87	الملاحق
89	Abstract

قائمة الجداول

48	جدول 1: الوصف الإحصائي للبيانات
49	جدول 2: الوصف الإحصائي لجنس المشاركين بالتجربة
50	جدول 3: الوصف الإحصائي لعمر المشاركين بالتجربة
51	جدول 4: الوصف الإحصائي للدرجة العلمية للمشاركين بالتجربة
52	جدول 5: الوصف الإحصائي لدى المشروع استراتيجية واضحة للأمن السيبراني
53	جدول 6: الوثق الإحصائي ليتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري
54	جدول 7: الوصف الإحصائي ليتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني
56	جدول 8: الوصف الإحصائي ليتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية
57	جدول 9: الوصف الإحصائي لتبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا
58	جدول 10: الوصف الإحصائي لساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء
60	جدول 11: الوصف الإحصائي لساعدت الإجراءات الأمنية في تعزيز ثقة العملاء
61	جدول 12: الوصف الإحصائي لتبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية
62	جدول 13: الوصف الإحصائي لتطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع
64	جدول 14: الوصف الإحصائي للاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق
65	جدول 15: الوصف الإحصائي لتكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع

66	جدول 16: الوصف الإحصائي لنقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.....
68	جدول 17: الوصف الإحصائي لصعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.....
69	جدول 18: الوصف الإحصائي لتعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً.....
70	جدول 19: الوصف الإحصائي لهنالك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.....
71	جدول 20: ملخص تحليل البيانات.....
71	جدول 21: تحليل المصادقية والموثوقية للبيانات.....
	جدول 22: اختبار كاي اسكوير لدور تدريب الموظفين في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....
73	جدول 23: اختبار كاي اسكوير لدور البرمجيات المتقدمة في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....
74	جدول 24: اختبار كاي اسكوير لدور الكفاءات المتخصصة في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....
76	جدول 25: تحليل التباين الأحادي لمتغيرات الدراسة.....
78	جدول 26: ملخص نموذج عامل بايز ^{أ، ب}

فهرس الأشكال

32	رسم توضيحي 1: الإطار النظري للدراسة.....
49	رسم توضيحي 2: التمثيل البياني لجنس المشاركين بالتجربة.....
50	رسم توضيحي 3: التمثيل البياني لعمر المشاركين بالتجربة.....
51	رسم توضيحي 4: التمثيل البياني للدرجة العلمية للمشاركين بالتجربة.....
53	رسم توضيحي 5: التمثيل البياني لدى المشروع استراتيجية واضحة للأمن السيبراني.....
54	رسم توضيحي 6: التمثيل البياني ليتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري.....
55	رسم توضيحي 7: التمثيل للبياني ليتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني.....
56	رسم توضيحي 8: التمثيل البياني ليتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية.....
57	رسم توضيحي 9: التمثيل البياني لتبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا.....
59	رسم توضيحي 10: التمثيل البياني لساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء.....
60	رسم توضيحي 11: التمثيل البياني لمساعدت الإجراءات الأمنية في تعزيز ثقة العملاء.....
61	رسم توضيحي 12: التمثيل البياني لتبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية.....
63	رسم توضيحي 13: التمثيل البياني لتطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع.....
64	رسم توضيحي 14: التمثيل البياني للاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق.....
65	رسم توضيحي 15: التمثيل البياني لتكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع.....

- رسم توضيحي 16: التمثيل البياني لنقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.....67
- رسم توضيحي 17: التمثيل البياني لصعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.....68
- رسم توضيحي 18: التمثيل البياني لتعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً.....69
- رسم توضيحي 19: التمثيل البياني لهنالك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.....70
- رسم توضيحي 20: متغيرات الدراسة التابعة والمستقلة.....72
- رسم توضيحي 21: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور تدريب الموظفين في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....73
- رسم توضيحي 22: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور البرمجيات المتقدمة في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....75
- رسم توضيحي 23: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور الكفاءات المتخصصة في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.....77

المستخلص

تهدف هذه الدراسة إلى استكشاف أثر تبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية السعودية، وذلك من خلال تحليل العلاقة بين ممارسات الأمن السيبراني ومستوى استمرارية هذه المشاريع في بيئة تنافسية متطورة. اتبعت الدراسة المنهجية الوصفية التحليلية، حيث تم جمع البيانات من خلال استبيانات موجهة إلى عينة مكونة من 155 مشاركاً من العاملين في المشاريع التقنية الناشئة. أظهرت النتائج أن تبني استراتيجيات أمنية واضحة ومدعومة من الإدارة العليا، بالإضافة إلى تحديث السياسات الأمنية وتدريب الموظفين واستخدام البرمجيات المتقدمة، يسهم بشكل كبير في حماية البيانات وتعزيز ثقة العملاء وتحسين سمعة المشاريع. كما أبرزت الدراسة تحديات مثل تكلفة تطبيق الأمن السيبراني ونقص الكفاءات المتخصصة، مما يستدعي تبني حلول داعمة تشمل التدريب والتمويل المناسب. ومن أهم التوصيات تعزيز دور الإدارة العليا في دعم الأمن السيبراني، وتطوير برامج تدريبية مستمرة، وتبسيط الإجراءات الأمنية لضمان مرونة العمل، بالإضافة إلى تشجيع التعاون بين الجهات الحكومية والقطاع الخاص.

الكلمات المفتاحية: الأمن السيبراني، المشاريع التقنية الناشئة، استدامة المشاريع، التدريب الأمني، البرمجيات

المتقدمة، الكفاءات المتخصصة، المملكة العربية السعودية.

الفصل الأول

المقدمة

في ظل الثورة الرقمية العالمية المتسارعة، أصبحت مبادرات التكنولوجيا الجديدة عناصر أساسية في إرساء اقتصاد المعرفة وتشجيع الابتكار، لا سيما في الدول التي تسعى إلى الريادة التقنية، مثل المملكة العربية السعودية. ويتمشى هذا التوجه مع رؤية المملكة 2030، التي تهدف إلى تنويع مصادر الدخل وتشجيع الاستثمار في التكنولوجيا وريادة الأعمال. ومع تزايد الاعتماد على الأنظمة الرقمية، برزت مخاطر الأمن السيبراني كواحدة من أبرز الصعوبات التي تواجه تطوير المبادرات، لا سيما في مراحلها الأولى، التي تتسم بالحساسية ونقص البنية التحتية الأمنية.

لم يعد اعتماد أساليب قوية للأمن السيبراني خياراً؛ بل أصبح ضرورة لضمان استمرارية هذه المبادرات واستمراريتها على المدى الطويل في عالم رقمي يتميز بالتغيرات السريعة والمخاطر العديدة. يمكن أن تتسبب الهجمات الإلكترونية وتسريب البيانات والاختراقات في انقطاع العمليات وفقدان الثقة، بل وحتى فشل المشروع في مراحله الأولى. ونتيجة لذلك، يُعد تحقيق التوازن بين الابتكار التقني والحماية الأمنية أمراً بالغ الأهمية لتطوير مبادرات تكنولوجيا قادرة على التوسع والمنافسة. وبناءً على ذلك، تُعد هذه الدراسة بالغة الأهمية، إذ ستبحث في تأثير تطبيق أساليب الأمن السيبراني على استدامة مبادرات تطوير التكنولوجيا في المملكة. وتركز على فهم العقبات التي تواجهها هذه المبادرات، ومدى إدراك رواد الأعمال لضرورة الأمن السيبراني، والتقنيات المستخدمة لتطبيقه بفعالية. ويهدف البحث من خلال ذلك إلى تقديم نصائح عملية تُساعد هذه المبادرات على أن تصبح أكثر مرونة وتزدهر في بيئة رقمية آمنة ومستدامة.

يُحدث التبني العالمي للتقنيات الجديدة تحولاتٍ في الاقتصادات والثقافات والصناعات بوتيرة غير مسبوقة، مُبشِّراً بعصرٍ ثوريٍّ تحوّل فيه الابتكار من ميزة تنافسيةٍ إلى ضرورةٍ ملحةٍ. تُغيّر تقنيات الذكاء الاصطناعي، والروبوتات، وإنترنت الأشياء، والبلوك تشين (blockchain) طريقة عمل الشركات وتعاونها لإنتاج القيمة. هذه الثورة عالمية النطاق، وتؤثر على كلّ من الدول المتقدمة والنامية. يستثمر كلّ من القطاعين العام والتجاري استثماراتٍ كبيرةً في الحلول الرقمية لزيادة الكفاءة، ودفع عجلة التنمية الاقتصادية، ومعالجة التحديات المجتمعية الصعبة.

في السنوات الأخيرة، ساد اعتقادٌ متزايدٌ بأن تطوير التقنيات قد يجعل الخدمات أكثر مرونةً وسلاسةً وقابليةً للتوسع عبر مجموعةٍ واسعةٍ من الصناعات، بما في ذلك الرعاية الصحية والتعليم والتمويل والتصنيع. وقد أتاحَت هذه التقنيات فرصاً جديدةً لجمع البيانات وتحليلها وأتمتة المهام وتطوير تجارب مُصمّمة خصيصاً. وفي نهاية المطاف، يؤدي هذا إلى زيادة الإنتاجية وتحسين عملية اتخاذ القرارات. تُدرك الدول في جميع أنحاء العالم الأهمية الاستراتيجية لتبني هذه

التقنيات، التي تُوفّر مزايا اقتصاديةً مع معالجة مخاوف رئيسيةٍ مثل تغيّر المناخ، والوصول إلى الرعاية الصحية، واستدامة البنية التحتية. ومع ذلك، فإن طريق تبني التقنيات الناشئة محفوف بالعقبات، لا سيما فيما يتعلق بحماية البيانات، والأمن السيبراني، وتشريد العمال، والفجوة الرقمية، وتعقيدات التنفيذ. لذا، فإن اتباع استراتيجية متوازنة تُعطي الأولوية للابتكار أمرٌ بالغ الأهمية للحكومات التي تسعى إلى تحقيق كامل إمكانات التقنيات الجديدة (dga, 2025).

نفذت المملكة العربية السعودية مجموعة متنوعة من المبادرات كجزء من استراتيجيتها للذكاء الاصطناعي، بما في ذلك:

- تميز المواهب، هدف جهود تميز المواهب إلى تطوير كفاءة المملكة المستقبلية في مجال الذكاء الاصطناعي. وتهدف إلى جعل المملكة مركزاً عالمياً للتدريب والتعليم في مجال الذكاء الاصطناعي من خلال التعاون مع الأكاديميين والجمهور وقطاع الأعمال.

- المؤسسات الرائدة في مجال الذكاء الاصطناعي، يشرف المركز الوطني للذكاء الاصطناعي (NCAI) على المهام والمبادرات المتعلقة بالذكاء الاصطناعي في العديد من القطاعات. كما يشرف على مبادرات تطبيق تقنيات الذكاء الاصطناعي، ويقدم الدعم لمنظومة الصناعة، ويضمن تحقيق الأهداف الوطنية.

- البحث والتطوير، يُجري المركز الوطني للذكاء الاصطناعي (NCAI) أبحاثاً أساسية وتطبيقية في مجال الذكاء الاصطناعي، مما يجعله المركز الوطني للابتكار في هذا المجال. ويشجع المركز على ترجمة نتائج الأبحاث إلى تطبيقات وحلول عملية، مما يعزز الاقتصاد القائم على المعرفة.

- مراكز الابتكار، يعزز مركز الابتكار التابع للمركز الوطني للذكاء الاصطناعي الابتكار وريادة الأعمال من خلال تسهيل إنشاء تطبيقات وحلول الذكاء الاصطناعي. يتعاون المركز مع الشركات الناشئة وحاضنات الأعمال لسد الفجوة بين التعليم والتوظيف، مما يتيح للشركات الجديدة المساهمة في التنمية الاقتصادية للمملكة.

- المبادرات، تسعى مبادرة "واحة الذكاء الاصطناعي" إلى تعزيز المعرفة العامة بالذكاء الاصطناعي من خلال عروض تفاعلية وفعاليات تعليمية. تدمج هذه المبادرة التكنولوجيا مع تاريخ وثقافة المملكة العربية السعودية الغنيين، مما يخلق تجربة تفاعلية تشجع الشباب على البحث عن وظائف في مجال البيانات والذكاء الاصطناعي.

- القمة العالمية، تُعد القمة العالمية للذكاء الاصطناعي، التي تنظمها الهيئة السعودية للبيانات والذكاء الاصطناعي، منصة رئيسية للحوار الدولي حول الذكاء الاصطناعي. عُقد الحدث الافتتاحي رقمياً يومي 21 و22

أكتوبر 2020، وجمع سياسيين وباحثين ومستثمرين ورواد أعمال وخبراء تكنولوجيا لتحديد مستقبل الذكاء الاصطناعي (my, 2025).

مشكلة الدراسة

مع التقدم المستمر في التكنولوجيا الرقمية، أصبحت مبادرات التكنولوجيا الجديدة في المملكة العربية السعودية ركيزة أساسية في النظام الاقتصادي الحديث، معتمدةً بشكل أساسي على الحلول الرقمية والبيانات المصاحبة لها. ومع ذلك، ونظرًا لاعتمادها المتزايد على البيئة الرقمية، أصبحت هذه المبادرات أكثر عرضة للهجمات السيبرانية، مما قد يؤثر بشكل مباشر على استمراريتهما واستمراريتها. على الرغم من مساعي الحكومة لتحسين الأمن السيبراني على المستوى الوطني، لا تزال العديد من المبادرات النامية تفتقر إلى سياسات أمنية محددة، أو لا تُعطي الأمن السيبراني الأولوية في خططها التشغيلية، إما بسبب نقص المعرفة أو الموارد. وهذا يجعلها أكثر عرضة لتهديدات مثل القرصنة، واختراق البيانات، والأعطال التكنولوجية.

ومن هنا، تتجلى مشكلة الدراسة في السؤال التالي:

- إلى أي مدى يُساهم تطبيق أساليب الأمن السيبراني في تحسين استدامة مبادرات التكنولوجيا النامية في المملكة العربية السعودية؟

تنبع هذه المشكلة من عدد من الأسئلة الفرعية، منها:

- ما مدى وعي رواد الأعمال العاملين في مبادرات التكنولوجيا الجديدة بمخاطر الأمن السيبراني؟
- ما هي استراتيجيات الأمن الأكثر استخدامًا في هذه المشاريع؟
- هل هناك علاقة بين نشر تقنيات الأمن السيبراني واستدامة المشاريع أو نموها؟ ما هي عقبات تطبيق هذه الاستراتيجيات في بيئة الشركات الناشئة؟

تساؤلات الدراسة

التساؤل الرئيسي:

- ما تأثير أساليب الأمن السيبراني على استمرارية الشركات التقنية الناشئة في المملكة العربية السعودية على المدى الطويل؟

التساؤلات الفرعية:

- إلى أي مدى يدرك رواد الأعمال في الشركات التقنية الناشئة مخاطر الأمن السيبراني؟
- ما هي أكثر أساليب الأمن السيبراني شيوعاً التي تستخدمها الشركات التقنية الناشئة؟
- ما العلاقة بين تطبيق سياسات الأمن السيبراني وتحقيق أهداف الاستدامة، مثل استمرارية الشركة ونموها؟
- ما هي العقبات التي يواجهها رواد الأعمال في مجال التكنولوجيا في المملكة في وضع استراتيجيات فعالة للأمن السيبراني؟
- كيف يمكن تطبيق أساليب الأمن السيبراني بشكل أفضل لمساعدة شركات التكنولوجيا على الازدهار؟

أهمية الدراسة

تكتسب هذه الدراسة أهميتها من كونها تجمع بين اتجاهين حاليين مهمين: الأمن السيبراني والمبادرات التكنولوجية الناشئة. وكلاهما ركيزتان أساسيتان في التحول الرقمي للمملكة العربية السعودية واستدامة أعمالها على المدى الطويل. ونظراً للتوجه الوطني لرؤية السعودية 2030 نحو اقتصاد قائم على المعرفة والابتكار، ثمة حاجة ملحة لفهم دور الأمن السيبراني كعامل تمكين لاستمرار هذه المبادرات وتوسيع نطاقها.

أولاً: الأهمية العلمية

- زيادة الفهم النظري للعلاقة بين أساليب الأمن السيبراني وجدوى المشاريع الناشئة، لا سيما في ظل العالم الرقمي الحالي.

- تتناول الدراسة نقصًا في البحث العلمي في الأدبيات العلمية العربية من خلال دراسة العلاقة بين الأمن السيبراني واستدامة المشاريع الجديدة، والتي كانت محدودة.
- تؤسس هذه الورقة البحثية أساسًا علميًا للبحوث المستقبلية في مجال التقاء التكنولوجيا وريادة الأعمال وإدارة المخاطر.

ثانيًا: الأهمية العملية

- يُثَقِّفُ البحث رواد الأعمال ومديري مشاريع التكنولوجيا الجديدة حول ضرورة دمج أساليب الأمن السيبراني في عملياتهم اليومية وتخطيطهم الاستراتيجي.
- ويُقدِّم مؤشرات وإجراءات فعّالة لاعتماد وتنفيذ سياسات أمن سيبراني فعّالة للحفاظ على الاستمرارية وتقليل المخاطر.
- ويُثَقِّفُ الجهات الحكومية وجهات دعم الشركات الناشئة حول ضرورة تقديم المشورة والمساعدة في مجال الأمن السيبراني، مما يضمن استمرارية القطاع على المدى الطويل.
- ويُساعد البحث على تعزيز الفهم المؤسسي والاجتماعي لضرورة الأمن السيبراني كعنصر أساسي في نجاح المشاريع الريادية، وليس مجرد عاملٍ تقنيٍّ ثانوي.

أهداف الدراسة

الهدف الرئيسي للدراسة:

- تقييم أثر تبني استراتيجيات الأمن السيبراني على استمرارية مشاريع التكنولوجيا الناشئة على المدى الطويل في المملكة العربية السعودية، ومدى مساهمة هذه الاستراتيجيات في الحد من المخاطر، وضمان استمراريتهما، وتعزيز الثقة الرقمية في منظومة ريادة الأعمال.

الأهداف الفرعية للدراسة:

- تحديد مستوى معرفة رواد الأعمال في مبادرات التكنولوجيا الجديدة بأهمية الأمن السيبراني ومخاطره.
- رصد مختلف تقنيات الأمن السيبراني المستخدمة في مبادرات التكنولوجيا الناشئة، ومدى شموليتها وفعاليتها.

- دراسة العلاقة بين تطبيق أساليب الأمن السيبراني ومقاييس استدامة المشاريع، مثل النمو، والاحتفاظ بالعملاء، واستمرارية العمليات.
- دراسة أبرز القضايا الملحة التي تواجه مشاريع التكنولوجيا الجديدة في وضع تدابير فعالة للأمن السيبراني.
- تقديم توصيات واقعية لتحسين كفاءة وفعالية الأمن السيبراني في منظومة ريادة الأعمال التكنولوجية، مما يزيد من فرص نجاح المشاريع واستمراريتها على المدى الطويل.

فرضيات الدراسة

الفرضية الرئيسية:

- يوجد أثر ذو دلالة إحصائية لتبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية السعودية.

الفرضيات الفرعية:

- يرتبط فهم رواد الأعمال لمخاوف الأمن السيبراني ارتباطاً إيجابياً بطول عمر شركات التكنولوجيا.
- سياسات الأمن السيبراني الشاملة والناجحة لها تأثير إيجابي على استمرارية شركات التكنولوجيا على المدى الطويل.
- يمكن أن يساعد تطبيق أساليب الأمن السيبراني الشركات على التخفيف من التحديات التكنولوجية وتحقيق نجاح طويل الأمد.
- تُصعّب تحديات البنية التحتية والمالية والخبرة التقنية اعتماد حلول فعالة للأمن السيبراني.
- يُحسن توافر الدعم المؤسسي والإشراف الحكومي من نجاح أساليب الأمن السيبراني بين شركات التكنولوجيا.

1. النظرية المؤسسية (Institutional Theory)

تُعد النظرية المؤسسية إحدى الركائز النظرية التي استند إليها هذا البحث في تفسير سلوك المشاريع التقنية الناشئة في المملكة العربية السعودية عند تبنيها لاستراتيجيات الأمن السيبراني. تنطلق هذه النظرية من فكرة أن المنظمات لا تتخذ قراراتها فقط بناءً على الكفاءة الاقتصادية، بل أيضًا استجابةً للضغوط المؤسسية التي تفرضها البيئة المحيطة، مثل القوانين، التشريعات، متطلبات السوق، وتوقعات العملاء. في البيئة السعودية، نجد أن الجهات التنظيمية مثل الهيئة الوطنية للأمن السيبراني تفرض معايير واضحة لضمان أمان الأنظمة والمعلومات، مما يشكل ضغطًا خارجيًا على المشاريع التقنية الناشئة لاعتماد ممارسات أمنية متقدمة. لذا، يُمكن تفسير تبني هذه المشاريع لاستراتيجيات الأمن السيبراني كوسيلة لاكتساب الشرعية المؤسسية وضمان البقاء ضمن بيئة تنظيمية متطورة (Alshammari, 2020).

2. نظرية الموارد والقدرات (Resource-Based View - RBV)

ترتكز هذه النظرية على فكرة أن استدامة المشروع وتحقيقه لميزة تنافسية يرتبطان بامتلاكه لموارد داخلية فريدة ونادرة يصعب تقليدها. في سياق الأمن السيبراني، تعتبر المعرفة الأمنية، الكفاءات التقنية، والقدرة على تطوير سياسات أمان فعالة من ضمن هذه الموارد الاستراتيجية. ووفقًا لهذه النظرية، فإن المشروع الذي يستثمر في بناء قدرات أمنية قوية يصبح أكثر قدرة على حماية بياناته، التفاعل مع التهديدات الأمنية، وكسب ثقة العملاء والمستثمرين. وبالتالي، فإن تبني استراتيجيات الأمن السيبراني ليس مجرد استجابة خارجية، بل هو أيضًا استثمار داخلي في موارد تؤثر بشكل مباشر على استدامة المشروع. هذا المنظور يُظهر أن الأمن السيبراني ليس فقط عبئًا تشغيليًا، بل عنصرًا تنافسيًا جوهريًا (Cao, 2019).

3. إطار النضج الأمني السيبراني (Cybersecurity Maturity Model - CMM)

لتحليل مدى تطور الممارسات الأمنية داخل المشاريع التقنية الناشئة، اعتمدت الدراسة على إطار النضج الأمني السيبراني. يُصنف هذا الإطار المنظمات إلى خمس مستويات من النضج تبدأ من المرحلة التمهيديّة (Ad-hoc) التي تتسم بالعشوائية في الإجراءات الأمنية، وتصل إلى المرحلة المثالية (Optimized) حيث تكون الاستراتيجيات الأمنية متكاملة ومبنية على التحسين المستمر. يساعد هذا النموذج في تقييم واقع الأمن السيبراني داخل المشاريع وتحديد مدى تأثير هذا

النضج على استدامتها. فالمشاريع التي وصلت إلى مستويات نضج متقدمة تُظهر قدرة أعلى على الصمود أمام الهجمات السيبرانية، واستمرارية العمل حتى في الظروف الطارئة، مما ينعكس إيجابًا على قدرتها على البقاء والنمو (Marican، 2022).

4. المنهج الكمي في التحليل العلمي

اتبعت الدراسة المنهج الكمي كمنهجية علمية رئيسية لقياس وتحليل العلاقة بين تبني استراتيجيات الأمن السيبراني واستدامة المشاريع التقنية الناشئة. تم تصميم استبانة كمية لجمع البيانات من عينة من أصحاب المشاريع ومديريها في السعودية، واحتوت على محاور تقيس درجة تطبيق الأمن السيبراني ومستوى استدامة المشروع. سمح هذا المنهج للباحث باستخدام أدوات إحصائية مثل تحليل الانحدار، التكرارات، واختبارات الارتباط، للتحقق من الفرضيات. وبهذا الأسلوب، يمكن للدراسة تقديم نتائج دقيقة وقابلة للتعميم ضمن المجتمع البحثي، كما يساعد المنهج الكمي في تقديم أدلة كمية على العلاقة بين المتغيرات قيد الدراسة (Renaud، 2021).

5. النموذج المفاهيمي للدراسة

تم تطوير نموذج مفاهيمي يعكس العلاقة بين متغيرات الدراسة بطريقة منهجية، حيث يمثل تبني استراتيجيات الأمن السيبراني المتغير المستقل، بينما تمثل الاستدامة المتغير التابع. كما تضمنت الدراسة متغيرات وسيطة مثل: حجم المشروع، ونوع النشاط التقني، وعدد سنوات التشغيل. يهدف هذا النموذج إلى تنظيم العلاقة بين المتغيرات في إطار واضح يُمكن من اختبار الفرضيات بدقة. ويساعد النموذج المفاهيمي أيضًا في تصور آلية التأثير، حيث يفترض أن المشاريع التي تطبق استراتيجيات أمنية متقدمة تمتلك فرصًا أكبر للاستدامة على المستويين التشغيلي والتنافسي. النموذج ليس فقط أداة للشرح، بل هو دليل إرشادي للباحث في مراحل جمع وتحليل البيانات (Khalufi، 2025).

6. تكامل الأطر النظرية والمنهجية

إن اختيار هذه النظريات والمنهجيات لم يكن اعتباطيًا، بل تم وفق منهج علمي يراعي طبيعة الموضوع ومتغيراته المعقدة. فالنظرية المؤسسية توضح الدوافع الخارجية لتبني الأمن السيبراني، في حين تشرح نظرية الموارد والقدرات الدوافع الداخلية التي تستند إلى رؤية استراتيجية. أما نموذج النضج الأمني، فيوفر أداة عملية لتقييم مستوى التطبيق، بينما يسمح المنهج الكمي بتحليل العلاقة بين هذه العناصر بطريقة قابلة للقياس. يتيح هذا التكامل بين الأطر النظرية

والمنهجية الوصول إلى نتائج دقيقة وشاملة، ويعزز من القيمة العلمية والتطبيقية للبحث في بيئة الاقتصاد الرقمي
السعودي (Stevens، 2020).

الفصل الثاني

الدراسات السابقة

المقدمة

يُعد هذا الفصل من الدراسة بمثابة الإطار المرجعي الذي يُرسّخ الأساس النظري والفكري للبحث، ويُمهّد لفهم أعمق ودقيق للعلاقة بين مفاهيم الدراسة الرئيسية. ففي سياق أكاديمي يستند إلى المنهج العلمي، لا يمكن تناول أي موضوع بحثي بمعزل عن سياقه المعرفي وموقعه داخل المنظومة النظرية ذات الصلة، إذ إن تحليل الظواهر المعاصرة—مثل تبني استراتيجيات الأمن السيبراني واستدامة المشاريع التقنية—يتطلب العودة إلى الأصول العلمية والنماذج المفاهيمية التي عالجت هذه القضايا من قبل، سواء في البيئات المحلية أو الدولية.

في ظل التحولات المتسارعة التي تشهدها المملكة العربية السعودية في مجال التحول الرقمي وريادة الأعمال التقنية، تبرز أهمية الربط بين الأمن السيبراني واستدامة المشاريع الناشئة، لا سيما مع ارتفاع وتيرة التهديدات الأمنية وتزايد اعتماد هذه المشاريع على البنية الرقمية. من هنا، يُسهم هذا الفصل في وضع هذه الدراسة ضمن سياقها الصحيح، من خلال تقديم خلفية علمية موسّعة تمكّن من تفسير طبيعة العلاقة بين عناصرها، وتُساعد في تفسير السلوك التنظيمي للمشاريع التقنية عند مواجهة التحديات الرقمية الحديثة.

كما يُتيح هذا الفصل للباحث استعراض التوجهات الفكرية والنظرية التي تم البناء عليها لفهم الظاهرة المدروسة، واستكشاف المفاهيم التي تمثل المحاور الأساسي للبحث. هذا التأسيس النظري لا يُعد مجرد عنصر تكميلي في الدراسة، بل يُشكل أحد الأعمدة الرئيسية التي تستند إليها عملية تحليل النتائج لاحقاً، ويضمن اتساق المسار المنهجي للبحث، من تحديد المشكلة، إلى بناء الفرضيات، ثم تفسير البيانات وتحليلها.

ومن خلال هذا الفصل، يتم كذلك تسليط الضوء على الجهود العلمية السابقة ذات الصلة، بما يُتيح للباحث تقييم ما تم إنجازه فعلاً في هذا المجال، وتحديد الفجوات المعرفية التي لم تُعالج بعد، وهو ما يُعزز من القيمة العلمية للدراسة، ويُبرر الحاجة إليها في السياق السعودي بشكل خاص. ففهم كيفية تعامل دراسات سابقة مع موضوعات مشابهة يُسهم في بلورة رؤية نقدية تجاه الأدبيات، ويُساعد على توجيه الجهد البحثي نحو جوانب أكثر دقة وتأثيراً.

يوفر هذا الفصل أُسساً متينة يمكن من خلالها تأطير العلاقة بين المفاهيم المطروحة ضمن إطار نظري مترابط، يُمكن من تحويل الفكرة العامة للدراسة إلى نموذج بحثي يمكن اختباره ميدانياً. وبذلك، يُمثل هذا الجزء خطوة حاسمة في ربط الجانب النظري بالجانب التطبيقي للبحث، وهو ما يُعزز من مصداقية النتائج ويساهم في بناء توصيات قابلة للتطبيق العملي في بيئة ريادة الأعمال التقنية في المملكة.

إن القيمة العلمية لهذا الفصل تكمن في قدرته على رسم ملامح الاتجاه البحثي، وتحديد مرتكزاته النظرية، وتوضيح المسارات التي سيتبعها الباحث في تحليل الظاهرة المدروسة. وبدون هذا التأسيس المنهجي، لن تكتسب النتائج المتوقعة من البحث معناها الكامل، ولن يكون من الممكن تقديم توصيات قائمة على تحليل علمي راسخ. ومن هنا، تتضح الأهمية البالغة لهذا الفصل ضمن البنية الكلية للدراسة، باعتباره الجسر الذي يربط بين النظرية والتطبيق، وبين الملاحظة العلمية والتفسير الأكاديمي المنهجي.

المتغير التابع والمستقل

- أولاً: المتغير التابع – استراتيجيات الأمن السيبراني

تُعد استراتيجيات الأمن السيبراني المتغير الرئيسي الذي تسعى هذه الدراسة إلى قياس أثره على استدامة المشاريع التقنية الناشئة. ويُقصد باستراتيجيات الأمن السيبراني تلك السياسات، والإجراءات، والأنظمة التي تعتمد عليها المشاريع التقنية بهدف حماية أصولها الرقمية، وضمان أمن المعلومات، والتصدي للتهديدات السيبرانية المتزايدة. تشمل هذه الاستراتيجيات عدّة أبعاد مترابطة، منها الجوانب التقنية كالتشفير، وأنظمة الكشف عن الاختراقات، وإدارة الهوية والوصول، وكذلك الجوانب الإدارية مثل سياسات التحكم، خطط الطوارئ، وتدريب الموظفين.

في بيئة سريعة التطور مثل بيئة ريادة الأعمال التقنية في المملكة العربية السعودية، أصبح امتلاك استراتيجية أمن سيبراني فعالة شرطاً أساسياً لاستمرار أي مشروع في السوق. حيث تُسهم هذه الاستراتيجيات في تعزيز ثقة العملاء والمستثمرين، والامتثال للأنظمة الوطنية مثل متطلبات الهيئة الوطنية للأمن السيبراني، إضافةً إلى تقليل الخسائر الناتجة عن الانتهاكات الأمنية. وبذلك، فإن الأمن السيبراني لم يعد مجرد عنصر داعم، بل أصبح جزءاً أصيلاً في الهيكل الاستراتيجي للمشاريع الناشئة الطامحة إلى الاستدامة والتوسع (Chagadama، 2022).

- ثانياً: المتغيرات المستقلة المؤثرة في استراتيجيات الأمن السيبراني

1. تدريب الموظفين

يمثل تدريب الموظفين أحد العوامل الجوهرية في تعزيز فعالية استراتيجيات الأمن السيبراني داخل المشاريع التقنية. فالموارد البشرية تُعد من نقاط القوة وأيضاً نقاط الضعف في أي منظومة أمنية، حيث أظهرت الدراسات أن النسبة الكبرى من الخروقات الأمنية تنجم عن أخطاء بشرية أو ضعف في الوعي السيبراني. ولذلك، فإن الاستثمار في تأهيل الموظفين وتوعيتهم بممارسات الأمن الرقمي السليم يُعزّز من قدرة المؤسسة على حماية نفسها من التهديدات.

يشمل هذا التدريب موضوعات متعددة مثل إدارة كلمات المرور، التعرف على رسائل الاحتيال الإلكتروني (Phishing)، كيفية التعامل مع البيانات الحساسة، بالإضافة إلى البروتوكولات التي يجب اتباعها عند حدوث خرق أمني. وبهذا المعنى،

يُعد التدريب المستمر بمثابة خط الدفاع الأول ضد المخاطر السيبرانية، ومؤشرًا على نضج الثقافة الأمنية داخل المشروع (Reeves، 2021).

2. البرمجيات المتقدمة

تشكل البنية التحتية التقنية المدعومة بالبرمجيات المتقدمة ركيزة أساسية في تطبيق استراتيجية أمن سيبراني فعالة. وتُشير البرمجيات المتقدمة هنا إلى الأدوات الرقمية الحديثة المستخدمة في رصد التهديدات، وتحليل الأنماط غير الطبيعية في النظام، والتعامل مع محاولات الاختراق أو تسريب المعلومات. تشمل هذه الأدوات برامج الجدران النارية (Firewalls)، أنظمة كشف التسلل (IDS/IPS)، أدوات التشفير، وتقنيات الذكاء الاصطناعي في تحليل البيانات.

تعتمد فعالية هذه الأدوات على مدى تكاملها مع أنظمة العمل اليومية للمشروع، وقدرتها على العمل الاستباقي في مواجهة المخاطر. فكلما زادت كفاءة البرمجيات المستخدمة وتطورها، زادت قدرة المشروع على الاستجابة الفورية للهجمات السيبرانية وتقليل أثارها، ما يُعزز من استمرارية العمليات التشغيلية ويُقلل من احتمالات التعرض لانقطاع الخدمة أو فقدان البيانات (Hlatshwayo، 2023).

3. الكفاءات المتخصصة

إلى جانب البنية التقنية والتدريب، تبرز الكفاءات المتخصصة كعنصر حيوي في تصميم وتنفيذ استراتيجيات أمن سيبراني متقدمة. وتشمل الكفاءات المتخصصة الأفراد أو الفرق التقنية المؤهلة أكاديميًا وعمليًا في مجالات أمن المعلومات، اختبار الاختراق، إدارة الحوادث السيبرانية، وتحليل الثغرات الأمنية. وجود هذه الكفاءات داخل المشروع أو ضمن شبكة دعم خارجية يُعد مؤشرًا على مدى احترافية استراتيجية الأمن المتبعة.

في سياق المشاريع التقنية الناشئة، غالبًا ما يُمثل نقص الكفاءات تحديًا واضحًا، نتيجة لمحدودية الموارد أو ضعف الوصول إلى الكفاءات المؤهلة. لذلك، يُعد توظيف أو التعاون مع مختصين ذوي خبرة خطوة استراتيجية أساسية لضمان وجود استجابة فعالة ومهنية عند مواجهة تهديدات محتملة، كما يُساهم في بناء سياسة وقائية مستمرة تتناسب مع تطور طبيعة المخاطر (Ismail، 2024).

- ثالثاً: العلاقة بين المتغيرات

تقوم العلاقة بين المتغيرات المستقلة (تدريب الموظفين، البرمجيات المتقدمة، الكفاءات المتخصصة) والمتغير التابع (استراتيجيات الأمن السيبراني) على افتراض سببي رئيسي، مفاده أن تبني مكونات فعالة في المحاور الثلاثة يُسهم بشكل مباشر في بناء استراتيجية أمنية أكثر تكاملاً وفعالية. حيث أن كل بُعد من الأبعاد الثلاثة يُمثل عنصراً أساسياً من عناصر استراتيجية الأمن السيبراني الشاملة، ويُسهم في تقوية جوانبها المختلفة.

فعلى سبيل المثال، حتى في ظل توفر أدوات برمجية متقدمة، فإن غياب الوعي الأمني لدى الموظفين قد يُعرض المشروع لتهديدات ناتجة عن استخدام خاطئ أو تجاهل للإجراءات الأمنية. وبالمثل، فإن وجود كفاءات متخصصة دون دعم من أدوات تقنية قوية قد يُقيد قدرتهم على التدخل أو التنبؤ بالمخاطر. ومن هنا، يمكن القول إن العلاقة بين المتغيرات علاقة تكاملية، حيث تُعزز كل أداة من أدوات الأمن السيبراني فاعلية الأخرى، ما يؤدي في النهاية إلى صياغة استراتيجية أمنية متماسكة تُشكل بدورها عاملاً حاسماً في استدامة المشروع، واستمراره في بيئة رقمية تتسم بالتغير والتعقيد (Nobrega, 2024).

الدراسات السابقة

يُسلّط بحث (dga, 2025) التحليلي لاستراتيجيات التحوّل الرقمي في المملكة العربية السعودية الضوء على الدور المحوري لهيئة الحكومة الرقمية في مساعدة مختلف المؤسسات الحكومية على تحقيق أهدافها في التحوّل الرقمي وتطبيق حلول مبتكرة. وفي هذا الصدد، تُقدّم الهيئة مجموعة متنوعة من الخدمات الاستشارية، مثل تحليل مبادرات التحوّل الرقمي والتأكد من توافقها مع الأهداف الوطنية للتحوّل الرقمي. وقد شكّلت هذه الخدمات أساساً لبحثنا. في عالم يشهد تحوُّلاً رقمياً متسارعاً، تطمح المملكة العربية السعودية إلى أن تكون في طليعة هذه الثورة. وفي هذا السياق، يُقدّم تقرير البحث الصادر عن هيئة الحكومة الرقمية لمحة عامة عن أنشطة المؤسسات الحكومية في هذا الصدد، مُستعرضاً مجالات التحسين المهمة والأهداف الاستراتيجية والجوانب المشتركة عبر برامج التحوّل الرقمي. ويُقدّم هذا التقرير نظرة شاملة على رحلة التحوّل الرقمي في المملكة وتوصيات للخطوات التالية.

برزت بيانات الاختبار التنظيمية كأداة مهمة لتسريع تبني التقنيات الجديدة في المملكة العربية السعودية. فهي توفر بيئة خاضعة للرقابة، تُمكن الشركات الناشئة والشركات الصغيرة والمتوسطة والشركات القائمة من اختبار الحلول والسلع والخدمات الرقمية المبتكرة تحت إشراف الجهات التنظيمية المختصة. تدعم هذه البرامج أهداف رؤية 2030 من خلال تعزيز النمو الاقتصادي، وتحفيز الاستثمار، وتسهيل تطوير صناعات تكنولوجية جديدة. أنشأت العديد من الجهات الحكومية بيئات اختبارية لمعالجة قطاعات وتطبيقات تكنولوجية محددة:

- أنشأ البنك المركزي السعودي بيئة اختبارية تنظيمية تُركز على التكنولوجيا المالية. يُشجع هذا البرنامج الشركات المحلية والأجنبية المهتمة بتطوير خدمات مالية رقمية مبتكرة في بيئة ديناميكية وخاضعة للرقابة. يهدف البرنامج إلى تحسين المعرفة بتأثير هذه التقنيات على القطاع المالي في المملكة، ومساعدتها على التطور لتصبح مركزاً مالياً ذكياً.
- تسعى بيئة اختبار تطبيقات التوصيل إلى تنظيم ومراقبة قطاعي البريد وتطبيقات التوصيل. يُعزز هذا المشروع توسيع منظومة التوصيل من خلال تقصير وقت التسويق، وخفض تكاليف الخدمة، والسماح لمطوري التطبيقات باختبار خدمات جديدة. إنها تفيد جميع المعنيين، بما في ذلك العملاء والمنتجين ومقدمي خدمات التوصيل.
- يهدف صندوق الاختبار التنظيمي للتقنيات الناشئة إلى مساعدة الشركات على اختبار الحلول المبتكرة القائمة على التقنيات المتقدمة مثل إنترنت الأشياء (IoT)، والبلوك تشين، والحوسبة السحابية، والذكاء الاصطناعي (AI)، والواقع المعزز والافتراضي (AR)، والتوائم الرقمية، والطباعة ثلاثية/رباعية الأبعاد. تتيح صناديق الاختبار هذه للشركات الناشئة والقائمة اختبار نماذج وخدمات الأعمال المبتكرة ضمن إطار تنظيمي مرن. كما يستفيد المشاركون من انخفاض عدم اليقين التنظيمي، وعمليات الموافقة السريعة، وسهولة الوصول إلى التمويل.
- كما طورت هيئة الحكومة الرقمية برنامج صندوق اختبار حصرياً لشركات التكنولوجيا الحكومية. ويسعى إلى التحقيق في المنصات والخدمات الرقمية الجديدة في القطاع العام والإشراف عليها، وتحسين البيئة التنظيمية لخدمات الحكومة الرقمية، وتحسين تجربة المستخدم من خلال حل المشكلات التنظيمية التي تواجهها الشركات والمنظمات في هذا المجال (my, 2025).

في عام ٢٠٢٤، أحرزت المملكة العربية السعودية تقدمًا ملحوظًا في تعزيز بيئة ريادة الأعمال والابتكار، في إطار جهودها المتواصلة لتحقيق رؤية ٢٠٣٠، التي تهدف إلى تنويع الاقتصاد الوطني. وتولي المملكة اهتمامًا بالغًا بدعم الشركات الناشئة، باعتبارها عنصرًا أساسيًا في توفير فرص عمل جديدة ودفع عجلة النمو الاقتصادي طويل الأجل. تواصل المملكة تعزيز بيئة ديناميكية من خلال عدد من البرامج الحكومية ومشاريع الدعم التي تستهدف تسريع نمو الشركات الناشئة في قطاعات متنوعة، بما في ذلك التكنولوجيا، والطاقة المتجددة، والرعاية الصحية، والتعليم، وغيرها. وفي ظل هذه البيئة، طورت العديد من الجهات الحكومية والشركات مبادرات تمويلية، بالإضافة إلى منصات استثمارية، لمساعدة الشركات على الحصول على التمويل اللازم (إبراهيم، 2024).

في إطار هدفها الطموح لرؤية 2030، تتبنى المملكة العربية السعودية التجديد والابتكار الشاملين لتحقيق تحول اقتصادي واجتماعي سريع. ويوجه الرؤساء التنفيذيون السعوديون شركاتهم للوفاء بالتزامات المملكة القوية ببناء اقتصاد مستدام وجاهز للمستقبل، والتي تشمل تعزيز القطاع الخاص، وإنشاء صناعات وقطاعات جديدة، وتوفير آلاف فرص العمل، وتشجيع المشاريع الخضراء. ويؤدي الرؤساء التنفيذيون السعوديون تفاؤلاً خاصاً بشأن آفاق تنمية الاقتصاد المحلي، حيث توقع 77% منهم نمواً في المملكة خلال الاثني عشر شهراً المقبلة، متجاوزين بذلك نظرائهم الإقليميين والعالميين. وتُعد المملكة الوجهة الاستثمارية الأولى للرؤساء التنفيذيين الإقليميين الآخرين خارج بلدانهم. وفيما يتعلق بالاستدامة، قام 72% من الرؤساء التنفيذيين السعوديين باستثمارات صديقة للمناخ في العام السابق، أي أكثر من نظرائهم في الدول الست التي شملتها الدراسة، مما يشير إلى التزام استباقي بموازنة النمو مع المسؤولية البيئية. ولدى الرؤساء التنفيذيين في المملكة جدول أعمال حافل للعام المقبل، حيث يستكشفون إمكانيات السوق الهائلة والتهديدات التي تواجهها، ويعيدون ابتكار شركاتهم للمستقبل (pwc، 2025).

يتناول هذا البحث كيفية مساهمة تكنولوجيا المعلومات في تحقيق أهداف الاستدامة في المملكة العربية السعودية. لا يزال تمكين الشركات من استخدام تكنولوجيا المعلومات بنجاح في مشاريع الاستدامة يمثل صعوبة، لا سيما في المملكة. نقوم بتحليل أربع دراسات حالة لمعرفة كيف تستخدم الشركات السعودية التكنولوجيا لتحقيق أهداف الاستدامة الخاصة بها. تُظهر النتائج توجهاً كبيراً نحو الجهود الخضراء في المملكة، مع استخدام تقنيات مثل إنترنت الأشياء (IoT) وسلسلة الكتل (blockchain) والذكاء الاصطناعي (AI). لعبت هذه التقنيات دوراً حاسماً في زيادة كفاءة الطاقة وتقليل النفقات. يؤكد البحث على دور التدخلات السياسية والشراكات بين القطاعين العام والخاص في تحقيق الاستدامة

البيئية والازدهار الاقتصادي. لتعزيز تطوير الممارسات المستدامة، يجب على الحكومة التركيز على تطوير المهارات الرقمية داخل الشركات وإزالة العقبات التكنولوجية. تُظهر دراسات الحالة لأربع شركات في المملكة العربية السعودية ممارسات مستدامة ومساعدة تكنولوجية مناسبة. تؤكد الدراسة على ضرورة استخدام تكنولوجيا المعلومات والتعاون لتسريع التقدم نحو أهداف الاستدامة الوطنية (Madkhali, 2023).

يهدف هذا المشروع إلى دراسة العوائق والمخاوف المرتبطة بتطبيق ممارسات الأمن السيبراني في المدن الذكية السعودية، بالإضافة إلى تصميم نموذج النظرية الموحدة لقبول واستخدام التكنولوجيا 3 (UTAUT3) القائم على الأمن السيبراني والتحقق منه. وللدراسة هدفان. أولاً، سلطت الضوء على أهم المشاكل والقضايا في تطبيق سياسات الأمن السيبراني في المدن الذكية السعودية. ثانياً، أنشأت نموذجاً قائماً على التكنولوجيا لتطبيق مبادئ الأمن السيبراني في المدن الذكية السعودية. وقد أُجري مسحان لتحقيق هذين الهدفين. كشفت الدراسة الأولية عن مشاكل وثرغات في تطبيق ممارسات الأمن السيبراني في المدن الذكية، بما في ذلك المخاوف بشأن ضعف منصات الأمن السيبراني، وقضايا الخصوصية، وتأثير البنية التحتية الحديثة لتكنولوجيا المعلومات على الثقافة السعودية (ن = 554 من عامة الناس). أما المسح الثاني (ن = 108: متخصصو تكنولوجيا المعلومات) فقد ركز على تطوير نموذج UTAUT3 القائم على الأمن السيبراني والتحقق من صحته، والذي تضمن تسعة عوامل: الأداء المتوقع، والجهد المتوقع، والتأثير الاجتماعي، والظروف التمكينية، والسلامة، والمرونة، والتوافر، والسرية، وسلامة الأمن السيبراني. تم تقييم صحة النموذج وموثوقيته، مما يدل على قدرته على فهم سلوك المستخدم واتجاهات تبني التكنولوجيا في المدن الذكية. وسلطت نتائج الدراسة الضوء على العوامل المؤثرة في تبني تدابير الأمن السيبراني في المدن الذكية السعودية، مؤكدةً على أهمية الاستراتيجيات المحددة، وبرامج التوعية الفعالة، وتعاون الجهات المعنية في تعزيز بيئة رقمية آمنة ومرنة (Alhalafi, 2023).

تتوسع قضايا الأمن السيبراني في الصناعات الخدمية والصناعية في المملكة العربية السعودية مع نمو الاستخدام الرقمي، مما يؤكد على أهمية التدابير الأمنية القوية والوعي بين الشركات الصغيرة والمتوسطة. ونتيجة لذلك، تُعد هذه الدراسة جديدة بالملاحظة نظراً للاعتماد المتزايد على التكنولوجيا الرقمية ومخاوف الأمن السيبراني الخاصة التي تواجهها الشركات الصغيرة والمتوسطة في هذه القطاعات الاقتصادية الحيوية. مع التقدم التقني السريع، أصبحت قدرات تكنولوجيا المعلومات والأمن السيبراني بالغة الأهمية، لا سيما في بيئة ما بعد كوفيد-19. وقد شهد كل من الصناعات الخدمية والصناعية في المملكة العربية السعودية تحولات كبيرة نحو العمليات الرقمية. وكان الغرض من هذه الدراسة

هو التحقيق في تأثير لوائح الأمن السيبراني التنظيمية على المرونة التنظيمية والأداء التجاري طويل الأجل في قطاعي الخدمات والتصنيع في المملكة العربية السعودية، بالإضافة إلى النظر في الآثار الوسيطة والمعدلة للمرونة التنظيمية والثقافة. وقد تم استخدام استراتيجية دراسة كمية تجمع بين تحليل شامل للأدبيات والبيانات الفعلية من عينة من 394 مشاركًا سعوديًّا، مقسمة بالتساوي بين قطاعي الخدمات والصناعة. وتم استخدام Smart PLS 3.3.3 للتحقق من صحة الفرضيات المقدمة. كشفت النتائج عن تأثير إيجابي لسياسات الأمن السيبراني التنظيمية على مرونة المؤسسة. وكان لقوانين الأمن السيبراني التنظيمية تأثير كبير على أداء الأعمال على المدى الطويل؛ ولم يكن للمرونة والثقافة التنظيمية دورٌ مُخفف. تُعد هذه الدراسة من أوائل الدراسات التي تُقدم مراجعةً منهجيةً لقدرات تكنولوجيا المعلومات والأمن السيبراني في قطاعي الخدمات والتصنيع في المملكة العربية السعودية، وخاصةً في فترة ما بعد جائحة كوفيد-19. تُسهم هذه النتائج في النقاش الأكاديمي، ولها آثار إدارية مهمة على الشركات السعودية التي تخوض غمار العصر الرقمي (Al-Somali, 2024).

تهدف دراسة (Al-Zahrani, 2025) إلى استكشاف عوامل النجاح التي دفعت المملكة العربية السعودية إلى صدارة أبحاث الأمن السيبراني. وتسعى إلى توفير إطار شامل للأمن السيبراني يشجع على تبادل المعلومات على مستوى العالم ويعزز معايير الأمن. وتستخدم الدراسة منهجية دراسة الحالة ومنهج البحث النوعي. وقد تناولت الدراسة الأوراق والمنشورات المتعلقة بالأمن السيبراني في المملكة العربية السعودية منذ عام 2017، عندما تأسست الهيئة الوطنية للأمن السيبراني، وحتى تصنيفها كأفضل دولة في مؤشر الأمن السيبراني العالمي 2024. وأجري تحليل موضوعي للمواد المدروسة باستخدام معايير PRISMA لاكتشاف الاتجاهات. وتُظهر نتائج الدراسة أن المملكة العربية السعودية قد تفوقت في مجال الأمن السيبراني بفضل عدد من العوامل المهمة، بما في ذلك نموذج حوكمة مركزي يعمل من خلال عمليات لامركزية، واستثمارات كبيرة في الأمن السيبراني، والتعاون الدولي، وبرنامج تنمية رأس المال البشري الذي يراعي التنوع بين الجنسين. كما تُسلط الدراسة الضوء على ضرورة ربط خطط الأمن السيبراني بالأهداف الوطنية، بالإضافة إلى تعزيز الشراكات بين القطاعين العام والخاص، من أجل تحسين القدرة على مواجهة التهديدات السيبرانية. تُسلط نتائج الدراسة الضوء على عوامل نجاح مهمة ساهمت في ترسيخ مكانة المملكة العربية السعودية كرائدة عالمية في مجال الأمن السيبراني. وتُسلط هذه الدراسة الضوء على عوامل النجاح المهمة التي دفعت المملكة العربية السعودية إلى صدارة تصنيفات الأمن

السيبراني. ويُمكن أن يُشكّل الإطار المُقترح نموذجًا يُحتذى به للدول الأخرى التي تسعى إلى تحسين قدراتها في مجال الأمن السيبراني، مُسلّطًا الضوء على أهمية اتباع أساليب متكاملة تشمل الحوكمة والاستثمار والتعاون وتنمية الموارد البشرية. أحدثت الصناعة 5.0 تحولاً في التكنولوجيا من خلال دمج الأنظمة المادية والشبكات الرقمية. وقد أدت هذه التطورات أيضاً إلى زيادة في الهجمات الإلكترونية، مما يشكل مخاطر كبيرة، لا سيما على الشركات الصغيرة والمتوسطة. تبحث هذه الدراسة في مقاومة الشركات الصغيرة والمتوسطة في المملكة العربية السعودية والمملكة المتحدة لتدابير الأمن السيبراني في سياق الصناعة 5.0، مع التركيز على الحوكمة والسياسات. كما تبحث في الأسباب الثقافية والاقتصادية التي تساهم في هذه المقاومة، مثل ضعف فهم مخاوف الأمن السيبراني، والقيود على الميزانية، وتضارب أهداف الشركات. كما يتناول التقرير أهمية السياسات والقوانين الحكومية في تعزيز ممارسات الأمن السيبراني بين الشركات الصغيرة والمتوسطة، بمقارنة أساليب المملكة العربية السعودية مع أساليب المملكة المتحدة. تعتمد الدراسة نهجاً متعدد الأساليب، يشمل مقابلات مع أصحاب الشركات الصغيرة والمتوسطة وخبراء، لتسليط الضوء على الصعوبات وإمكانات تعزيز حوكمة الأمن السيبراني واللوائح التنظيمية في كلا البلدين. وتسلط النتائج الضوء على أهمية الحلول الشخصية، نظراً للاختلافات الثقافية والاقتصادية بين المملكة العربية السعودية والمملكة المتحدة. تُركز الدراسة على معرفة وتطبيق الأمن السيبراني بين الشركات الصغيرة والمتوسطة السعودية، ومدى التزامها بالمبادئ التوجيهية الأساسية لضوابط الأمن السيبراني (ECC-1:2018). كما تتناول أساليب التوعية والامتثال للأمن السيبراني الحالية في المملكة المتحدة، مُقارنةً مواد المشورة الرسمية المُصممة لمساعدة الشركات الصغيرة والمتوسطة على تحسين عملياتها المتعلقة بالأمن السيبراني. ووفقاً لهذه الدراسة، يُقترح زيادة التفاعل مع هذه الأوراق في كلا البلدين لزيادة فهم الشركات الصغيرة والمتوسطة وثقتها وامتثالها، مما يُعزز وضعها الأمني السيبراني. تُقدم هذه الورقة دراسة مُقارنة للحوكمة والسياسات في المملكة العربية السعودية والمملكة المتحدة، مع توصيات لتحسين الوعي والتثقيف في مجال الأمن السيبراني، وتعزيز الأطر التنظيمية، وتشجيع الشراكات بين القطاعين العام والخاص لمكافحة تهديدات الأمن السيبراني في سياق الثورة الصناعية الخامسة (Rawindaran, 2023).

حققت المملكة العربية السعودية تقدماً هائلاً في مجال الأمن السيبراني. فقد حافظت على إجراءات تنظيمية صارمة للكشف عن المخالفين وتبعهم ومعاقبتهم، مما يحمي مصالح المستخدمين الأفراد والشركات من المخاطر السيبرانية مثل سرقة البيانات. ويؤدي الاعتماد المتزايد على تكنولوجيا المعلومات والخدمات المدعومة بتكنولوجيا المعلومات (ITES) إلى

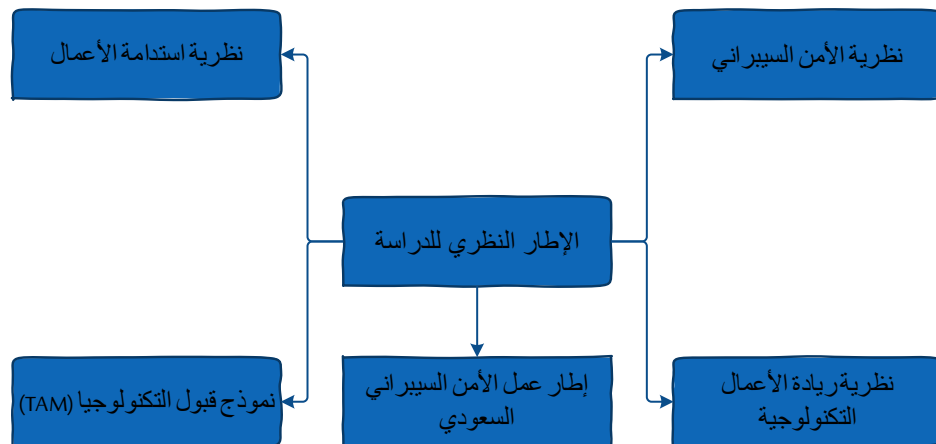
تحسين التدابير الأمنية. وتُعد بيئة التهديد المتغيرة باستمرار للأمن السيبراني قضية مثيرة للجدل. في هذا السياق، تقدم هذه المقالة مراجعة شاملة لكيفية تطور الجرائم الإلكترونية في المملكة العربية السعودية حاليًا، بالإضافة إلى دراسة لبعض أبرز الاعتداءات الإقليمية. وتهدف الأطر والإجراءات التنظيمية الحالية في المملكة العربية السعودية إلى تثبيط السلوك الإجرامي على الإنترنت. وقد تم وضع العديد من نماذج الكفاءة لمعالجة المهارات اللازمة لمنع الجرائم الإلكترونية في هذه البيئة. ويمكن للباحثين في هذا المجال أيضًا الاستفادة من تحديد مستوى الكفاءة الأساسية لضمان الأمن الأمثل. للإجابة على هذه المسألة البحثية، يستخدم هذا التقييم مختبر تجربة وتقييم صنع القرار الضبابي (Fuzzy-DMTAE)، وعملية التسلسل الهرمي التحليلي الضبابي (F.AHP)، ومنهج TOPSIS الضبابي لتحسين كفاءة سياسات الأمن السيبراني القطاعية. يتناول هذا التقييم أوجه التشابه والاختلاف بين هذه المناهج الثلاثة. ويحدد هذا التقييم للأمن السيبراني أن المركز الوطني للأمن السيبراني (NCSC) يُمثل أولوية قصوى. ويواصل التقرير تحليل الصعوبات التي يجب دراستها ومعالجتها من أجل بناء إجراءات أمن سيبراني أكثر مصداقية وفعالية، مما يؤدي إلى اقتصاد قائم على خدمات تكنولوجيا المعلومات (ITES) أكثر تمكينًا في المملكة العربية السعودية. علاوة على ذلك، يجب على خبراء الأمن السيبراني والمسؤولين العمل معًا للدفاع عن الأصول الرقمية للبلاد في عصر الحرب السيبرانية العلنية والسرية (Alhakami, 2024).

باعتباره أحد أهداف التنمية المستدامة، يُعدّ "التعليم للجميع" أمرًا بالغ الأهمية. ومع ذلك، فقد جلب الانخراط في قطاع التعليم مخاطر أمنية وفوائد في آنٍ واحد. فقد جعل تعرّض الطلاب للإنترنت أكثر عرضة لتهديدات الأمن السيبراني. ولتعزيز الاستخدام طويل الأمد للتكنولوجيا، يجب تثقيف الطلاب حول تهديدات أمن المعلومات وكيفية حماية أنفسهم على الإنترنت. في هذا البحث، نقدّم نتائج دراسة مقطعية حول الوعي بأمن المعلومات بين الطلاب السعوديين. استُخدم استبيان إلكتروني لجمع البيانات التجريبية، ثم حُللت باستخدام نمذجة المعادلات الهيكلية الجزئية للمربعات الصغرى. واستنادًا إلى الأدبيات المتاحة، ركّزنا على أربعة مفاهيم رئيسية: إدارة كلمات المرور، وإدارة البنية التحتية، وإدارة البريد الإلكتروني، والإدراك الأمني. ووفقًا لنتائج هذا الاستطلاع، رأى المشاركون أن إدارة البريد الإلكتروني وإدارة البنية التحتية مهمتان، لكن إدارة كلمات المرور والإدراك الأمني لم يكونا كذلك. كما نُقدّم توصيات لرفع مستوى الوعي بالأمن السيبراني بين الطلاب. ومن المرجح أن تُساعد نتائج هذه الدراسة المؤسسات التعليمية وأولياء الأمور على تثقيف الطلاب حول السلوك الآمن على الإنترنت (Saeed, 2023).

التجارة الإلكترونية عنصر أساسي في رؤية السعودية 2030، التي تتمتع بإمكانيات هائلة، لكنها تنطوي أيضًا على خطر الهجمات الإلكترونية. يهدف القطاع المصرفي إلى تعزيز التنمية والابتكار التكنولوجي وزيادة الوصول إلى الخدمات المالية. ويشمل ذلك تعزيز الخدمات المصرفية الرقمية، وزيادة الثقافة المالية، وتوفير التمويل للشركات الصغيرة والمتوسطة. وقد أدى اعتماد القطاع المالي والمصرفي العالمي على التكنولوجيا الجديدة إلى جعله أكثر عرضة للهجمات الإلكترونية. وبالتالي، كان الهدف الرئيسي من هذا البحث هو اكتشاف العناصر التي قد تزيد من الأمن السيبراني بين موظفي البنوك السعودية. وبحث هذه الدراسة في آثار الفائدة المتصورة، والاستعداد التكنولوجي، والتدريب والتطوير، ورضا المستخدم على تبني الأمن السيبراني. كما بحثت في كيفية لعب رضا العملاء دور الوسيط. وقد استخدم نهج بحثي مقطعي في هذه الدراسة. واستُخدمت استبيانات المسح للحصول على بيانات من موظفي البنوك الخاصة السعودية. وبلغ معدل الاستجابة القابل للاستخدام للدراسة 63.14%. وتم تحليل البيانات التي تم جمعها باستخدام Smart PLS 3.3.9. أظهرت النتائج أن الفائدة المُدرَكة، والتدريب والتطوير، والاستعداد التقني، كانت جميعها مؤشرات قوية على رضا المستخدم. وبالمثل، أثر رضا المستخدم بشكل كبير على نوايا تبني الأمن السيبراني. كما دعمت نتائج الدراسة تأثير نوايا المستخدم الوسيط (Mian, 2023).

الإطار النظري للدراسة

تعتمد هذه الدراسة على مجموعة من الأسس النظرية والأفكار الإطارية التي تشكل منصة لفهم العلاقة بين الأمن السيبراني واستدامة المبادرات التكنولوجية النامية، مثل:



رسم توضيحي 1: الإطار النظري للدراسة

• أولاً: نظرية الأمن السيبراني

تستند هذه الدراسة إلى العديد من الأسس النظرية التي تُشكل إطاراً فكرياً لتحليل العلاقة بين تبني استراتيجية الأمن السيبراني واستدامة مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية على المدى الطويل. أولى هذه النظريات هي نظرية الأمن السيبراني، التي تُركز على حماية الأنظمة الرقمية والمعلومات الحيوية من التهديدات والهجمات السيبرانية من خلال إدارة المخاطر الرقمية، وتطبيق التدابير الوقائية والاستباقية، والالتزام بالمعايير التنظيمية التي وضعتها الجهات الرسمية، مثل الهيئة الوطنية للأمن السيبراني (Al-Somali, 2024).

• ثانياً: نظرية استدامة الأعمال

تستند الدراسة أيضاً إلى نظرية استدامة الأعمال، التي تؤكد أن استمرارية المشاريع لا تتحدد فقط بالربحية قصيرة الأجل، بل أيضاً بقدرتها على تحمل العقبات والتكيف مع التغيرات، وخاصةً تلك التي تؤثر على البنية التحتية الرقمية. تُعد الاستدامة التقنية جانباً مهماً في ضمان النجاح التشغيلي لتطوير المبادرات التقنية (Sagar, 2023).

• ثالثاً: نظرية ريادة الأعمال التكنولوجية

تستند الدراسة أيضاً إلى نظرية ريادة الأعمال التقنية، التي تصف كيف تُوفر التطورات التكنولوجية الأساس لنجاح ريادة الأعمال. وهذا يعني أن تطبيق تقنيات الحماية والأمن يُعدّ أحد العوامل التي تعزز ثقة السوق، وله تأثير مباشر على نجاح المشروع واستمراره (Maduwanthi, 2022).

• رابعاً: نموذج قبول التكنولوجيا (TAM)

يستخدم البحث أيضاً نموذج قبول التكنولوجيا (TAM)، الذي يصف كيفية قبول الأفراد والمؤسسات لتقنيات التكنولوجيا. ويُفترض أن اعتماد تقنيات الأمن السيبراني يرتبط برؤية مزاياها المتوقعة وسهولة استخدامها، مما يجعلها عنصراً أساسياً في قرارات الشركات الناشئة (Schorr, 2023).

• خامساً: إطار عمل الأمن السيبراني السعودي

يأخذ التقرير في الاعتبار الإطار الوطني السعودي للأمن السيبراني، الذي يغطي السياسات والأنشطة الموضحة في رؤية المملكة 2030. ويُعدّ التحول الرقمي المستدام جانبًا مهمًا من الأجندة الوطنية، ويُعدّ الأمن السيبراني عنصرًا أساسيًا في حماية الاقتصاد الرقمي المزدهر والحفاظ على تنميته واستدامته (Alnasser, 2024).

الفصل الثالث

منهجية الدراسة

المقدمة

يمثل هذا الفصل من الدراسة المحور التنفيذي الذي يُترجم الإطارين النظري والمفاهيمي إلى خطة بحثية منهجية قابلة للتطبيق، حيث يُعنى بوضع الأسس العلمية التي تم اتباعها في تصميم الدراسة وتنفيذها ميدانيًا. ففي أي بحث علمي يسعى إلى تقديم نتائج موثوقة يمكن البناء عليها لاتخاذ قرارات واقعية، تبرز أهمية التصميم المنهجي الدقيق الذي يراعي طبيعة الظاهرة المدروسة، وأهداف البحث، والسياق الذي تجري فيه الدراسة. ومن هذا المنطلق، يأتي هذا الفصل ليوضح الكيفية التي تم بها تحويل الإشكالية النظرية إلى خطوات عملية قابلة للقياس والتحليل.

يُشكل هذا الجزء من الدراسة حجر الزاوية في بناء مصداقية النتائج، حيث أنه يحدد الإطار العملي الذي تحرك ضمنه الباحث، ويعكس درجة الالتزام بالمنهج العلمي في اختيار العينة، تصميم أدوات جمع البيانات، وتحديد الإجراءات التي تم من خلالها التحقق من دقة النتائج وصدقها. فالبحث العلمي لا يُقاس فقط ببراء الإطار النظري، بل أيضًا بمدى انضباطه المنهجي في التنفيذ، وهو ما يُميز الدراسات الأكاديمية الجادة عن غيرها من الجهود غير المنضبطة أو الارتجالية. وفي ضوء الاهتمام المتزايد بموضوعات الأمن السيبراني وريادة الأعمال في المملكة العربية السعودية، تظهر الحاجة إلى دراسة دقيقة تستند إلى خطوات بحثية ممنهجة، تراعي خصوصية البيئة التقنية السعودية، وتُراعي كذلك التحديات التي تواجه المشاريع التقنية الناشئة في سبيل تحقيق الاستدامة. إن تقديم وصف تفصيلي للطريقة التي تم بها تصميم الدراسة وتنفيذها على أرض الواقع، يُسهم في إظهار مدى التوافق بين أهداف البحث وخطواته التنفيذية، كما يسمح للقارئ بفهم الظروف التي تم فيها جمع البيانات وتحليلها، مما يضيف مصداقية عالية على النتائج التي سيتم استعراضها لاحقًا.

إن هذا الفصل يُمكن الباحث من توضيح مدى التزامه بالمعايير الأخلاقية والعلمية، ويُظهر طريقة اختياره للوسائل التي من خلالها تمت دراسة الظاهرة قيد البحث بشكل موضوعي ومتوازن. كما أنه يُساهم في تعزيز شفافية البحث من خلال الكشف عن البيئة التي نُفذ فيها، وتوضيح الاعتبارات التي أُخذت بعين الاعتبار أثناء إعداد الأداة البحثية واختيار الميدان المناسب، بما يتماشى مع أهداف الدراسة وظروفها.

يُضاف إلى ذلك أن هذا الجزء يُمهّد أيضًا لفهم أفضل للنتائج التي سيتم طرحها في الفصول اللاحقة، إذ يُساعد في تفسيرها ضمن السياق الإجرائي الذي تم فيه تنفيذ الدراسة. وعليه، فإن هذا الفصل لا يؤدي وظيفة وصفية فحسب، بل يلعب دورًا تفسيريًا وتحليليًا محوريًا، يجعل من نتائج البحث لاحقًا أكثر وضوحًا وربطًا بالواقع.

إن القيمة الحقيقية لهذا الفصل تكمن في كونه يُمثل العمود الفقري للجانب التطبيقي من البحث، حيث يُظهر قدرة الباحث على الانتقال من التنظير إلى التطبيق، ومن الطرح النظري إلى المعالجة الواقعية المبنية على خطوات علمية مدروسة. ومن خلال هذا التأسيس، يمكن ضمان أن ما سيتم تقديمه لاحقاً من نتائج وتحليلات، يستند إلى منهجية واضحة، ومقاربة بحثية يمكن إعادة استخدامها في دراسات مستقبلية ضمن السياق نفسه أو سياقات مشابهة.

المنهجية وطرق البحث

1. تصميم البحث

يعتمد تصميم هذه الدراسة على منهجية وصفية تحليلية، مع دراسة حالة كأساس. وتهدف إلى عرض الوضع الراهن وتقييم أثر تطبيق سياسات الأمن السيبراني على جدوى مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية على المدى الطويل. تتيح هذه البنية فهماً شاملاً للتفاعلات بين المتغيرات من خلال جمع وتحليل البيانات الواقعية، بهدف التوصل إلى رؤى قابلة للتعميم جزئياً على مشاريع مماثلة.

2. منهجية دراسة الحالة

يعتمد التقرير على منهجية دراسة الحالة، مع التركيز على عدد محدد من مبادرات التكنولوجيا الناشئة في المملكة العربية السعودية التي طبقت تقنيات الأمن السيبراني. ويسعى هذا الأسلوب إلى تقديم تقييم شامل وكامل لكيفية تأثير هذه الاستراتيجيات على النجاح التشغيلي والمالي لهذه المشاريع على المدى الطويل، مع التركيز على الجوانب التنظيمية والتقنية والبيئية.

3. تقنيات جمع البيانات

يجمع هذا البحث بيانات كمية من عينة الدراسة، وذلك باستخدام استبيان مغلق ذي مقياس ليكرت خماسي النقاط. صُمم الاستبيان ليشمل مواضيع مثل مستوى تنفيذ خطط الأمن السيبراني، وأشكال التهديدات الرقمية، ومعرفة الإدارة بمخاطر الأمن السيبراني، ومؤشرات الاستدامة التشغيلية والتنظيمية. كما سيتم إجراء مقابلات شبه منظمة مع بعض المسؤولين التنفيذيين في مشاريع التكنولوجيا للحصول على بيانات نوعية تُعزز النتائج الكمية وتُثري الدراسة.

4. استراتيجية أخذ العينات

سُتستخدم عينة غير احتمالية، تُعرف غالبًا بالعينة القصدية. سيتم اختيار عينة من مبادرات التكنولوجيا الناشئة المسجلة لدى الهيئة السعودية للمنشآت الصغيرة والمتوسطة (منشآت) والتي تستخدم البنية التحتية الرقمية لأغراض تشغيلية. تم اختيار العينة بناءً على عوامل مثل توافر أنظمة الأمن السيبراني، وعدد سنوات التشغيل، والاعتماد على الخدمات الرقمية لتوفير أو صيانة منتجاتها.

5. أساليب تحليل البيانات

سيتم تحليل البيانات الكمية المجمعة من خلال الاستبيان إحصائيًا باستخدام برنامج SPSS، باستخدام الأساليب الإحصائية الوصفية (المتوسطات الحسابية، الانحراف المعياري) والاستدلالية (اختبار t، تحليل التباين، والانحدار الخطي البسيط والمتعدد) لتحديد العلاقة بين المتغيرات المستقلة (استراتيجيات الأمن السيبراني) والمتغير التابع (استدامة المشروع). سيُستخدم التحليل الموضوعي للكشف عن الأنماط والاختلافات الشائعة في وجهات نظر المشاركين من البيانات النوعية التي جُمعت خلال المقابلات.

6. الصلاحية، والموثوقية، والاعتبارات الأخلاقية

لضمان الصلاحية الداخلية، طُوّرت أدوات الدراسة باستخدام مراجع أكاديمية مرموقة، وعُرضت على مُحكمين محترفين لتقييم مدى ملاءمتها للأهداف. سيُستخدم معامل ألفا كرونباخ لتقييم الموثوقية وضمان اتساق الاستجابات. وفيما يتعلق بالاعتبارات الأخلاقية، تم اتباع معايير البحث الأخلاقي. وتم إطلاع المشاركين على طبيعة البحث، والحصول على موافقتهم الطوعية. وتم التأكيد على سرية البيانات، والتأكد من أنها لن تستخدم إلا لأغراض البحث العلمي، دون الكشف عن هويات المشاركين أو البيانات المؤسسية.

أدوات الدراسة

1. دليل المقابلات شبه المنظمة

يُكان أول هذه الموارد دليلاً للمقابلات شبه المنظمة. أُعدَّ هذا الدليل لتسهيل إجراء مقابلات معمقة مع عدد محدود من مسؤولي الأمن السيبراني والمديرين التنفيذيين العاملين على مبادرات تكنولوجيا ناشئة. كان الهدف هو التعرف على تجاربهم ووجهات نظرهم حول واقع تبني استراتيجيات الأمن السيبراني، والتحديات التي يواجهونها، وتأثير هذه

الاستراتيجيات على أداء المؤسسة واستدامتها. تُعدّ المقابلات شبه المنظمة مفيدة في استخلاص معلومات نوعية لا تستطيع الأساليب الكمية توفيرها.

2. الاستبيان

يُؤد استخدام استبيان كأداة رئيسية للحصول على بيانات كمية. صُمم الاستبيان بمقياس ليكرت خماسي النقاط لتقييم آراء المشاركين حول مدى تبني أساليب الأمن السيبراني وتأثيرها على عوامل الاستدامة الرئيسية. وُزِع الاستبيان على عينة من الموظفين العاملين في مشاريع تكنولوجيا ناشئة، وتضمّن بيانات حول مواضيع الدراسة، مثل فعالية التدابير الأمنية، والاستجابة للطوارئ السيبرانية، والأمن التشغيلي، ورضا العملاء، وثقة المستثمرين.

3. قائمة مراجعة الوثائق

بالإضافة إلى ذلك، استُخدمت أداة قائمة تدقيق الوثائق لتقييم جوهر السياسات والخطط والوثائق الداخلية الرسمية في بعض الشركات التقنية. وشملت الوثائق التي تم تحليلها سياسات أمن المعلومات، وسجلات الحوادث الأمنية، وتقارير الأداء، وخطط الاستدامة. تساعد هذه القائمة على تقييم موثوقية البيانات التي تم الحصول عليها من المشاركين، بالإضافة إلى اكتشاف الممارسات التنظيمية الحقيقية.

4. بروتوكول المراقبة

من أساليب البحث الأخرى تقنية المراقبة، التي طُبقت بشكل روتيني خلال الزيارات الميدانية إلى العديد من الشركات التقنية. راقب هذا البروتوكول سلوك الموظفين أثناء تطبيق اللوائح الأمنية، وتابع إجراءات إدارة البيانات الحساسة، وتتبع الإجراءات المرتبطة بأمن النظام ضد الهجمات الإلكترونية. ووُضعت خطة مراقبة منتظمة لتسجيل هذه النتائج علميًا.

5. برنامج تحليل البيانات

لتحليل البيانات الكمية، استُخدم برنامج SPSS لإجراء تحليلات إحصائية ذات صلة، مثل التكرارات والمتوسط الحسابي والانحراف المعياري، بالإضافة إلى تقييم الارتباطات بين المتغيرات باستخدام تحليل الانحدار. تم تحليل البيانات النوعية من المقابلات والملاحظات موضوعيًا باستخدام أدوات مثل NVivo، مما يسمح للباحث بتحديد الأنماط التفسيرية والمعاني الأساسية وراء إجراءات ومواقف الأمن السيبراني.

مجتمع البحث

يُشكّل مجتمع البحث الأساس الذي تنبني عليه الدراسة الميدانية، ويُعبّر عن الفئة المستهدفة التي تمثل مصدر البيانات الأولية اللازمة للإجابة على أسئلة البحث والتحقق من فروضه. وفي ضوء موضوع هذه الدراسة الذي يركز على العلاقة بين تبني استراتيجيات الأمن السيبراني واستدامة المشاريع التقنية الناشئة في المملكة العربية السعودية، فقد تم تحديد مجتمع البحث بعناية ليتوافق مع طبيعة المشكلة البحثية والهدف منها.

يتكوّن مجتمع البحث في هذه الدراسة من رواد الأعمال، مؤسسي ومديري المشاريع التقنية الناشئة، والعاملين في الإدارات الفنية أو الأمنية في هذه المشاريع، والذين يُعدّون الأكثر ارتباطاً وتأثيراً في عمليات تبني استراتيجيات الأمن السيبراني داخل مؤسساتهم. ويأتي اختيار هذه الفئة تحديداً استناداً إلى مسؤوليتهم المباشرة عن اتخاذ القرارات الاستراتيجية، وتوجيه الموارد، وتحديد أولويات النمو والتوسع، بما في ذلك الجوانب المتعلقة بحماية البيانات وأمن الأنظمة.

تتركّز هذه المشاريع ضمن منظومة ريادة الأعمال التقنية في المملكة، والتي تشهد نمواً ملحوظاً في ظل التحولات الرقمية المتسارعة التي تتبناها الدولة، وضمن بيئة داعمة تشمل حاضنات الأعمال، ومسرّعات النمو، ومراكز الابتكار، إضافة إلى دعم مؤسسات مثل "منشآت"، وصناديق الاستثمار الجريء، والمبادرات الحكومية الرامية إلى تعزيز الاقتصاد الرقمي. وعليه، فإن اختيار هذا المجتمع لا يُعد فقط منطقياً من حيث الصلة بالموضوع، بل هو أيضاً ضروري لفهم كيف تتعامل هذه المشاريع مع التهديدات السيبرانية في بيئة ريادية ناشئة.

ولأن هذه المشاريع تختلف من حيث الحجم، وعدد الموظفين، وطبيعة النشاط التقني، ومستوى النضج المؤسسي، فإن مجتمع البحث في هذه الدراسة يتسم بالتنوع، مما يثري النتائج ويُتيح فهماً أكثر شمولية للواقع. فبعض المشاريع تكون في المراحل الأولية من التأسيس، وتعتمد على فرق صغيرة وإمكانات محدودة، بينما تكون أخرى قد تجاوزت هذه المرحلة وأصبحت في طور النمو أو التوسع، وهو ما قد يؤثر في مدى اهتمامها بالأمن السيبراني وتخصيص الموارد له.

إن دراسة هذا المجتمع تكتسب أهمية إضافية في السياق السعودي نظراً للتوجه الوطني نحو التحول الرقمي، وتعظيم دور الاقتصاد المعرفي، إلى جانب التهديدات السيبرانية المتزايدة التي باتت تستهدف حتى أصغر الكيانات التقنية. وبالتالي، فإن فهم مدى إدراك هذه المشاريع لأهمية الأمن السيبراني، وكيفية تبنيهم لاستراتيجياته، يُسهم بشكل مباشر في تقييم جاهزيتهم للاستدامة، واستمراريتهم في مواجهة التحديات التقنية والأمنية.

إن هذا المجتمع يُعد مصدرًا غنيًا بالمعلومات التي تعكس الواقع العملي لتطبيق الأمن السيبراني في بيئة ناشئة، بعيدًا عن التصورات النظرية، ما يُعزّز من قيمة الدراسة وواقعيتها. كما أن التركيز على المشاريع التقنية الناشئة يُمكن من سد فجوة معرفية قائمة، حيث تندر الدراسات التي تتناول هذه الفئة بالتحديد في ظل ازدياد عددها وتأثيرها الاقتصادي والاجتماعي في المملكة.

إن تحديد مجتمع البحث بدقة، مع مراعاة تنوعه وملاءمته لأهداف الدراسة، يُعد خطوة منهجية أساسية تُسهم في تعزيز جودة البيانات التي سيتم جمعها، وتمكين الباحث من تقديم تحليل دقيق ونتائج قابلة للتطبيق، خاصة في ظل التوجهات السعودية الطموحة نحو بناء اقتصاد رقمي مستدام وآمن.

خطوات جمع البيانات

1. تحديد مصادر البيانات المناسبة

في البداية، كان من الضروري تحديد نوع البيانات المطلوب جمعها ومدى ارتباطها بمشكلة البحث وأهدافه. وبما أن هذه الدراسة تعتمد على المنهج الكمي، فقد تم التركيز على البيانات الأولية التي يتم الحصول عليها بشكل مباشر من مجتمع البحث، نظرًا لما توقّره من معلومات حديثة تعكس الواقع الفعلي للمشاريع التقنية الناشئة في المملكة. وتمثلت هذه البيانات في الآراء والممارسات والإجراءات الفعلية التي تتبعها تلك المشاريع فيما يتعلق بالأمن السيبراني واستراتيجيات الاستدامة.

2. تصميم أداة جمع البيانات

تمثلت الخطوة الثانية في تصميم الأداة البحثية المناسبة، والتي جاءت في صورة استبانة إلكترونية مُهيكلّة، تم تطويرها بعناية لتغطي جميع أبعاد الدراسة: من مستوى تبني استراتيجيات الأمن السيبراني، إلى العوامل التي تؤثر في هذا التبني، وصولًا إلى قياس مدى تأثيره على استدامة المشروع. وقد تم بناء أسئلة الاستبانة استنادًا إلى أدبيات سابقة ونماذج علمية موثوقة، مع الأخذ بعين الاعتبار مواءمتها للبيئة المحلية واللغة المستخدمة في قطاع ريادة الأعمال التقنية. تم تنظيم الاستبانة إلى محاور رئيسية تشمل: بيانات تعريفية عن المشروع، مدى توافر التدريب الأمني، نوعية البرمجيات المستخدمة، وجود الكفاءات المتخصصة، ومؤشرات الاستدامة التنظيمية والتشغيلية. كما تم استخدام مقياس ليكرت الخماسي لتحديد درجة الاتفاق أو التقييم على مجموعة من العبارات، بما يُسهّل لاحقًا عملية التحليل الإحصائي.

3. اختبار صلاحية الأداة (التحكيم والتجريب)

قبل توزيع الاستبانة على مجتمع الدراسة، تم إخضاعها لمرحلة التحكيم العلمي، حيث تم عرضها على مجموعة من الأساتذة والباحثين المتخصصين في مجالات الأمن السيبراني، وتقنيات المعلومات، والبحوث الإحصائية، بهدف التأكد من وضوح الأسئلة وسلامة الصياغة، ومدى ملاءمة المؤشرات المستخدمة لأهداف الدراسة. كما تم إجراء اختبار أولي (Pilot Study) على عينة صغيرة من المشاريع الناشئة بهدف التأكد من فهم المستجيبين للأسئلة، وسهولة الإجابة عليها، والكشف عن أية مشكلات تقنية أو صياغية. وقد أدت هذه المرحلة إلى إدخال بعض التعديلات الطفيفة لتحسين جودة الأداة وضمان دقتها وموثوقيتها.

4. تحديد وسيلة التوزيع وجمع الاستجابات

نظرًا لطبيعة المجتمع المستهدف – والذي يتمثل في مشاريع تقنية ناشئة تعتمد بدرجة كبيرة على الأدوات الرقمية – تم اعتماد التوزيع الإلكتروني كوسيلة أساسية لجمع البيانات. حيث تم إرسال رابط الاستبانة عبر البريد الإلكتروني، ومنصات التواصل الاجتماعي المهنية، والمجموعات الخاصة بريادة الأعمال التقنية، إضافة إلى التعاون مع بعض حاضنات ومسرعات الأعمال المحلية لتسهيل الوصول إلى المشاريع المستهدفة. وقد تم تحديد فترة زمنية لجمع البيانات امتدت لعدة أسابيع، بما يضمن إعطاء المستجيبين وقتًا كافيًا للإجابة، وزيادة حجم العينة المستجيبة، وبالتالي رفع مستوى التمثيل الإحصائي للنتائج.

5. التحقق من اكتمال البيانات وتنظيفها

بعد انتهاء فترة جمع البيانات، تم الانتقال إلى خطوة مراجعة البيانات والتحقق من اكتمالها. حيث تم استبعاد الاستجابات غير المكتملة أو تلك التي أظهرت نمطًا غير جدي (مثل اختيار نفس الإجابة لجميع الأسئلة). ثم تم تحويل البيانات إلى صيغة رقمية مناسبة لبرامج التحليل الإحصائي، مثل SPSS أو Excel، تمهيدًا لتحليلها في الفصل التالي. تُعد هذه المرحلة ضرورية لضمان نزاهة العينة، وتجنب الأخطاء التي قد تؤثر على النتائج وتُضعف من موثوقية الدراسة.

6. الحفاظ على الجوانب الأخلاقية والخصوصية

حرصت الدراسة في جميع خطوات جمع البيانات على الالتزام بالجوانب الأخلاقية، من خلال ضمان سرية المعلومات، وعدم مطالبة المشاركين بإفشاء أية بيانات تعريفية حساسة. كما تم إرفاق مقدمة توضيحية في بداية الاستبانة تتضمن شرحًا لهوية الباحث، وهدف الدراسة، وحق المشاركين في الانسحاب دون إلزام، مع تأكيد أن البيانات ستُستخدم

لأغراض بحثية فقط. هذا الالتزام الأخلاقي يُعد جزءاً أساسياً من جودة أي دراسة أكاديمية، ويُعزز من ثقة المشاركين، ويضمن جمع بيانات دقيقة وغير متحيزة.

حدود البحث

تُعدّ حدود الدراسة سمةً مهمةً يجب تحديدها بوضوح. فهي تُساعد على توضيح نطاق البحث وتحديد الأطر التي أُجريت ضمنها، سواءً من حيث العينة المستهدفة، أو الفترة الزمنية، أو الموقع الجغرافي والمكاني. وفيما يلي القيود المحددة لهذه الدراسة:

• الحدود البشرية

ركّز هذا البحث على الأفراد العاملين في تطوير المبادرات التكنولوجية في المملكة العربية السعودية، بمن فيهم جهات الأمن السيبراني، وكبار المديرين، وموظفو الإدارات التقنية. وقد اختيرت هذه المجموعة لخبرتهم المباشرة في سياسات واستراتيجيات الأمن السيبراني، مما يجعلهم الأكثر تأهيلاً لتقديم إحصاءات موثوقة حول اعتماد هذه الأساليب وتأثيرها على استدامة المشاريع.

• الحدود الزمنية

أُجريت هذه الدراسة من يناير 2024 إلى يونيو 2025. وشهد هذا العام تقدماً هائلاً في تطبيق السياسات الرقمية والتحول الرقمي كجزء من رؤية المملكة 2030. وقد سمح هذا للباحث بتتبع هذه التغييرات وتأثيرها على المبادرات التكنولوجية بطريقة معاصرة وحديثة.

• الحدود المكانية

أُجريت هذه الدراسة في مدن رئيسية في المملكة العربية السعودية، بما في ذلك الرياض وجدة والدمام، وهي مراكز للتطوير والابتكار التقني. تحتضن هذه المدن غالبية المشاريع التكنولوجية الناشئة، وتوفر بيئة داعمة لريادة الأعمال التقنية، مما يجعلها مناسبة لدراسة تأثير الأمن السيبراني على جدوى هذه المبادرات على المدى الطويل.

الفصل الرابع

نتائج الدراسة

يُمثّل هذا الفصل المرحلة الحاسمة في البناء البحثي للدراسة، حيث تلتقي فيه الجهود النظرية والمنهجية التي بُذلت في الفصول السابقة، لتثمر نتائج واضحة تستند إلى تحليل علمي دقيق وموثوق. فبعد استعراض الخلفيات النظرية، وتأطير المفاهيم، وتحديد خطوات التنفيذ الميداني، تأتي هذه المرحلة لعرض المخرجات الحقيقية للدراسة، والتي من خلالها تتضح أبعاد الظاهرة المدروسة، وتُختبر الفرضيات الموضوعة على أرض الواقع.

تنبع أهمية هذا الفصل من كونه يُجسّد عملية الربط العملي بين البيانات التي تم جمعها والأهداف البحثية التي انطلقت منها الدراسة. إذ لا يقتصر دور هذا الجزء على العرض الكمي أو الوصفي للبيانات، بل يتعداه إلى عملية تفسير عميق تساعد في فهم ما تعنيه هذه الأرقام في سياق الدراسة، وما تحمله من مؤشرات حول طبيعة العلاقة بين تبني استراتيجيات الأمن السيبراني واستدامة المشاريع التقنية الناشئة في المملكة. ولذلك، فإن ما يُقدّم في هذا الفصل لا يُعد مجرد نتائج رقمية، بل هو انعكاس ملموس لتفاعلات واقعية حدثت داخل الميدان البحثي، وتم جمعها وتحليلها باستخدام أدوات دقيقة ومُصممة بعناية.

يُتيح هذا الفصل كذلك الفرصة للباحث للانتقال من مجرد جمع البيانات إلى مستوى أعمق يتم فيه تفسير المعطيات ضمن سياقها العملي والنظري، وربطها بالواقع العملي الذي تعيشه المشاريع التقنية في بيئة الاقتصاد الرقمي المتطور في المملكة. فهنا، تتضح ملامح الاتجاهات السائدة، والأنماط المتكررة، والانحرافات التي قد تكشف عن تحديات أو فرص كامنة. ويُعدّ ذلك جزءاً جوهرياً من تحقيق أهداف البحث، لأنه يسمح ببناء فهم أكثر شمولية ودقة للظاهرة المدروسة.

كما يُعد هذا الفصل المجال الطبيعي الذي يمكن من خلاله تقييم مدى اتساق النتائج مع ما تم التوصل إليه في أدبيات سابقة، أو ما تم افتراضه ضمن النموذج النظري الذي تم بناؤه في بداية الدراسة. هذه المرحلة لا تخلو من التحليل النقدي والمقارنة، حيث يُصبح من الممكن فحص أوجه الاتفاق أو الاختلاف مع نتائج دراسات سابقة، والوقوف على المبررات أو الظروف التي قد تُفسر تلك الفروقات. وهو ما يُضفي على البحث عمقاً علمياً ويزيد من قيمته التفسيرية. يُوفّر هذا الفصل مجاًلاً مهماً لطرح الرؤى المستقبلية التي يمكن أن تساهم في تطوير الممارسات العملية داخل المشاريع التقنية، لا سيما فيما يخص دمج ممارسات الأمن السيبراني ضمن الهياكل الإدارية والتشغيلية لتلك المشاريع.

فالدروس المستخلصة من هذا التحليل لا تقتصر على حدود الدراسة، بل تمتد لتقدم إضافة معرفية يمكن أن تستفيد منها قطاعات ريادة الأعمال، وصنّاع السياسات، وحتى الباحثين في مجالات مقاربة.

يُعد هذا الفصل ذروة الجهد البحثي، والمكان الذي تتكامل فيه جميع مكونات الدراسة السابقة لإنتاج معرفة قابلة للفهم والتطبيق، قائمة على أدلة وبيانات وتحليلات منضبطة. وما يُطرح فيه من نتائج وتفسيرات، من شأنه أن يُشكّل الأساس الذي تقوم عليه التوصيات، ويوجّه أصحاب العلاقة نحو قرارات أفضل وأكثر استنادًا إلى الواقع العملي المدروس.

تحليل البيانات

- الوصف الإحصائي للبيانات

الوصف الإحصائي للبيانات هو عملية تحليل البيانات بهدف تلخيصها وتوضيح أهم الخصائص والأنماط التي تتسم بها بشكل مبسط وواضح. يتضمن الوصف الإحصائي مجموعة من الأدوات والطرق التي تُستخدم لتلخيص المعلومات المتاحة في مجموعات البيانات، وتقديم صورة شاملة عن كيفية توزيع القيم وترتيبها.

بعبارة أخرى، يعد الوصف الإحصائي الخطوة الأولى في معالجة البيانات قبل القيام بأي تحليلات متقدمة. يتضمن هذا التوصيف استخدام مجموعة من المقاييس مثل المتوسطات، والانحرافات المعيارية، والوسيط، والمدى، والربعيات، بالإضافة إلى تمثيل البيانات باستخدام الرسوم البيانية مثل المدرج التكراري، والرسوم الصندوقية، والتمثيلات البيانية الأخرى التي تساعد في فهم التركيبة الكلية للبيانات (Yellapu, 2018).

- أهمية الوصف الإحصائي للبيانات

- الوصف الإحصائي يساعد في تبسيط كميات ضخمة من البيانات وتحويلها إلى معلومات قابلة للفهم. فمن خلال استخدام مقاييس مثل المتوسط الحسابي والانحراف المعياري، يمكن تلخيص البيانات المعقدة إلى قياسات تعكس الفكرة العامة للبيانات دون الحاجة إلى النظر إلى كل نقطة بيانات على حدة.
- يمكن للوصف الإحصائي أن يكشف عن الأنماط والتوجهات الرئيسية في البيانات. على سبيل المثال، يمكن أن يكشف توزيع البيانات إذا كانت هناك تركيزات عالية في بعض القيم أو ما إذا كانت البيانات تتبع توزيعاً معيناً (مثل التوزيع الطبيعي). هذا يساعد الباحثين في اتخاذ قرارات قائمة على معلومات واضحة ومدروسة.
- أحد الأغراض المهمة للوصف الإحصائي هو اكتشاف القيم الشاذة أو الاستثنائية (outliers)، وهي القيم التي تختلف بشكل كبير عن معظم البيانات الأخرى. قد تشير هذه النقاط إلى أخطاء في البيانات أو ظواهر غير معتادة تتطلب دراسة إضافية.
- من خلال الفهم الجيد للبيانات المبدئية عبر الوصف الإحصائي، يمكن تحديد الاتجاهات التي يجب التركيز عليها في التحليلات الأكثر تقدماً. على سبيل المثال، إذا أظهرت البيانات أن هناك توزيعاً غير متماثل، فإن الباحثين قد يتوجهون نحو أساليب إحصائية تتعامل مع هذه الخصائص بدقة أكبر.

- إن تمثيل البيانات بشكل وصفي يمكن أن يعزز عملية اتخاذ القرارات، حيث يكون لدى صانعي القرار فهم أفضل للسياق العام للبيانات. هذا مفيد في مجالات مثل الأعمال، والطب، والهندسة، والاقتصاد، حيث يعتمد الأفراد على هذه التحليلات لاختيار الحلول الأكثر فعالية.
- يعد الوصف الإحصائي أيضًا مرحلة تمهيدية مهمة قبل تطبيق التقنيات الإحصائية المتقدمة مثل تحليل الانحدار، والتحليل التبايني، أو النمذجة الرياضية. يساعد ذلك في اختيار الأدوات المناسبة وتحديد الفرضيات الأساسية التي يمكن اختبارها في الدراسات المتعمقة (Adebajo, 2023).

Statistics							
Std. Error of Kurtosis	Kurtosis	Std. Error of Skewness	Skewness	Std. Deviation	Std. Error of Mean	N	
						Valid	
0.387	-1.916	0.195	-0.330	0.495	0.040	155	الجنس
0.387	-1.408	0.195	0.361	1.193	0.096	155	العمر
0.387	-1.443	0.195	0.163	1.510	0.121	155	الدرجة العلمية
0.387	-1.195	0.195	-0.154	1.348	0.108	155	لدى المشروع استراتيجيات واضحة للأمن السيبراني.
0.387	-0.984	0.195	-0.261	1.268	0.102	155	يتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني.
0.387	-1.170	0.195	-0.232	1.363	0.109	155	يتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية.
0.387	-1.231	0.195	-0.039	1.373	0.110	155	تبني استراتيجيات الأمن السيبراني مدعوم من الإدارة العليا.
0.387	-1.148	0.195	-0.277	1.367	0.110	155	ساهمت استراتيجيات الأمن السيبراني في حماية بيانات المشروع والعملاء.
0.387	-1.191	0.195	-0.202	1.344	0.108	155	ساعدت الإجراءات الأمنية في تعزيز ثقة العملاء.
0.387	-1.338	0.195	-0.168	1.421	0.114	155	تبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية.
0.387	-1.114	0.195	-0.205	1.301	0.105	155	تطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع.
0.387	-0.963	0.195	-0.301	1.293	0.104	155	الاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق.
0.387	-1.224	0.195	-0.012	1.333	0.107	155	تكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع.
0.387	-1.142	0.195	-0.178	1.314	0.106	155	نقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.
0.387	-1.220	0.195	-0.295	1.409	0.113	155	صعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.
0.387	-1.264	0.195	-0.257	1.415	0.114	155	تعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً.
0.387	-1.124	0.195	-0.391	1.380	0.111	155	هناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.

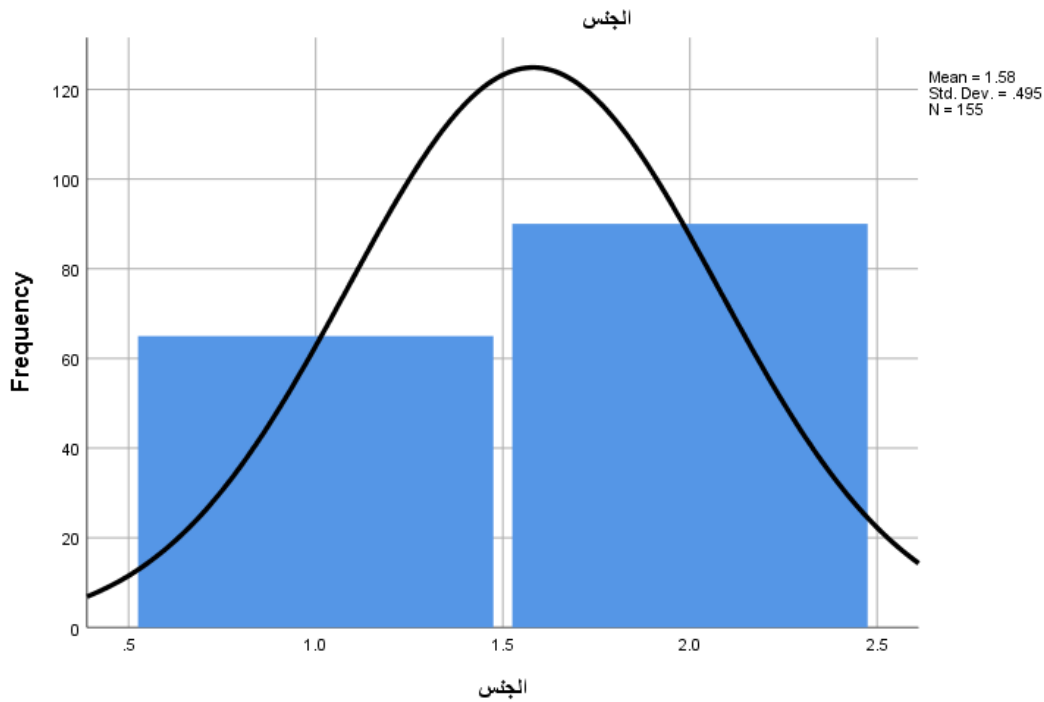
جدول 1: الوصف الإحصائي للبيانات.

- جنس المشاركين في التجربة

اتضح من النتائج أن الأكثر مشاركة في التجربة هم الذكور، وذلك بنسبة 58.1%، مما يدل على أن الذكور يشكلون النسبة الأكبر من المهتمين أو العاملين في مجال المشاريع التقنية الناشئة في المملكة العربية السعودية، وقد يعكس هذا التوجه واقع سوق العمل الحالي في القطاع التقني، حيث لا تزال مشاركة الذكور أعلى من الإناث في هذا المجال، سواء من حيث تأسيس المشاريع أو إدارتها. كما قد يشير إلى وجود فجوة محتملة في تمثيل المرأة في ريادة الأعمال التقنية، وهو ما يستدعي دراسة أعمق لفهم الأسباب وتعزيز مبادرات تمكين المرأة في هذا القطاع الحيوي.

الجنس		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	انثى	65	41.9	41.9	41.9
	ذكر	90	58.1	58.1	100.0
	Total	155	100.0	100.0	

جدول 2: الوصف الإحصائي لجنس المشاركين بالتجربة.



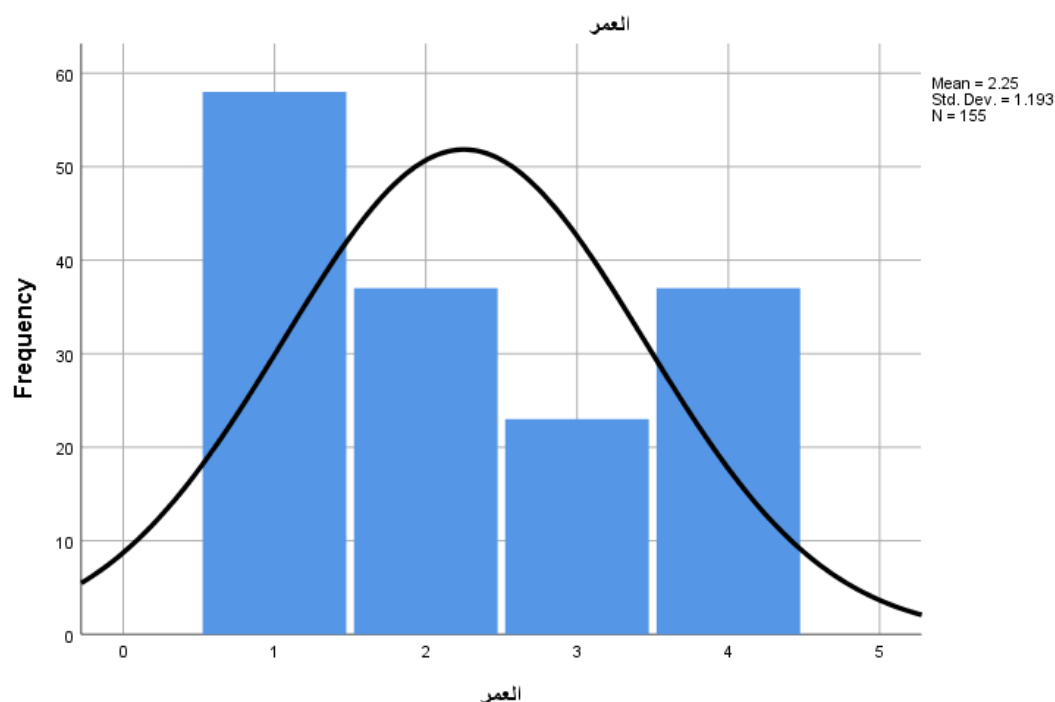
رسم توضيحي 2: التمثيل البياني لجنس المشاركين بالتجربة

- عمر المشاركين في التجربة

اتضح من النتائج أن الأكثر تشاركاً في التجربة انحصرت أعمارهم بين 20 و30 عامًا، وذلك بنسبة 37.4%، مما يدل على أن فئة الشباب هي الأكثر انخراطاً واهتماماً بالمشاريع التقنية الناشئة في المملكة العربية السعودية، وقد يُعزى ذلك إلى طبيعة هذه الفئة العمرية التي تتميز بالحيوية والقدرة على التكيف مع التطورات التقنية الحديثة، إضافة إلى كونها الأكثر استخداماً للتقنيات الرقمية ومعرفةً بمتطلبات الأمن السيبراني. كما يعكس هذا الاتجاه توجهاً وطنياً نحو تمكين الشباب ودعم ريادة الأعمال التقنية ضمن رؤية المملكة 2030، مما يجعلهم قوة دافعة نحو تحقيق الاستدامة في هذا القطاع.

العمر					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-30	58	37.4	37.4	37.4
	31-40	37	23.9	23.9	61.3
	41-50	23	14.8	14.8	76.1
	51-65	37	23.9	23.9	100.0
	Total	155	100.0	100.0	

جدول 3: الوصف الإحصائي لعمر المشاركين بالتجربة.



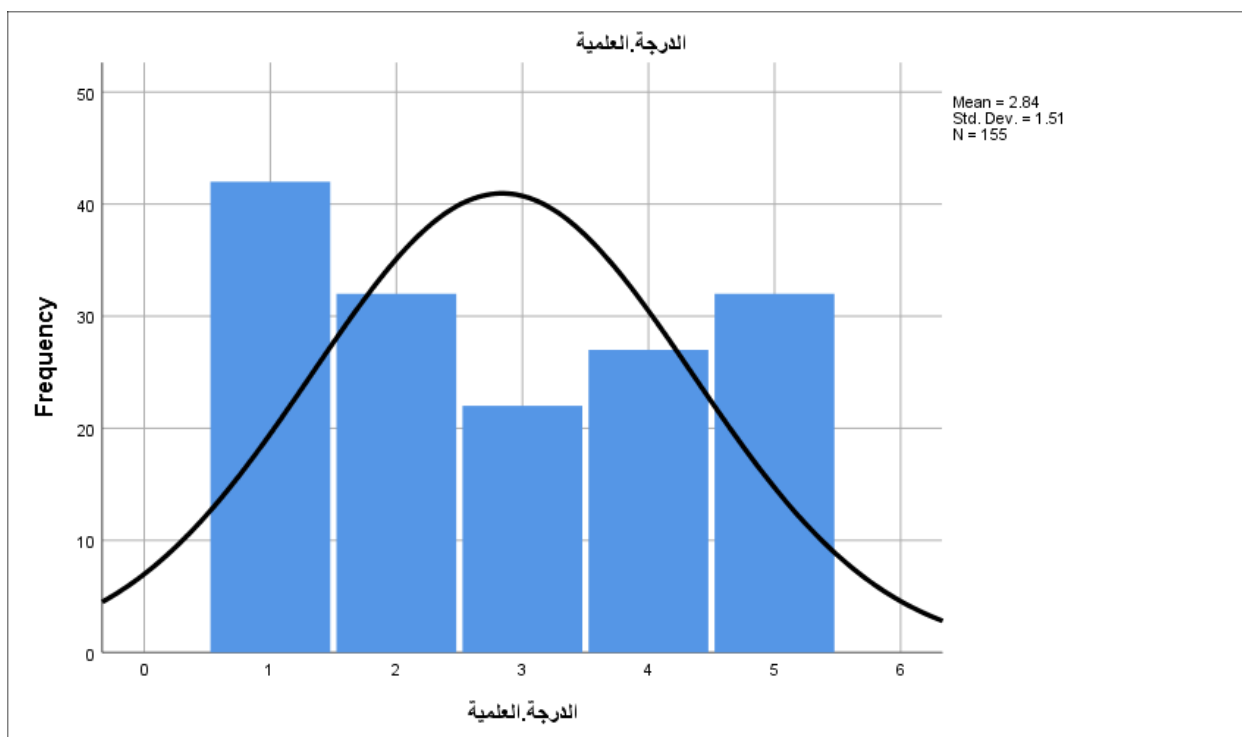
رسم توضيحي 3: التمثيل البياني لعمر المشاركين بالتجربة

- الدرجة العلمية للمشاركين في التجربة

اتضح من النتائج أن الحاصلين على درجة البكالوريوس هم الأكثر تشاركا في التجربة، وذلك بنسبة 27.1%، مما يدل على أن شريحة كبيرة من رواد الأعمال أو العاملين في المشاريع التقنية الناشئة في المملكة يمتلكون مستوى تعليميا جامعيا يؤهلهم لفهم متطلبات الأمن السيبراني وأهميته في استدامة مشاريعهم. كما يعكس ذلك ارتباط مستوى التعليم بالوعي التقني والقدرة على تبني استراتيجيات متقدمة لحماية البيانات والبنى التحتية الرقمية، وهو ما يؤكد دور التعليم العالي في دعم نمو وتطور القطاع التقني، وتحقيق أهداف التحول الرقمي ضمن رؤية المملكة 2030.

الدرجة العلمية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	بكالوريوس	42	27.1	27.1	27.1
	دبلوم	32	20.6	20.6	47.7
	دكتورة	22	14.2	14.2	61.9
	شهادة ثانوية	27	17.4	17.4	79.4
	ماجستير	32	20.6	20.6	100.0
	Total	155	100.0	100.0	

جدول 4: الوصف الإحصائي للدرجة العلمية للمشاركين بالتجربة.



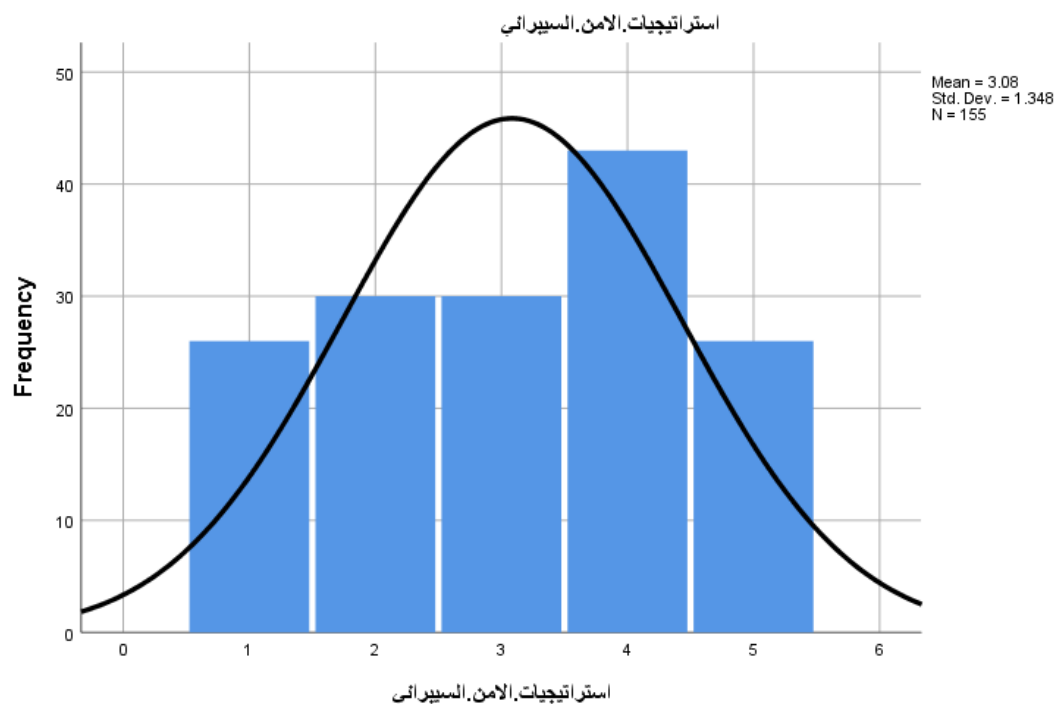
رسم توضيحي 4: التمثيل البياني للدرجة العلمية للمشاركين بالتجربة

- لدى المشروع استراتيجية واضحة للأمن السيبراني.

أكدت استجابات المشاركين بالموافقة على أن لدى المشروع استراتيجية واضحة للأمن السيبراني، وذلك بنسبة 27.7%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن جزءاً كبيراً من المشاريع التقنية الناشئة في المملكة العربية السعودية بات يُدرك أهمية وجود استراتيجية واضحة للأمن السيبراني ضمن بنيتها التشغيلية. ويعكس هذا الوعي المتزايد التوجه الإيجابي نحو تعزيز الحماية الرقمية وضمان استمرارية الأعمال، خاصة في ظل التهديدات السيبرانية المتزايدة. كما يشير إلى أن تبني استراتيجيات أمن سيبراني فعالة قد أصبح عنصراً أساسياً في بناء الثقة لدى العملاء والمستثمرين، ما يعزز فرص استدامة هذه المشاريع على المدى الطويل.

لدى المشروع استراتيجية واضحة للأمن السيبراني					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	26	16.8	16.8	16.8
	غير موافق بشدة	30	19.4	19.4	36.1
	محايد	30	19.4	19.4	55.5
	موافق	43	27.7	27.7	83.2
	موافق بشدة	26	16.8	16.8	100.0
	Total	155	100.0	100.0	

جدول 5: الوصف الإحصائي لدى المشروع استراتيجية واضحة للأمن السيبراني.



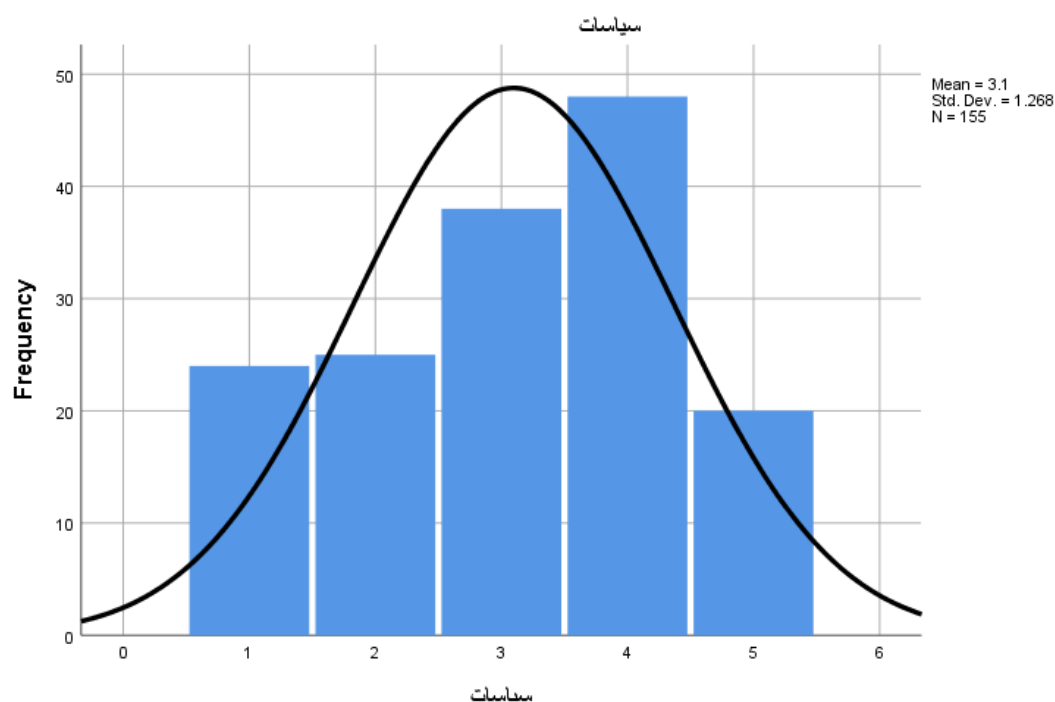
رسم توضيحي 5: التمثيل البياني للبيانات لدى المشروع استراتيجيات واضحة للأمن السيبراني

- يتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري.

أكدت استجابات المشاركين بالموافقة على أنه يتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري، وذلك بنسبة 31.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على وعي ملحوظ لدى المشاريع التقنية الناشئة بأهمية التحديث المستمر لإجراءات الأمن السيبراني لمواكبة التغيرات السريعة في طبيعة التهديدات السيبرانية. كما يعكس ذلك إدراكًا متزايدًا بأن الاستدامة في البيئة الرقمية لا تتحقق فقط بوضع سياسات أمنية، بل بالالتزام بتحديثها وتطويرها بانتظام لضمان فعالية الحماية وتعزيز ثقة العملاء والمستفيدين، وهو ما يتماشى مع أفضل الممارسات العالمية في إدارة المخاطر السيبرانية.

يتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	24	15.5	15.5	15.5
	غير موافق بشدة	25	16.1	16.1	31.6
	محايد	38	24.5	24.5	56.1
	موافق	48	31.0	31.0	87.1
	موافق بشدة	20	12.9	12.9	100.0
	Total	155	100.0	100.0	

جدول 6: الوثائق الإحصائية لبيانات تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري.



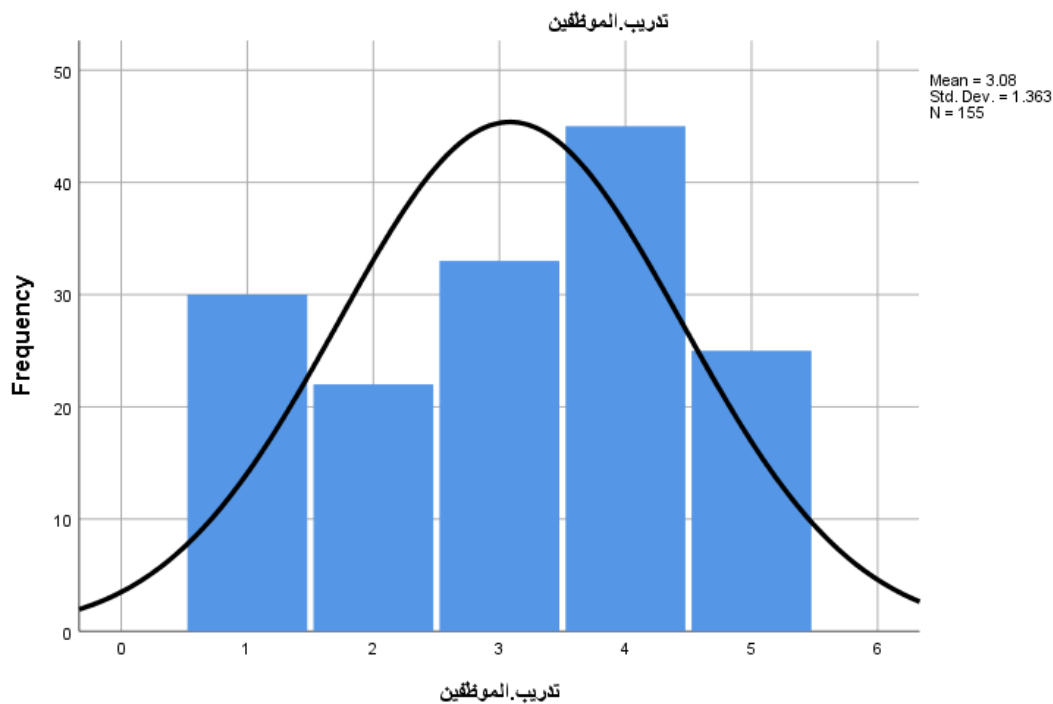
رسم توضيحي 6: التمثيل البياني ليتم تحديث سياسات وإجراءات الأمن السيبراني بشكل دوري

- يتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني.

أكدت استجابات المشاركين بالموافقة على أنه يتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني، وذلك بنسبة 29.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن المشاريع التقنية الناشئة في المملكة العربية السعودية تولي أهمية كبيرة لتأهيل الكوادر البشرية وتعزيز وعيهم الأمني كجزء أساسي من استراتيجيات الحماية السيبرانية. ويُعد هذا التوجه مؤشراً إيجابياً على فهم متزايد بأن العامل البشري يمثل أحد أهم خطوط الدفاع ضد التهديدات السيبرانية، وأن الاستثمار في تدريب الموظفين يساهم بشكل مباشر في تقليل المخاطر الأمنية، ويدعم استدامة المشروع وموثوقيته في بيئة رقمية تتسم بالتطور والتحديات المستمرة.

يتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	30	19.4	19.4	19.4
	غير موافق بشدة	22	14.2	14.2	33.5
	محايد	33	21.3	21.3	54.8
	موافق	45	29.0	29.0	83.9
	موافق بشدة	25	16.1	16.1	100.0
	Total	155	100.0	100.0	

جدول 7: الوصف الإحصائي ليتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني.



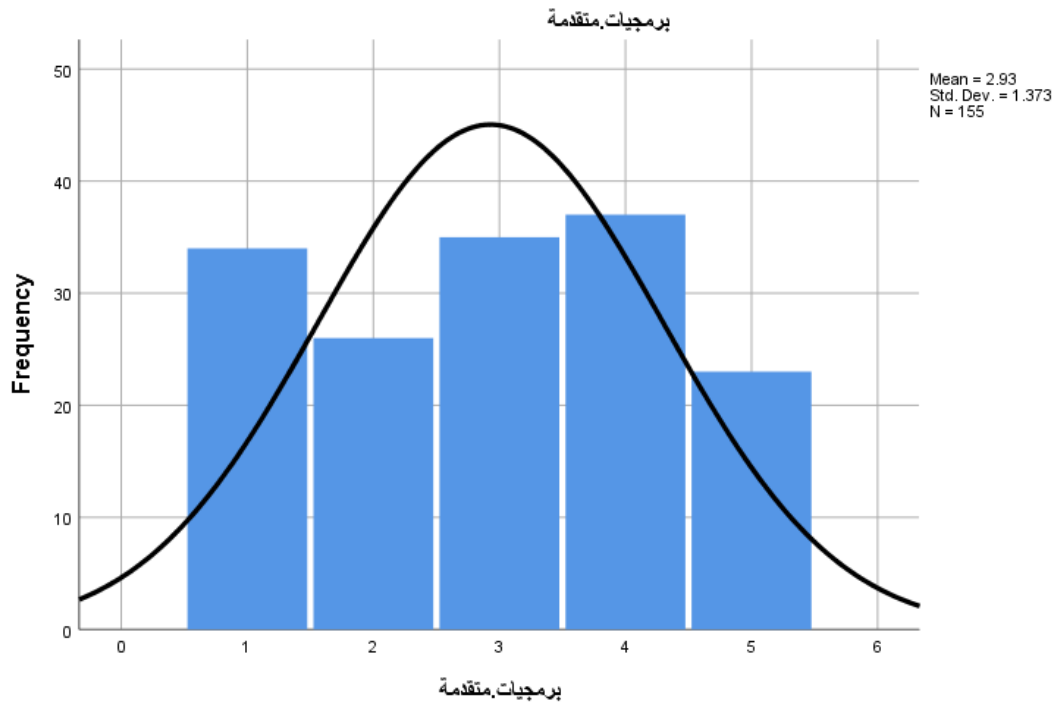
رسم توضيحي 7: التمثيل للبيانات لـ تدريب الموظفين بانتظام على ممارسات الأمن السيبراني

- يتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية.

أكدت استجابات المشاركين بالموافقة على أنه يتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية، وذلك بنسبة 23.9%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن المشاريع التقنية الناشئة في المملكة العربية السعودية بدأت تدرك أهمية تبني حلول تقنية متطورة كجزء من استراتيجياتها الأمنية. ويشير ذلك إلى وعي متنامٍ بضرورة الاستعانة بأدوات متقدمة قادرة على رصد ومنع الهجمات السيبرانية بفعالية، مما يعزز من جاهزية هذه المشاريع لمواجهة المخاطر الرقمية، ويدعم قدرتها على الاستمرار والنمو بثقة في بيئة رقمية متغيرة وسريعة التطور.

يتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	34	21.9	21.9	21.9
	غير موافق بشدة	26	16.8	16.8	38.7
	محايد	35	22.6	22.6	61.3
	موافق	37	23.9	23.9	85.2
	موافق بشدة	23	14.8	14.8	100.0
	Total	155	100.0	100.0	

جدول 8: الوصف الإحصائي لـ استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية.



رسم توضيحي 8: التمثيل البياني لـ استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية

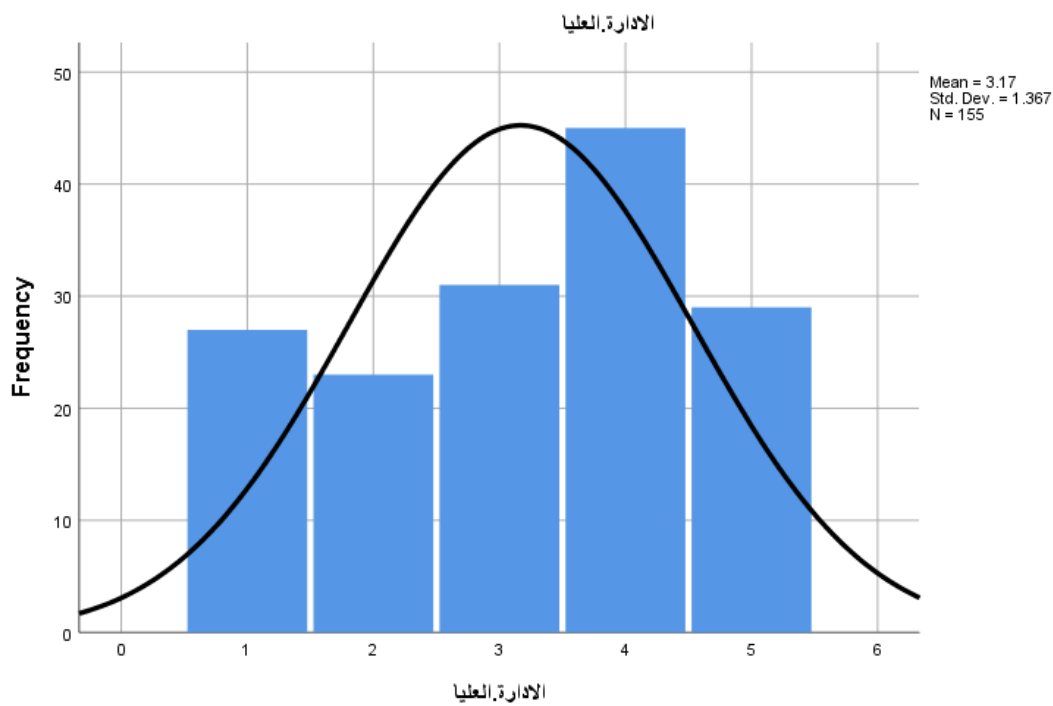
- تبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا.

أكدت استجابات المشاركين بالموافقة على أن تبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا، وذلك بنسبة 29.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن المشاريع التقنية الناشئة في المملكة العربية السعودية بدأت تدرك أهمية الدور القيادي للإدارة العليا في دعم وتفعيل ممارسات الأمن السيبراني. ويُعد هذا الدعم مؤشراً إيجابياً على وجود التزام مؤسسي حقيقي بأمن المعلومات، مما يساهم في

تخصيص الموارد اللازمة، ورفع الوعي بين الموظفين، وضمان تنفيذ السياسات الأمنية بفعالية، وهو ما يعزز من قدرة المشروع على تحقيق الاستدامة في ظل التحديات والتهديدات الرقمية المتزايدة.

تبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	27	17.4	17.4	17.4
	غير موافق بشدة	23	14.8	14.8	32.3
	محايد	31	20.0	20.0	52.3
	موافق	45	29.0	29.0	81.3
	موافق بشدة	29	18.7	18.7	100.0
	Total	155	100.0	100.0	

جدول 9: الوصف الإحصائي لتبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا.



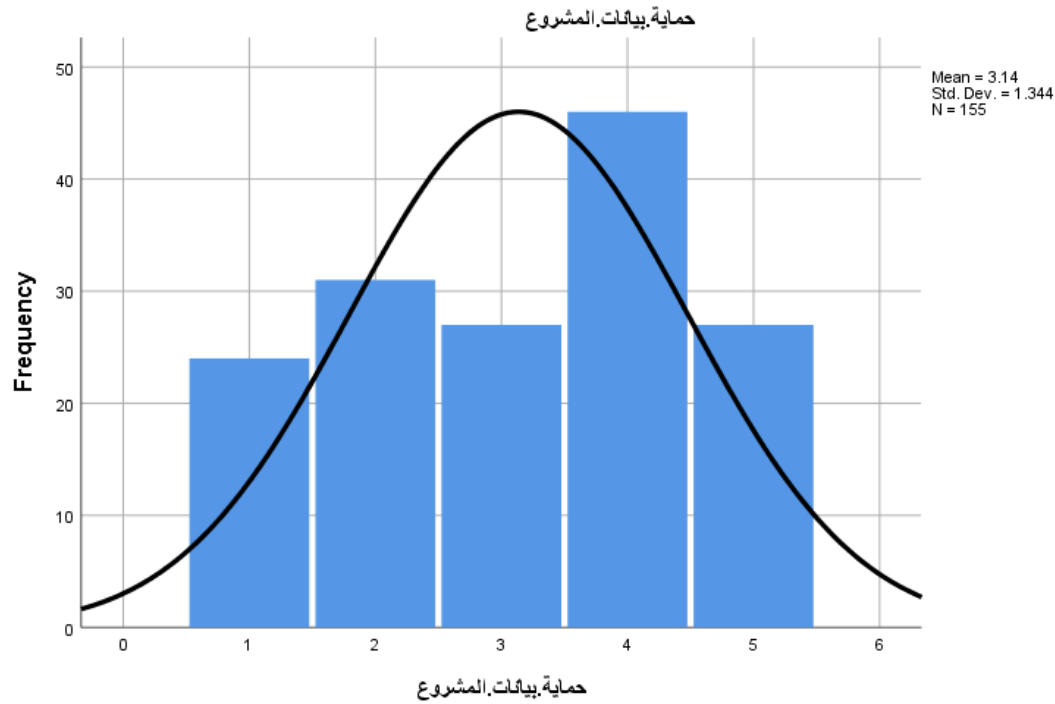
رسم توضيحي 9: التمثيل البياني لتبني استراتيجية الأمن السيبراني مدعوم من الإدارة العليا

- ساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء.

أكدت استجابات المشاركين بالموافقة على أن استراتيجية الأمن السيبراني ساهمت في حماية بيانات المشروع والعملاء، وذلك بنسبة 29.7%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على فاعلية الاستراتيجيات الأمنية المتبعة في المشاريع التقنية الناشئة في المملكة العربية السعودية. ويعكس ذلك وعيًا متزايدًا بأهمية حماية البيانات كأحد الأصول الحيوية للمشروع، خاصة في ظل تصاعد التهديدات السيبرانية وتزايد الاعتماد على الحلول الرقمية. كما يشير إلى أن تبني ممارسات أمنية قوية لا يقتصر فقط على الامتثال، بل يسهم بشكل مباشر في بناء الثقة مع العملاء، وتعزيز سمعة المشروع، وضمان استمراريته ونموه في بيئة تقنية متطورة وسريعة التغير.

ساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	24	15.5	15.5	15.5
	غير موافق بشدة	31	20.0	20.0	35.5
	محايد	27	17.4	17.4	52.9
	موافق	46	29.7	29.7	82.6
	موافق بشدة	27	17.4	17.4	100.0
	Total	155	100.0	100.0	

جدول 10: الوصف الإحصائي لساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء.



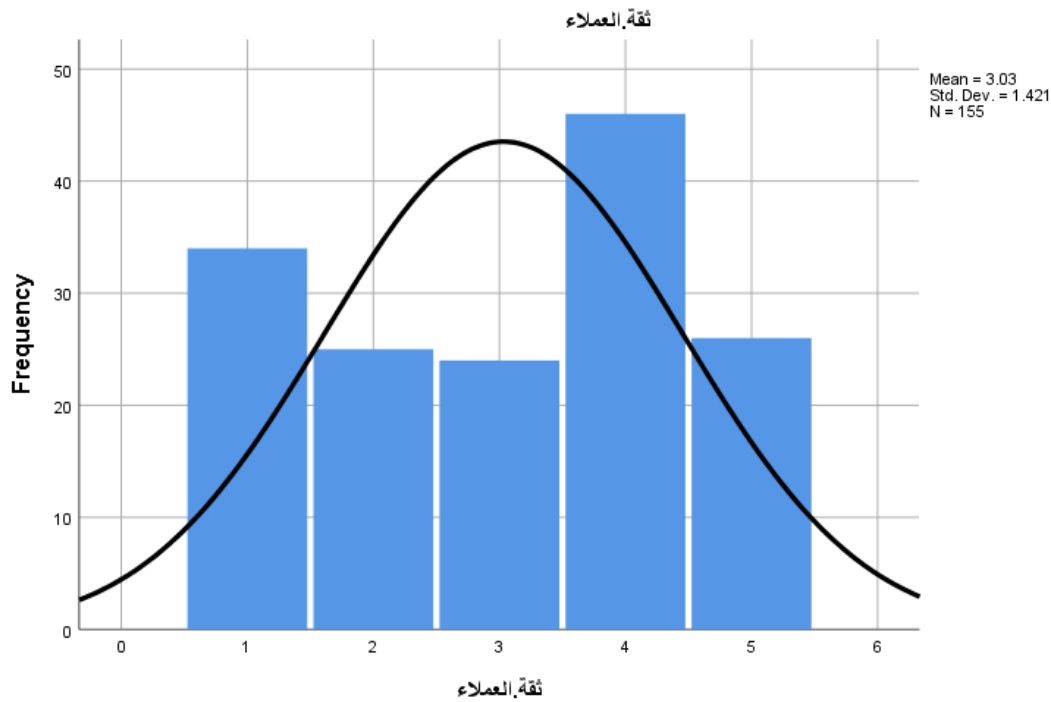
رسم توضيحي 10: التمثيل البياني لساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء

- ساعدت الإجراءات الأمنية في تعزيز ثقة العملاء.

أكدت استجابات المشاركين بالموافقة على أن الإجراءات الأمنية ساعدت في تعزيز ثقة العملاء، وذلك بنسبة 29.7%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن تبني ممارسات فعالة في الأمن السيبراني لا يقتصر تأثيره على حماية الأنظمة والبيانات فحسب، بل يمتد ليشمل بناء علاقة قوية مع العملاء قائمة على الثقة والاطمئنان. ويظهر ذلك أن العملاء أصبحوا أكثر وعياً بأهمية الأمان الرقمي، وأن المشاريع التي تستثمر في أمنها السيبراني تحظى بميزة تنافسية في السوق، مما يسهم بشكل مباشر في استدامتها واستمرار نموها في البيئة الرقمية المتسارعة.

ساعدت الإجراءات الأمنية في تعزيز ثقة العملاء					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	34	21.9	21.9	21.9
	غير موافق بشدة	25	16.1	16.1	38.1
	محايد	24	15.5	15.5	53.5
	موافق	46	29.7	29.7	83.2
	موافق بشدة	26	16.8	16.8	100.0
	Total	155	100.0	100.0	

جدول 11: الوصف الإحصائي لمساعدت الإجراءات الأمنية في تعزيز ثقة العملاء.



رسم توضيحي 11: التمثيل البياني لمساعدت الإجراءات الأمنية في تعزيز ثقة العملاء

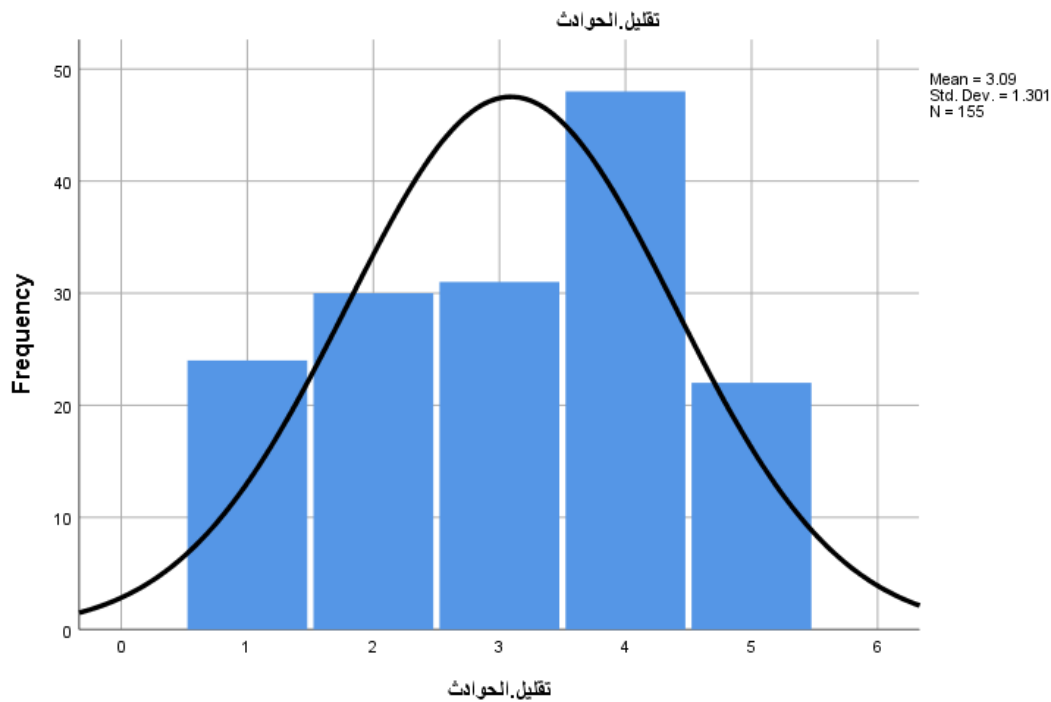
- تبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية.

أكدت استجابات المشاركين بالموافقة على أن تبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية، وذلك بنسبة 31.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على فاعلية الاستراتيجيات الأمنية المتبعة في الحد من التهديدات السيبرانية وتأثيرها السلبي على العمليات التشغيلية. ويعكس

ذلك أن المشاريع التقنية الناشئة في المملكة العربية السعودية أصبحت تدرك أن الاستثمار في الأمن السيبراني لا يُعد خيارًا ثانويًا، بل هو ضرورة تساهم في حماية استمرارية الأعمال وتقليل الخسائر المحتملة، مما يدعم استدامة هذه المشاريع في بيئة عمل رقمية تعتمد بشكل كبير على الكفاءة والاستقرار التقني.

تبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	24	15.5	15.5	15.5
	غير موافق بشدة	30	19.4	19.4	34.8
	محايد	31	20.0	20.0	54.8
	موافق	48	31.0	31.0	85.8
	موافق بشدة	22	14.2	14.2	100.0
	Total	155	100.0	100.0	

جدول 12: الوصف الإحصائي لتبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية.



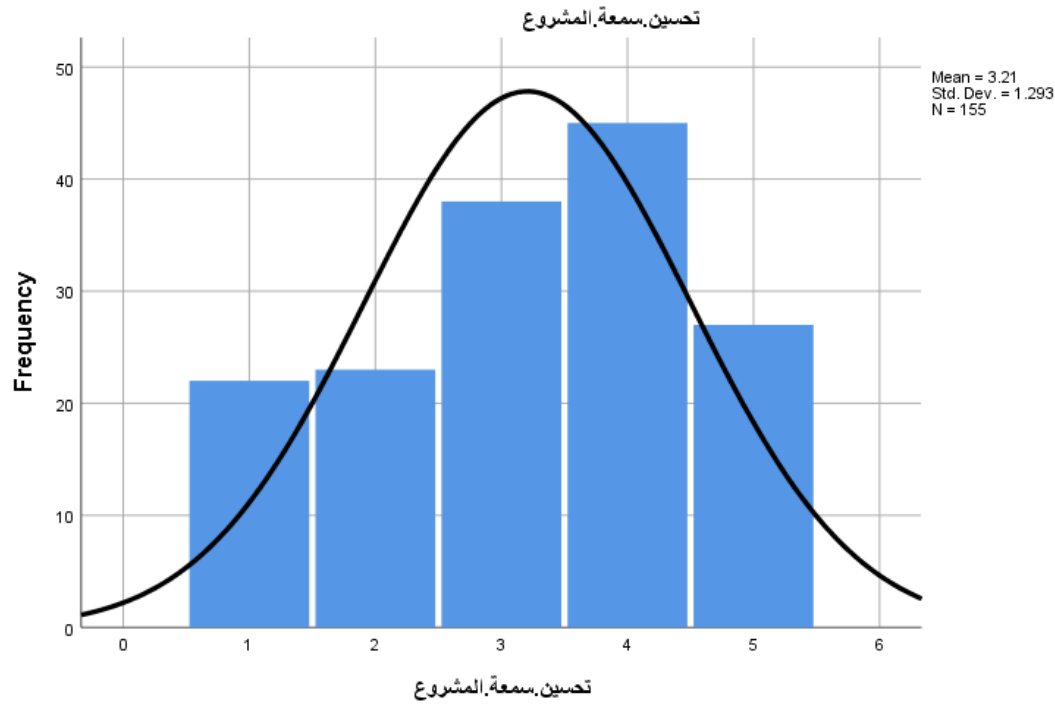
رسم توضيحي 12: التمثيل البياني لتبني الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية

- تطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع.

أكدت استجابات المشاركين بالموافقة على أن تطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع، وذلك بنسبة 29.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن الالتزام بإجراءات وممارسات أمنية فعالة أصبح يُنظر إليه كعامل أساسي في بناء صورة إيجابية وموثوقة للمشاريع التقنية الناشئة في المملكة العربية السعودية. ويعكس ذلك إدراكًا متزايدًا لأهمية الأمن السيبراني ليس فقط كوسيلة للحماية، بل كأداة استراتيجية تعزز من ثقة العملاء والشركاء والمستثمرين، وتمنح المشروع ميزة تنافسية في سوق يتزايد فيه الوعي بقضايا الأمان الرقمي، وهو ما يدعم بشكل مباشر استدامة المشروع ونموه المستقبلي.

تطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	22	14.2	14.2	14.2
	غير موافق بشدة	23	14.8	14.8	29.0
	محايد	38	24.5	24.5	53.5
	موافق	45	29.0	29.0	82.6
	موافق بشدة	27	17.4	17.4	100.0
	Total	155	100.0	100.0	

جدول 13: الوصف الإحصائي لتطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع.



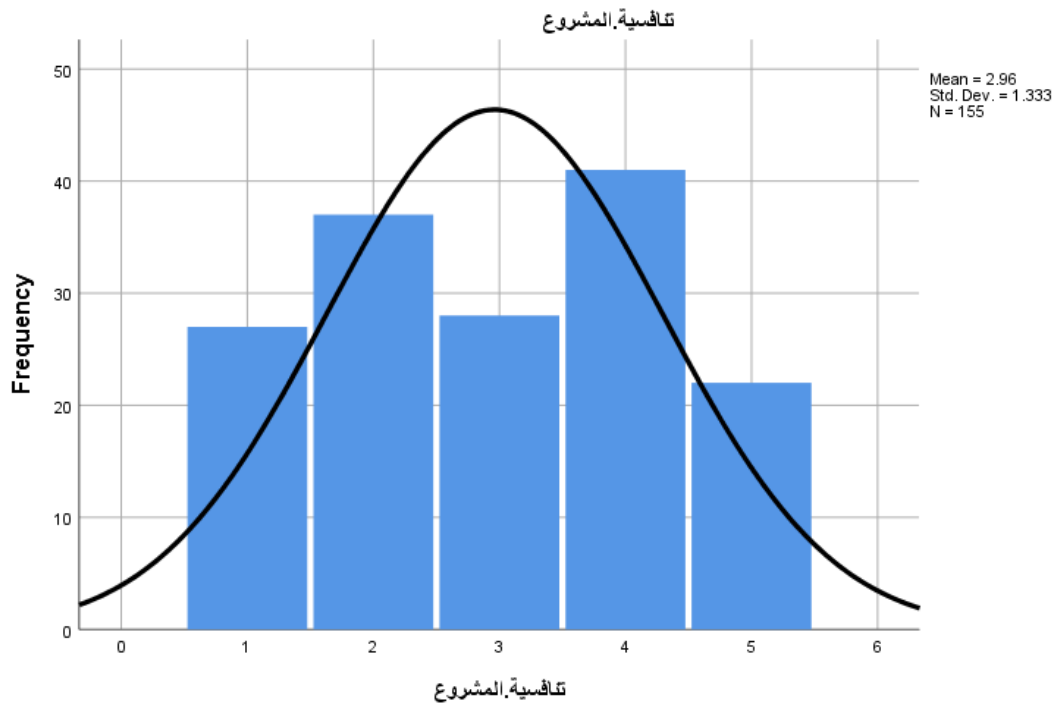
رسم توضيحي 13: التمثيل البياني لتطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع

- الاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق.

أكدت استجابات المشاركين بالموافقة على أن الاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق، وذلك بنسبة 26.5%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن تبني حلول أمنية فعالة لا يُعد فقط وسيلة للحماية، بل يمثل عاملاً استراتيجيًا يساهم في تميز المشروع ضمن بيئة الأعمال التنافسية. ويعكس ذلك وعيًا متزايدًا لدى المشاريع التقنية الناشئة في المملكة العربية السعودية بأهمية الأمن السيبراني كأداة لتعزيز الثقة، وجذب العملاء، وكسب ميزة تنافسية في السوق، الأمر الذي يساهم بشكل مباشر في دعم استدامة المشروع ونموه المستقبلي في ظل التحول الرقمي المتسارع.

الاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	27	17.4	17.4	17.4
	غير موافق بشدة	37	23.9	23.9	41.3
	محايد	28	18.1	18.1	59.4
	موافق	41	26.5	26.5	85.8
	موافق بشدة	22	14.2	14.2	100.0
	Total	155	100.0	100.0	

جدول 14: الوصف الإحصائي للاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق.



رسم توضيحي 14: التمثيل البياني للاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق

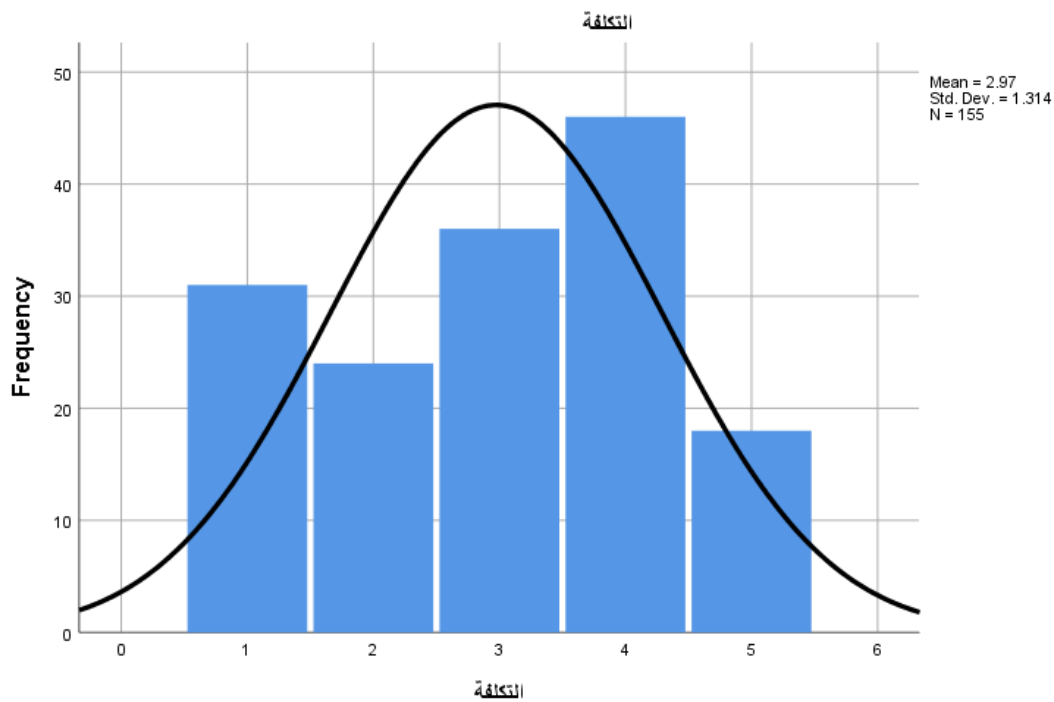
- تكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع.

أكدت استجابات المشاركين بالموافقة على أن تكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع، وذلك بنسبة 29.7%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن التحديات المالية تُعد من أبرز العقبات التي تواجه المشاريع التقنية الناشئة في تبني استراتيجيات الأمن السيبراني بشكل كامل وفعال. ويعكس ذلك الحاجة إلى إيجاد توازن بين أهمية حماية البيانات والأنظمة وبين الموارد المالية المتاحة، كما يشير إلى ضرورة

دعم الجهات المختصة والمستثمرين لهذه المشاريع من خلال توفير حلول تمويلية أو برامج دعم تساعد على تجاوز هذه العقبة، بما يضمن تعزيز استدامتها وقدرتها على مواجهة التهديدات السيبرانية المتزايدة.

تكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	31	20.0	20.0	20.0
	غير موافق بشدة	24	15.5	15.5	35.5
	محايد	36	23.2	23.2	58.7
	موافق	46	29.7	29.7	88.4
	موافق بشدة	18	11.6	11.6	100.0
	Total	155	100.0	100.0	

جدول 15: الوصف الإحصائي لتكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع.



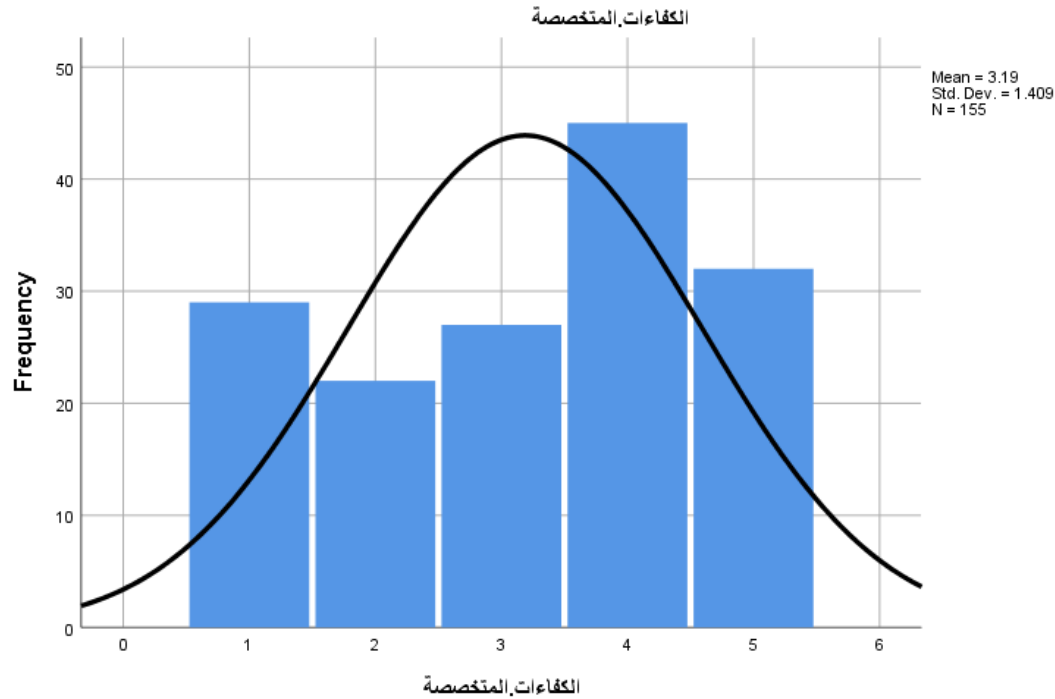
رسم توضيحي 15: التمثيل البياني لتكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع

- نقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.

أكدت استجابات المشاركين بالموافقة على أن نقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً، وذلك بنسبة 29.0%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن المشاريع التقنية الناشئة في المملكة العربية السعودية تواجه صعوبة في الحصول على خبرات ومهارات أمنية متخصصة تضمن تنفيذ استراتيجيات أمنية فعالة. ويعكس هذا الواقع الحاجة الملحة إلى تطوير البرامج التدريبية والتعليمية وتوفير فرص تأهيلية متخصصة في مجال الأمن السيبراني، بالإضافة إلى دعم مبادرات جذب الكفاءات وتأهيلها، وذلك لتعزيز القدرة على حماية المشاريع من التهديدات الرقمية، وبالتالي ضمان استدامتها ونموها في بيئة تقنية متزايدة التعقيد.

نقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	29	18.7	18.7	18.7
	غير موافق بشدة	22	14.2	14.2	32.9
	محايد	27	17.4	17.4	50.3
	موافق	45	29.0	29.0	79.4
	موافق بشدة	32	20.6	20.6	100.0
	Total	155	100.0	100.0	

جدول 16: الوصف الإحصائي لنقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.



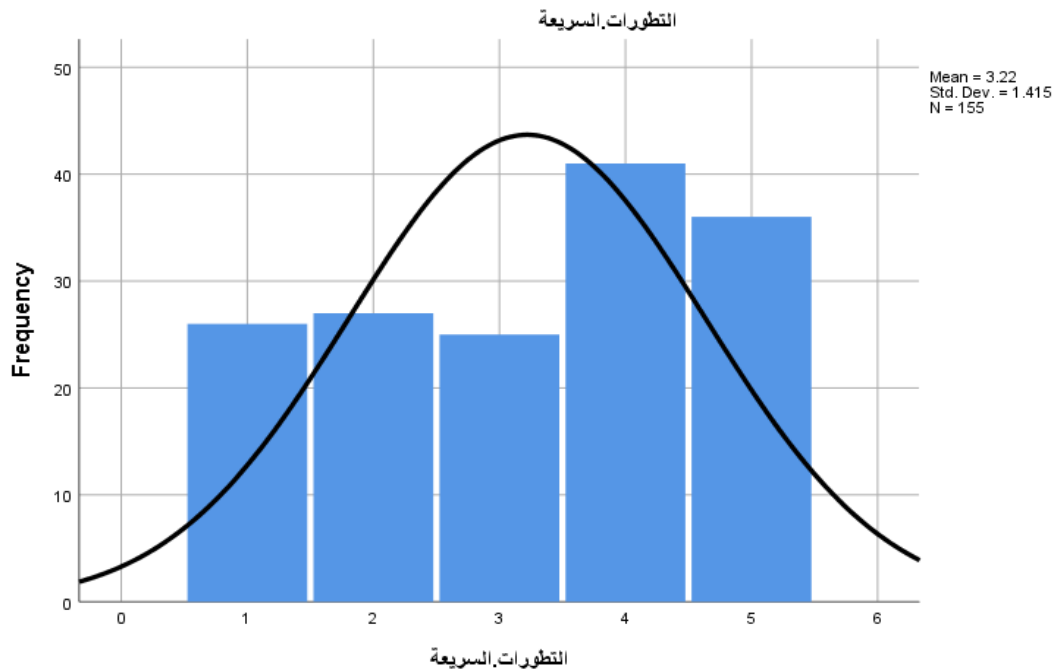
رسم توضيحي 16: التمثيل البياني لنقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً

- صعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.

أكدت استجابات المشاركين بالموافقة على أن صعوبة مواكبة التطورات السريعة في التهديدات السيبرانية تمثل تحدياً، وذلك بنسبة 26.5%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن المشاريع التقنية الناشئة تواجه ضغطاً مستمراً لمواكبة التغيرات المتسارعة في أساليب الهجوم السيبراني والتقنيات المرتبطة به. ويبرز هذا التحدي أهمية تبني نهج استباقي في تحديث استراتيجيات الأمن السيبراني بشكل دوري، بالإضافة إلى الحاجة لتعزيز القدرات التقنية والبشرية للمشروع، لضمان حماية فعالة تواكب بيئة التهديدات الديناميكية، مما يساهم في الحفاظ على استدامة المشاريع وقدرتها على النمو في سوق تنافسية ومعقدة.

صعوبة مواكبة التطورات السريعة في التهديدات السيبرانية					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	26	16.8	16.8	16.8
	غير موافق بشدة	27	17.4	17.4	34.2
	محايد	25	16.1	16.1	50.3
	موافق	41	26.5	26.5	76.8
	موافق بشدة	36	23.2	23.2	100.0
	Total	155	100.0	100.0	

جدول 17: الوصف الإحصائي لصعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.



رسم توضيحي 17: التمثيل البياني لصعوبة مواكبة التطورات السريعة في التهديدات السيبرانية

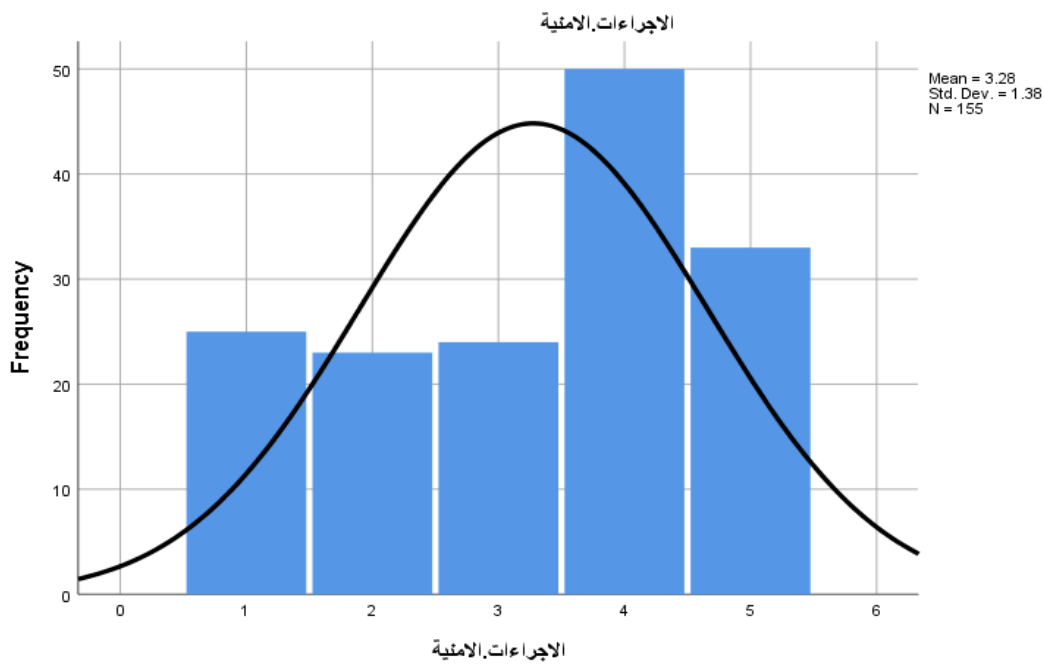
- تعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً.

أكدت استجابات المشاركين بالموافقة على أن تعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً، وذلك بنسبة 32.3%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على أن تطبيق استراتيجيات الأمن السيبراني في المشاريع التقنية الناشئة قد يواجه تحدياً عملياً يتعلق بتوازن بين الحماية الفعالة وسلسلة العمليات التشغيلية. ويشير ذلك إلى ضرورة تصميم وتنفيذ حلول أمنية مرنة ومتكاملة تسمح بحماية قوية دون

التأثير سلباً على إنتاجية الفريق أو سرعة الإنجاز، وهو أمر بالغ الأهمية لضمان قبول الموظفين لهذه الإجراءات واستمرارية الأداء الفعال للمشروع في بيئة تنافسية تتطلب سرعة واستجابة عالية.

تعقيد الإجراءات الأمنية قد يبطن سير العمل أحياناً					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	25	16.1	16.1	16.1
	غير موافق بشدة	23	14.8	14.8	31.0
	محايد	24	15.5	15.5	46.5
	موافق	50	32.3	32.3	78.7
	موافق بشدة	33	21.3	21.3	100.0
	Total	155	100.0	100.0	

جدول 18: الوصف الإحصائي لتعقيد الإجراءات الأمنية قد يبطن سير العمل أحياناً.



رسم توضيحي 18: التمثيل البياني لتعقيد الإجراءات الأمنية قد يبطن سير العمل أحياناً

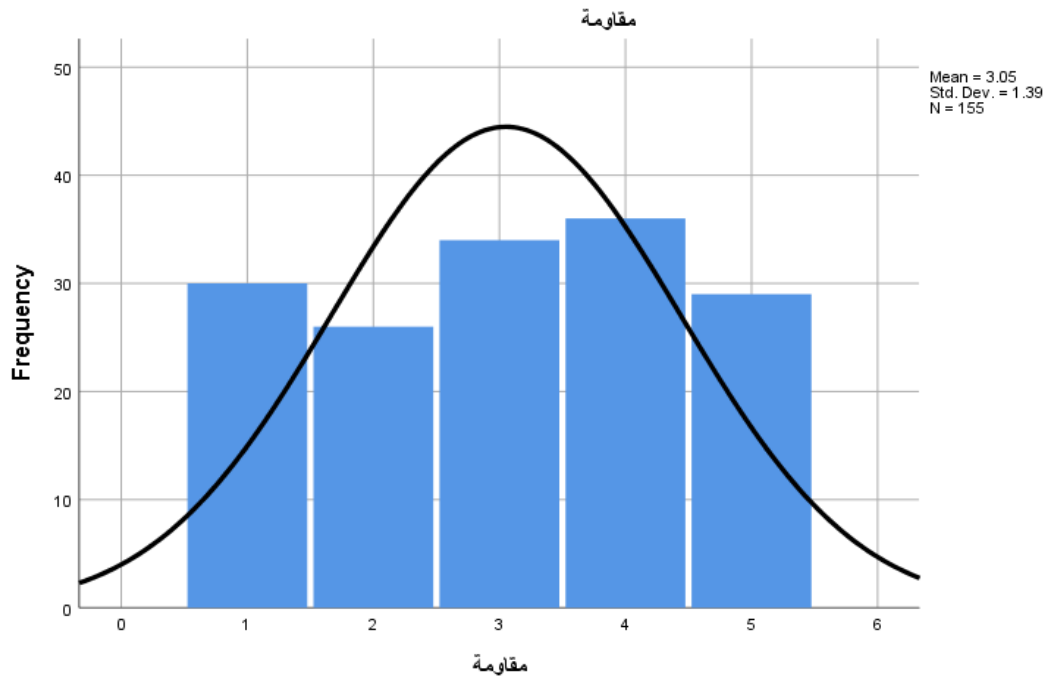
- هناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.

أكدت استجابات المشاركين بالموافقة على أن هناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة، وذلك بنسبة 23.2%، ومثلت هذه النسبة أعلى نسبة استجابة من بين استجابات المشاركين في التجربة، مما يدل على وجود

تحدي بشري مهم يواجه المشاريع التقنية الناشئة في تطبيق استراتيجيات الأمن السيبراني. ويعكس ذلك الحاجة إلى تعزيز ثقافة الوعي الأمني داخل المؤسسات من خلال برامج تدريبية وتواصل فعال، بهدف تقليل المقاومة وتعزيز فهم الموظفين لأهمية هذه الإجراءات، مما يساهم في تسهيل تنفيذ السياسات الأمنية وتحقيق حماية أفضل للمشروع دون التأثير سلباً على بيئة العمل.

هناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	غير موافق	30	19.4	19.4	19.4
	غير موافق بشدة	26	16.8	16.8	36.1
	محايد	34	21.9	21.9	58.1
	موافق	36	23.2	23.2	81.3
	موافق بشدة	29	18.7	18.7	100.0
	Total	155	100.0	100.0	

جدول 19: الوصف الإحصائي لهناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.



رسم توضيحي 19: التمثيل البياني لهناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.

- تحليل الموثوقية والمصدقية لبيانات الدراسة

تشير نتائج ملخص معالجة الحالات (Case Processing Summary) إلى أن جميع البيانات التي تم جمعها في الدراسة كانت صالحة وقابلة للتحليل، حيث بلغ عدد الحالات الصالحة 155 حالة، أي بنسبة 100% من إجمالي العينات، ولم يتم استبعاد أي حالة (0.0%) بسبب نقص البيانات أو عدم اكتمالها. هذا الأمر يعكس جودة عالية في جمع البيانات واهتماماً دقيقاً بضمان اكتمال الاستجابات، مما يعزز ثقة الباحثين في شمولية وتمثيل العينة المستخدمة في الدراسة. كما يضمن ذلك أن النتائج المستخلصة تعكس بدقة آراء ومواقف المشاركين دون وجود تحيز ناتج عن فقدان بيانات.

أما بالنسبة لمؤشر الموثوقية، فيظهر من خلال إحصائية ألفا كرونباخ (Cronbach's Alpha) أن قيمة الموثوقية العامة بلغت 0.822، بينما بلغت قيمة ألفا كرونباخ بناءً على العناصر المعيارية 0.864، وذلك لعدد 18 عنصراً أو سؤالاً تم تضمينه في أداة الدراسة. تُعد هذه القيم مرتفعة ومؤشراً قوياً على أن الأداة البحثية تتمتع بدرجة عالية من الاتساق الداخلي، مما يعني أن العناصر المستخدمة تقيس نفس المفهوم بشكل موحد ومتسق. هذا المستوى من الموثوقية يُعطي ثقة كبيرة في دقة وديمومة النتائج التي تم التوصل إليها، حيث يُعد قيمة ألفا فوق 0.7 عادة معياراً مقبولاً في البحوث الاجتماعية، وقيمة 0.8 أو أعلى تدل على موثوقية ممتازة، مما يعزز مصداقية الاستنتاجات المتعلقة بأثر تبني استراتيجيات الأمن السيبراني على استدامة المشاريع التقنية الناشئة في المملكة العربية السعودية.

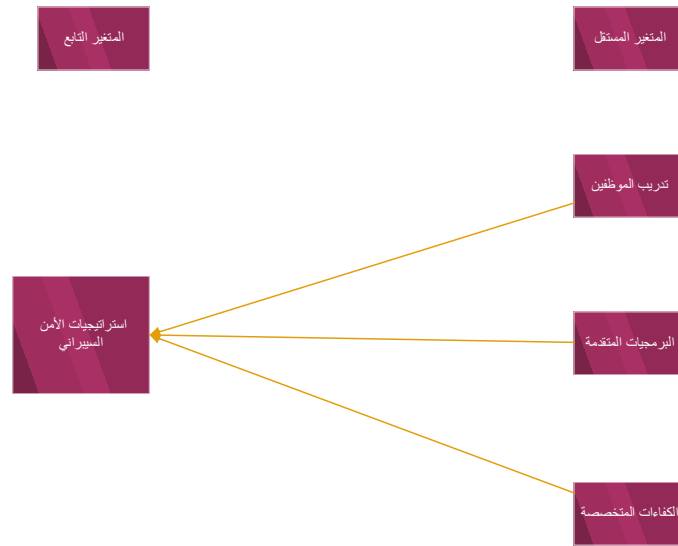
Case Processing Summary			
		N	%
Cases	Valid	155	100.0
	Excluded ^a	0	.0
	Total	155	100.0
a. Listwise deletion based on all variables in the procedure.			

جدول 20: ملخص تحليل البيانات.

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.822	.864	18

جدول 21: تحليل المصدقية والموثوقية للبيانات.

- متغيرات الدراسة



رسم توضيحي 20: متغيرات الدراسة التابعة والمستقلة

- تحليل الجداول المتقاطعة لمتغيرات الدراسة

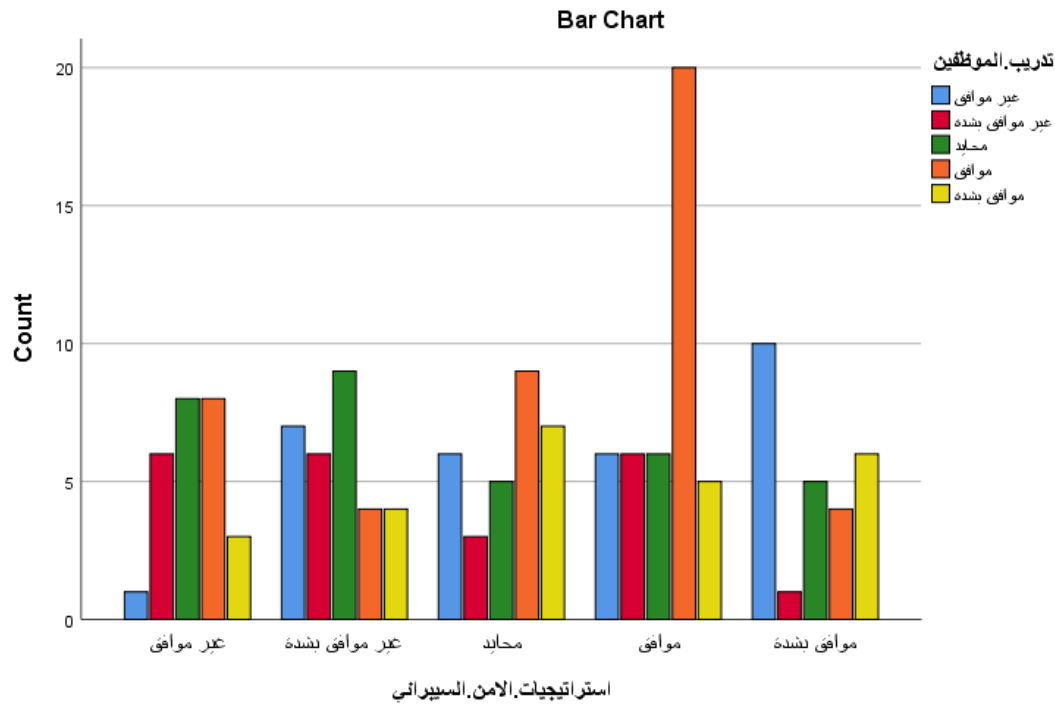
1. دور تدريب الموظفين في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية السعودية
 تعكس نتائج اختبار مربع كاي (Chi-Square) الذي تم إجراؤه لدراسة دور تدريب الموظفين في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية في المملكة العربية السعودية وجود علاقة ذات دلالة إحصائية بين المتغيرات المدروسة. حيث بلغت قيمة اختبار Pearson Chi-Square 28.680 بدرجات حرية 4، وكانت القيمة الاحتمالية (Asymptotic Significance) المصاحبة له 0.026، وهي أقل من مستوى الدلالة التقليدي 0.05، ما يشير إلى رفض فرضية العدم ووجود ارتباط معنوي بين تدريب الموظفين وتطوير استراتيجيات الأمن السيبراني. هذا يعني أن تدريب الموظفين يعد عاملاً مؤثراً وذا أهمية في تحسين وتطوير هذه الاستراتيجيات ضمن المشاريع التقنية الناشئة.

يؤكد اختبار Likelihood Ratio بقيمة 29.876 ومستوى دلالة 0.019 النتائج السابقة، مما يعزز من موثوقية وجود هذا الارتباط الإيجابي. ومع ذلك، فإن اختبار Linear-by-Linear Association أظهر قيمة 0.018 مع مستوى دلالة 0.892، وهو ما يشير إلى غياب علاقة خطية واضحة بين المتغيرات، مما يعني أن تأثير تدريب الموظفين على تطوير استراتيجيات الأمن السيبراني قد لا يكون بالضرورة تصاعدياً أو يتبع نمطاً خطياً بسيطاً، بل قد يتأثر بعوامل أخرى تتداخل في العلاقة. وبالنظر إلى عدد الحالات الصالحة 155، يمكن القول إن النتائج تمثل عينة جيدة نسبياً من مجتمع الدراسة، ما يضيف

إلى قوة التحليل. بصفة عامة، تؤكد هذه النتائج أن تدريب الموظفين يلعب دورًا هامًا في تطوير الاستراتيجيات الأمنية، لكنه قد يتطلب تكاملًا مع عوامل أخرى لتحقيق أثر أكثر وضوحًا وفعالية في تعزيز أمن المشاريع التقنية الناشئة بالمملكة.

Chi-Square Tests			
	Value	Degrees of Freedom	Asymptotic Significance (2-sided)
Pearson Chi-Square	28.680 ^a	4	.026
Likelihood Ratio	29.876	4	.019
Linear-by-Linear Association	.018	1	.892
N of Valid Cases	155		
a. 8 cells (32.0%) have expected count less than 5. The minimum expected count is 3.69.			

جدول 22: اختبار كاي اسكوير لدور تدريب الموظفين في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.



رسم توضيحي 21: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور تدريب الموظفين في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالمملكة العربية السعودية

2. دور البرمجيات المتقدمة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية

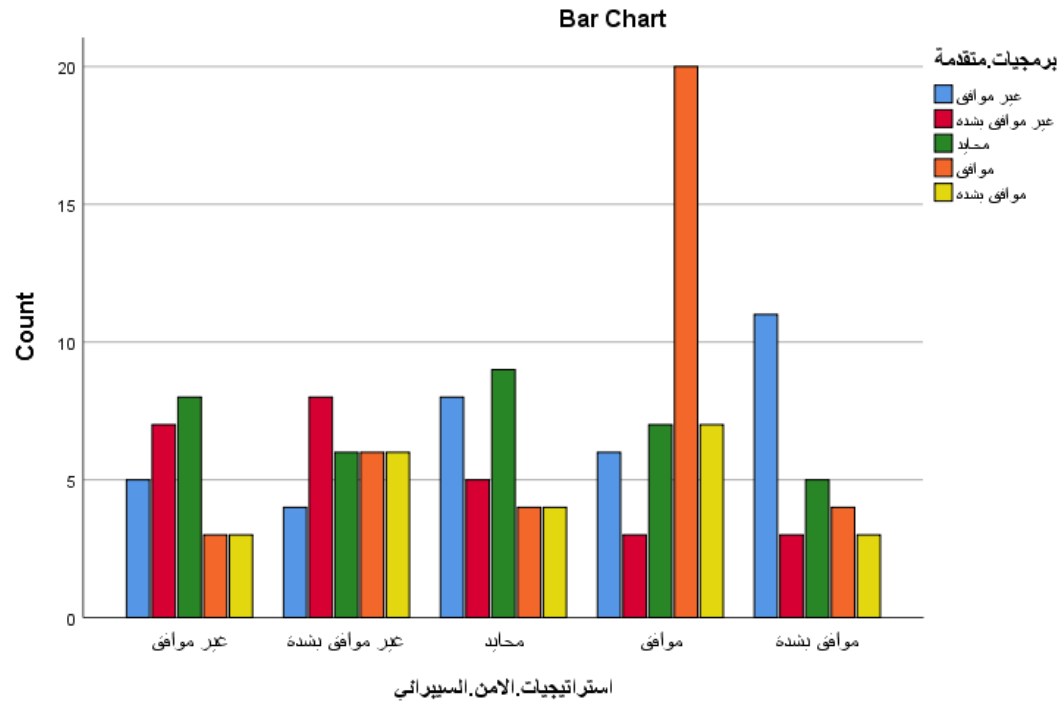
السعودية

تشير نتائج اختبار مربع كاي (Chi-Square) الذي تم إجراؤه لدراسة دور البرمجيات المتقدمة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية في المملكة العربية السعودية إلى وجود علاقة ذات دلالة إحصائية بين استخدام هذه البرمجيات وتطوير الاستراتيجيات الأمنية. حيث بلغت قيمة اختبار Pearson Chi-Square 30.568 بدرجات حرية 3، وكانت القيمة الاحتمالية (Asymptotic Significance) المصاحبة له 0.015، وهي أقل من مستوى الدلالة التقليدي 0.05، مما يدل على رفض فرضية العدم ووجود ارتباط معنوي بين المتغيرين. هذا يشير إلى أن الاعتماد على برمجيات متقدمة يلعب دورًا مهمًا في تحسين وتطوير استراتيجيات الأمن السيبراني ضمن المشاريع التقنية الناشئة.

كما يدعم اختبار Likelihood Ratio هذه النتيجة بقيمة 28.766 ومستوى دلالة 0.026، مما يعزز من صحة وجود هذا الارتباط. بالمقابل، أظهر اختبار Linear-by-Linear Association قيمة 0.029 مع مستوى دلالة 0.864، مما يشير إلى عدم وجود علاقة خطية واضحة بين المتغيرين، وهذا يعني أن التأثير قد لا يتطور بشكل خطي وإنما يتأثر بعوامل متعددة أو قد يظهر بصورة غير مباشرة. وبالنظر إلى أن عدد الحالات الصالحة هو 155، فإن النتائج تعكس عينة تمثيلية جيدة تمكن الباحثين من استخلاص استنتاجات موثوقة حول أهمية البرمجيات المتقدمة في تعزيز استراتيجيات الأمن السيبراني للمشاريع التقنية في المملكة، مع ضرورة مراعاة العوامل المكملية الأخرى لتحقيق أقصى استفادة من هذه التقنيات.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	30.568 ^a	3	.015
Likelihood Ratio	28.766	3	.026
Linear-by-Linear Association	.029	1	.864
N of Valid Cases	155		
a. 6 cells (24.0%) have expected count less than 5. The minimum expected count is 3.86.			

جدول 23: اختبار كاي اسكوير لدور البرمجيات المتقدمة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.



رسم توضيحي 22: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور البرمجيات المتقدمة في تطوير استراتيجيات الامن السيبراني للمشاريع التقنية بالملكة العربية السعودية

3. دور الكفاءات المتخصصة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية

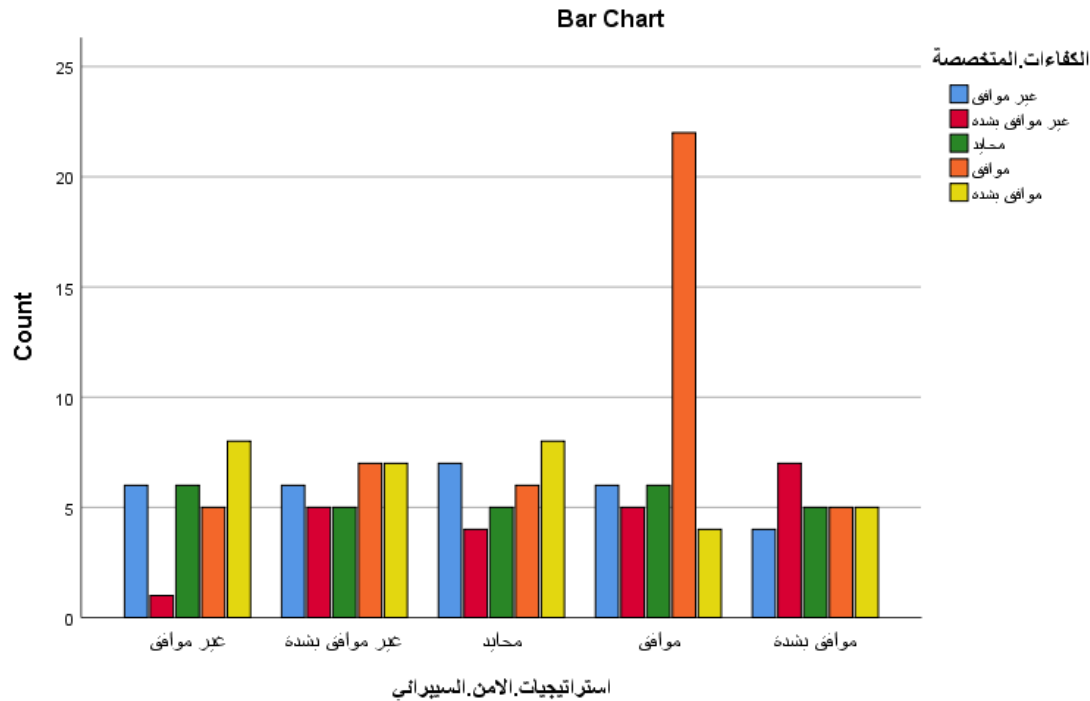
السعودية

تشير نتائج اختبار مربع كاي (Chi-Square) لدراسة دور الكفاءات المتخصصة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية في المملكة العربية السعودية إلى عدم وجود علاقة ذات دلالة إحصائية بين المتغيرات محل الدراسة. حيث بلغت قيمة اختبار Pearson Chi-Square 22.206 بدرجات حرية 4، وكانت القيمة الاحتمالية (Asymptotic Significance) المصاحبة له 0.137، وهي أعلى من مستوى الدلالة التقليدي 0.05، مما يعني عدم رفض فرضية العدم، وبالتالي عدم وجود ارتباط معنوي بين وجود الكفاءات المتخصصة وتطوير استراتيجيات الأمن السيبراني ضمن عينة الدراسة. هذا يشير إلى أن تأثير الكفاءات المتخصصة قد لا يكون واضحاً أو مباشراً في هذه المرحلة من المشاريع التقنية الناشئة، أو أن هناك عوامل أخرى تؤثر على العلاقة.

وبالمثل، تدعم نتائج اختبار Likelihood Ratio هذا الاستنتاج بقيمة 21.874 ومستوى دلالة 0.147، إضافة إلى اختبار Linear-by-Linear Association الذي أظهر قيمة 0.160 مع مستوى دلالة 0.689، مما يشير إلى غياب علاقة خطية واضحة بين المتغيرات. مع الأخذ في الاعتبار أن حجم العينة كان 155 حالة صالحة، يمكن القول إن هذه النتائج توحى بوجود تعقيدات أو عوامل وسيطة تؤثر على دور الكفاءات المتخصصة في تطوير الاستراتيجيات الأمنية، مما يستدعي إجراء مزيد من الدراسات المتعمقة لفهم كيفية تعزيز تأثير هذه الكفاءات بشكل أكثر فعالية في مشاريع الأمن السيبراني بالمملكة.

Chi-Square Tests			
	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	22.206 ^a	4	.137
Likelihood Ratio	21.874	4	.147
Linear-by-Linear Association	.160	1	.689
N of Valid Cases	155		
a. 8 cells (32.0%) have expected count less than 5. The minimum expected count is 3.69.			

جدول 24: اختبار كاي اسكوير لدور الكفاءات المتخصصة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية السعودية.



رسم توضيحي 23: المقاييس المتماثلة في تحليل الجداول المتقاطعة لدور الكفاءات المتخصصة في تطوير استراتيجيات الأمن السيبراني للمشاريع التقنية بالمملكة العربية السعودية

- تحليل التباين الأحادي لمتغيرات الدراسة

تشير نتائج تحليل التباين الأحادي (ANOVA) إلى وجود علاقة ذات دلالة إحصائية بين المتغيرات المستقلة (تدريب الموظفين، البرمجيات المتقدمة، الكفاءات المتخصصة) والمتغير التابع (استراتيجيات الأمن السيبراني) في المشاريع التقنية بالمملكة العربية السعودية. فقد بلغ مقدار مربع التباين التفسيري (Regression Sum of Squares) 47.758، مع 5 درجات حرية، وبلغ متوسط المربع 3.980، في حين بلغ مقدار مربع التباين غير المفسر (Residual Sum of Squares) 232.152 مع 142 درجة حرية ومتوسط مربع 1.635. وقد أظهر الاختبار قيمة F بلغت 2.434 مع مستوى دلالة (Sig.) 0.007، وهو أقل من 0.05، مما يدل على أن النموذج التفسيري الذي يضم المتغيرات المستقلة يفسر بشكل معنوي التغيرات في استراتيجيات الأمن السيبراني. هذا يؤكد أن هناك تأثيراً مشتركاً لهذه العوامل على تطوير وتحسين الاستراتيجيات الأمنية في المشاريع التقنية.

أما ملخص نموذج بايز (Bayes Factor Model Summary)، فيظهر أن معامل الارتباط (R) للنموذج هو 0.413، مما يدل على وجود علاقة متوسطة القوة بين المتغيرات المدروسة واستراتيجيات الأمن السيبراني. أما قيمة R Square فقد بلغت 0.171، أي أن حوالي 17.1% من التغيرات في استراتيجيات الأمن السيبراني يمكن تفسيرها من خلال المتغيرات الثلاثة (تدريب الموظفين، البرمجيات المتقدمة، الكفاءات المتخصصة). بعد تعديل قيمة R Square لأخذ حجم العينة وعدد المتغيرات في

الاعتبار، بلغت القيمة 0.101، وهو ما يشير إلى أن النموذج يقدم تفسيرًا محدودًا لكنه مهم. كما أن الخطأ المعياري للتقدير (Std. Error of the Estimate) بلغ 1.28، مما يعكس مدى دقة التنبؤ بالنموذج. بصفة عامة، تدعم هذه النتائج أهمية التدريب واستخدام البرمجيات المتقدمة والكفاءات المتخصصة في تحسين استراتيجيات الأمن السيبراني، مع الإشارة إلى أن هناك عوامل أخرى محتملة لم يتم تضمينها في النموذج قد تسهم في تفسير المزيد من التباين في هذه الاستراتيجيات.

ANOVA ^{a,b}					
Source	Sum of Squares	df	Mean Square	F	Sig.
Regression	47.758	5	3.980	2.434	.007
Residual	232.152	142	1.635		
Total	279.910	147			
a. Dependent Variable: استراتيجيات الامن السيبراني					
b. Model: (Intercept), تدريب الموظفين, برمجيات متقدمة, الكفاءات المتخصصة					

جدول 25: تحليل التباين الأحادي لمتغيرات الدراسة.

Bayes Factor Model Summary ^{a,b}				
Bayes Factor ^c	R	R Square	Adjusted R Square	Std. Error of the Estimate
.000	.413	.171	.101	1.28
a. Method: JZS				
b. Model: (Intercept), تدريب الموظفين, برمجيات متقدمة, الكفاءات المتخصصة				
c. Bayes factor: Testing model versus null model (Intercept).				

جدول 26: ملخص نموذج عامل بايز^{أ،ب}.

المناقشة

تُعد استراتيجيات الأمن السيبراني من الركائز الأساسية التي تضمن استدامة المشاريع التقنية الناشئة، خاصة في ظل البيئة الرقمية المتسارعة والتحديات المتزايدة التي تواجهها هذه المشاريع في المملكة العربية السعودية. أظهرت نتائج الدراسة أن تبني استراتيجيات أمنية واضحة ومدعومة من الإدارة العليا يمثل حجر الزاوية في حماية بيانات المشاريع والعملاء، وهذا بدوره يعزز من ثقة العملاء في المشاريع الناشئة، حيث يعتبر الأمن السيبراني أحد العوامل الحاسمة التي تؤثر على السمعة التنافسية للمشروع في السوق. وعليه، فإن المشاريع التي تولي اهتمامًا كبيرًا لتطوير هذه الاستراتيجيات وتحسين إجراءاتها الأمنية قادرة على بناء قاعدة عملاء قوية ومستدامة، ما يزيد من فرص نموها وتطورها في بيئة عمل مليئة بالتحديات التقنية والتهديدات السيبرانية المتطورة.

أضافت الدراسة أن تدريب الموظفين بانتظام على ممارسات الأمن السيبراني يسهم بشكل فعال في رفع مستوى الحماية وتقليل مخاطر الاختراقات أو الأعطال التقنية، مما ينعكس إيجابًا على استقرار العمليات التشغيلية داخل المشاريع التقنية. ويشير هذا إلى أن العنصر البشري يمثل خط الدفاع الأول والأهم في منظومة الأمن السيبراني، حيث أن وعي الموظفين بمخاطر التهديدات وكيفية التعامل معها يعزز من فرص اكتشاف وإدارة المخاطر قبل تفاقمها. لكن الدراسة أوضحت أيضًا وجود مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة، وهو تحدٍ بشري يستوجب جهودًا مضاعفة في مجال التوعية وبناء ثقافة أمنية قوية داخل المؤسسات، إذ أن عدم تقبل الموظفين لهذه الإجراءات قد يؤدي إلى ضعف تطبيق السياسات الأمنية ويعرض المشروع لمخاطر أكبر.

على الرغم من الفوائد العديدة لتبني استراتيجيات الأمن السيبراني، أظهرت النتائج أن تكلفة تطبيق هذه الاستراتيجيات تمثل عبئًا ماليًا على المشاريع الناشئة، خصوصًا في مراحلها الأولى التي عادةً ما تعاني من محدودية الموارد المالية. هذا الواقع يبرز الحاجة إلى دعم حكومي أو شراكات مع القطاع الخاص لتوفير التمويل أو التقنيات المناسبة بأسعار معقولة، مما يتيح لهذه المشاريع القدرة على الاستثمار في أمنها السيبراني دون التأثير سلبيًا على جوانب أخرى من العمل. كذلك، تمثل الكفاءات المتخصصة في الأمن السيبراني تحديًا آخر، حيث أن نقص الخبرات الفنية المؤهلة يحد من قدرة المشاريع على تطوير وتنفيذ استراتيجيات أمنية فعالة. بناءً عليه، يتطلب الأمر إنشاء برامج تدريبية متخصصة وشراكات مع المؤسسات التعليمية لتأهيل كوادر قادرة على مواجهة التهديدات المتطورة والمساهمة في بناء بيئة تقنية أكثر أمانًا.

أظهرت الدراسة أن التعقيدات المرتبطة بالإجراءات الأمنية قد تؤدي أحياناً إلى تباطؤ سير العمل داخل المشاريع، وهو ما يتطلب إعادة النظر في تصميم وتنفيذ هذه الإجراءات بحيث تكون مرنة وسهلة التطبيق، دون المساس بمستوى الحماية. فالتوازن بين الأمان وسلاسة العمليات يعتبر من أهم التحديات التي تواجه المشاريع التقنية الناشئة، حيث أن الإجراءات المعقدة قد تخلق عوائق أمام الإنتاجية وقد تؤدي إلى تراجع التزام الموظفين بها. لذلك، يتعين على المؤسسات البحث عن حلول تقنية متقدمة تسهل تطبيق الأمن السيبراني بشكل متكامل دون تعقيد العمل اليومي.

إن تبني استراتيجيات الأمن السيبراني في المشاريع التقنية الناشئة في المملكة العربية السعودية يلعب دوراً جوهرياً في تعزيز استدامة هذه المشاريع وضمان تنافسيتها في السوق الرقمية. ومع ذلك، فإن نجاح هذه الاستراتيجيات يتطلب تضافر الجهود بين الإدارة العليا، والموظفين، والقطاع الحكومي، والقطاع التعليمي لتوفير البيئة المناسبة التي تُمكن المشاريع من حماية نفسها بفعالية، مع معالجة التحديات المالية والبشرية والفنية التي تعترض الطريق. وتعد هذه الدراسة خطوة مهمة في فهم هذه العلاقة المعقدة وتقديم توصيات تساهم في تعزيز الأمن السيبراني، مما يساهم في بناء مستقبل تقني مستدام وقوي في المملكة.

الخاتمة

في ختام هذه الدراسة، يتضح جلياً أن تبني استراتيجيات الأمن السيبراني يمثل عاملاً حاسماً في دعم استدامة المشاريع التقنية الناشئة بالمملكة العربية السعودية. لقد أظهرت النتائج أن المشاريع التي تحرص على وضع استراتيجيات أمنية واضحة ومدعومة من الإدارة العليا، مع تحديث دوري للسياسات الأمنية وتدريب مستمر للموظفين، تتمتع بقدرة أكبر على حماية بياناتها وبيانات عملائها، مما ينعكس إيجابياً على تعزيز ثقة العملاء وتحسين سمعة المشروع في السوق التنافسي. هذا يؤكد أن الاستثمار في الأمن السيبراني ليس مجرد خيار تقني بل ضرورة استراتيجية تضمن استمرار نمو المشاريع واستقرارها في مواجهة التحديات الرقمية المتزايدة.

ورغم الفوائد الواضحة، كشفت الدراسة أيضاً عن تحديات حقيقية تواجه المشاريع الناشئة في تبني وتنفيذ هذه الاستراتيجيات، منها التكلفة المالية المرتفعة التي قد تشكل عبئاً على الموارد المحدودة، ونقص الكفاءات المتخصصة التي تعيق القدرة على تطوير وتنفيذ حلول أمنية فعالة. كما برزت صعوبات أخرى مثل مقاومة بعض الموظفين لتغيير الإجراءات الأمنية وتعقيد تلك الإجراءات أحياناً، مما قد يبطئ العمليات التشغيلية. هذه التحديات تتطلب تبني نهج شمولي يشمل دعماً مالياً وتقنياً من الجهات الحكومية والقطاع الخاص، بالإضافة إلى تطوير برامج تدريب وتأهيل متخصصة لبناء كوادر وطنية قادرة على مواجهة التهديدات السيبرانية المعاصرة بكفاءة.

تؤكد نتائج الدراسة على أهمية الموازنة بين تطبيق إجراءات أمنية مشددة وبين الحفاظ على مرونة العمليات التشغيلية لضمان سير العمل دون عوائق كبيرة، وهو أمر يحتاج إلى ابتكار حلول تقنية متقدمة تعزز الأمان دون تعقيد الإجراءات اليومية. ومن هذا المنطلق، يُمكن النظر إلى الأمن السيبراني كعامل تمكين وليس مجرد عقبة تنظيمية، حيث يعزز من القدرة التنافسية للمشاريع التقنية الناشئة ويضمن نموها المستدام في بيئة سوقية متغيرة ومتطلبة.

تمثل هذه الدراسة مساهمة مهمة في تسليط الضوء على الدور المحوري للأمن السيبراني في تحقيق استدامة المشاريع التقنية الناشئة في المملكة، كما تبرز الحاجة إلى جهود مشتركة وتنسيق مستمر بين كافة الأطراف المعنية لضمان بيئة تقنية آمنة ومستقرة. إن الاستثمار في الأمن السيبراني، بجانب تعزيز القدرات البشرية والتقنية، هو استثمار في مستقبل المشاريع الوطنية ومفتاح لتحقيق رؤية المملكة 2030 التي تسعى إلى اقتصاد رقمي قوي ومزدهر قائم على الابتكار والتكنولوجيا.

التوصيات

- ينبغي على المؤسسات التقنية الناشئة ضمان التزام الإدارة العليا بدعم وتبني استراتيجيات الأمن السيبراني، حيث يلعب هذا الدعم دورًا محوريًا في نجاح تنفيذ السياسات الأمنية وتعزيز ثقافة الأمن داخل المشروع.
- يجب تخصيص موارد كافية وبرامج تدريب منتظمة لرفع وعي وكفاءة الموظفين في ممارسات الأمن السيبراني، حيث يساهم ذلك بشكل كبير في تقليل المخاطر السيبرانية وحماية أصول المشروع.
- على المشاريع الناشئة تبني واستخدام أحدث التقنيات والبرمجيات المتطورة للحماية من التهديدات السيبرانية المتزايدة، بما يعزز من قدرة المشروع على اكتشاف والتعامل مع المخاطر بشكل فعال.
- من الضروري تطوير برامج تأهيل وتدريب مهنية بالتعاون مع الجامعات والمؤسسات التقنية لتخريج كوادر مؤهلة ومتخصصة قادرة على دعم وتعزيز الأمن السيبراني في المشاريع الناشئة.
- يُنصح الجهات الحكومية والقطاع الخاص بتوفير حوافز مالية أو دعم تقني للمشاريع الناشئة لتمكينها من تبني حلول أمنية فعالة دون أن يشكل ذلك عبئًا ماليًا يعيق نموها.
- يجب تصميم وتنفيذ سياسات أمنية مرنة وسهلة التطبيق بحيث لا تعيق سير العمل أو تسبب تعقيدًا مفرطًا، مع الحفاظ على المستوى المطلوب من الحماية.
- يتطلب الأمر جهودًا تواصلية مستمرة لبناء بيئة عمل تدعم التغيير وتعزز من قبول الموظفين للإجراءات الأمنية الجديدة، عبر حملات توعية وورش عمل تفاعلية.
- من المهم تعزيز الشراكات بين القطاع الحكومي والخاص والمؤسسات التعليمية لإنشاء منظومة متكاملة تدعم تطوير الأمن السيبراني، سواء من خلال تبادل المعرفة أو دعم البنية التحتية التقنية.

المراجع

- المراجع العربية:

- إبراهيم، ش. (2024). حصاد 2024.. السعودية تقود مستقبل الشركات الناشئة باستثمارات مليارية . Retrieved from <https://sharikatmubasher.com/media-hub/experts-thoughts/6273>
- dga. (2025). استراتيجيات التحول الرقمي في المملكة العربية السعودية-dga. Retrieved from <https://dga.gov.sa/ar/digital-knowledge/study-of-digital-transformation-strategy>
- dga. (2025). جاهزية تبني التقنيات الناشئة في الجهات الحكومية لعام 2025م-ET-adoption-readiness in-government-entities-2025. Retrieved from <https://dga.gov.sa/ar/ET-adoption-readiness-in-government-entities-2025>
- التجريبية وأدوات استشراف المستقبل. Retrieved from <https://my.gov.sa/ar/content/172>
- my. (2025). تبني التقنيات الناشئة. Retrieved from <https://my.gov.sa/ar/content/175>
- Nobrega, K. M. (2024). The whole of cyber defense: Syncing practice and theory. Retrieved from <https://www.sciencedirect.com/science/article/pii/S096386872400043X>
- pwc. (2025). الاستطلاع الثامن والعشرون لانطباعات الرؤساء التنفيذيين: نتائج المملكة العربية السعودية. Retrieved from <https://www.pwc.com/m1/en/ceo-survey/28th-ceo-survey-middle-east-findings-2025/saudi-arabia-findings-ar.html>

- المراجع الأجنبية:

- Adebajo, B. A. (2023). Introduction to Descriptive statistics. Retrieved from https://www.researchgate.net/publication/374981645_Introduction_to_Descriptive_statistics
- Alhakami, W. (2024). Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach. 29(2). Retrieved from https://openurl.ebsco.com/EPDB%3Aagd%3A9%3A4949817/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Aagd%3A178454206&crl=c&link_origin=scholar.google.com
- Alhalafi, N. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. 6(3). Retrieved from <https://www.mdpi.com/2624-6511/6/3/72>
- Alnasser, A. (2024). Navigating Digital Transformation in Alignment with Vision 2030: A Review of Organizational Strategies, Innovations, and Implications in Saudi Arabia. 3(2), 21-29. Retrieved from https://www.researchgate.net/publication/378544191_Navigating_Digital_Transformation_in_Alignment_with_Vision_2030_A_Review_of_Organizational_Strategies_Innovations_and_Implications_in_Saudi_Arabia
- Alshammari, T. S. (2020). An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia. Retrieved from https://www.researchgate.net/publication/342744584_An_Institutional_Theory_Perspective_on_Developing_a_Cyber_Security_Legal_Framework_A_Case_of_Saudi_Arabia

- Al-Somali. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *16*(5). Retrieved from <https://www.mdpi.com/2071-1050/16/5/1880>
- Al-Somali, S. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *16*(5). Retrieved from <https://www.mdpi.com/2071-1050/16/5/1880>
- Al-Zahrani, A. A. (2025). Success Factors in Achieving Excellence in Cybersecurity (A Case Study of the Kingdom of Saudi Arabia). Retrieved from <https://www.ijrsp.com/volume/issue-68/3/>
- Cao, G. (2019). The link between information processing capability and competitive advantage mediated through decision-making effectiveness. Retrieved from https://www.researchgate.net/publication/330799867_The_link_between_information_processing_capability_and_competitive_advantage_mediated_through_decision-making_effectiveness
- Chagadama, J. (2022). Cyberattacks: A Huge Concern for Small Business Sustainability. Retrieved from https://www.researchgate.net/publication/366621804_Cyberattacks_A_Huge_Concern_for_Small_Business_Sustainability
- Hlatshwayo, M. (2023). CYBERSECURITY IN THE DIGITAL SPACE. Retrieved from https://www.researchgate.net/publication/375115830_CYBERSECURITY_IN_THE_DIGITAL_SPACE
- Ismail, M. (2024). Cybersecurity activities for education and curriculum design: A survey. Retrieved from <https://www.sciencedirect.com/science/article/pii/S2451958824001349>
- Khalufi, N. A. (2025). Evaluating the Impact of Sustainability Practices on Customer Relationship Quality: An SEM-PLS Approach to Align with SDG. Retrieved from <https://www.mdpi.com/2071-1050/17/2/798>
- Madkhali, A. (2023). Exploring the Role of Information Technology in Supporting Sustainability Efforts in Saudi Arabia. *15*(16). Retrieved from <https://www.mdpi.com/2071-1050/15/16/12375>
- Maduwanthi, D. (2022). The Emergence of Technopreneurship for Sustainable and Ethical Economic Growth: Theory, Research and Practice. Retrieved from https://www.researchgate.net/publication/361464450_The_Emergence_of_Technopreneurship_for_Sustainable_and_Ethical_Economic_Growth_Theory_Research_and_Practice
- Marican, M. N. (2022). Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review. Retrieved from https://www.researchgate.net/publication/366336280_Cyber_Security_Maturity_Assessment_Framework_for_Technology_Startups_A_Systematic_Literature_Review
- Mian, T. S. (2023). Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector. Retrieved from <https://www.hnjournal.net/en/4-9-8/>
- my. (2025). البيانات التنظيمية

- Rawindaran, N. (2023). Enhancing Cyber Security Governance and Policy for SMEs in Industry 5.0: A Comparative Study between Saudi Arabia and the United Kingdom. 200-231. Retrieved from <https://www.mdpi.com/2673-6470/3/3/14>
- Reeves, A. (2021).
https://www.researchgate.net/publication/349987854_Encouraging_Employee_Engagement_With_Cybersecurity_How_to_Tackle_Cyber_Fatigue. Retrieved from
https://www.researchgate.net/publication/349987854_Encouraging_Employee_Engagement_With_Cybersecurity_How_to_Tackle_Cyber_Fatigue
- Renaud, K. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Retrieved from
https://www.researchgate.net/publication/353296672_A_cyber_situational_awareness_model_to_predict_the_implementation_of_cyber_security_controls_and_precautions_by_SMEs
- Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. 15(12). Retrieved from <https://www.mdpi.com/2071-1050/15/12/9426>
- Sagar, S. (2023). Innovation and Sustainability in Business: Navigating the Future Landscape. Retrieved from
https://www.researchgate.net/publication/377112499_Innovation_and_Sustainability_in_Business_Navigating_the_Future_Landscape
- Schorr, A. (2023). The Technology Acceptance Model (TAM) and its Importance for Digitalization Research: A Review. 55-65. Retrieved from
https://www.researchgate.net/publication/372301809_The_Technology_Acceptance_Model_TAM_and_its_Importance_for_Digitalization_Research_A_Review
- Stevens, S. (2020). A Framework for Ethical Cyber-Defence for Companies. Retrieved from
https://www.researchgate.net/publication/339162511_A_Framework_for_Ethical_Cyber-Defence_for_Companies
- Yellapu, V. (2018). Descriptive statistics. Retrieved from
https://www.researchgate.net/publication/327496870_Descriptive_statistics

الملاحق

الاستبانة

الإجابة					الأسئلة
1- الأسئلة العامة					
60+	50-60	40-50	30-40	20-30	العمر
			أنثى	ذكر	الجنس
دكتوراه	ماجستير	شهادة عليا	درجة البكالوريوس	شهادة الدراسة الثانوية	الدرجة العلمية
2- أسئلة الإستبيان					
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	لدى المشروع استراتيجية واضحة للأمن السيبراني.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	يتم تدريب الموظفين بانتظام على ممارسات الأمن السيبراني.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	يتم استخدام أدوات وبرمجيات متقدمة للحماية من التهديدات السيبرانية.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تبنى استراتيجية الأمن السيبراني مدعوم من الإدارة العليا.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	ساهمت استراتيجية الأمن السيبراني في حماية بيانات المشروع والعملاء.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	ساعدت الإجراءات الأمنية في تعزيز ثقة العملاء.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تبنى الأمن السيبراني أدى إلى تقليل حوادث الاختراق أو الأعطال التقنية.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تطبيق الأمن السيبراني ساهم في تحسين سمعة المشروع.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	الاستثمارات في الأمن السيبراني عززت تنافسية المشروع في السوق.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تكلفة تطبيق الأمن السيبراني تمثل عبئاً على المشروع.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	نقص الكفاءات المتخصصة في الأمن السيبراني يمثل تحدياً.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	صعوبة مواكبة التطورات السريعة في التهديدات السيبرانية.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	تعقيد الإجراءات الأمنية قد يبطئ سير العمل أحياناً.
أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة	هناك مقاومة من بعض الموظفين لتبني الإجراءات الأمنية الجديدة.

✓ https://docs.google.com/forms/d/1D_GmyHd7achvD5KSfTPFInyeXAO3BY1368THF0ZtE8U/edit

Abstract

This study aims to explore the impact of adopting cybersecurity strategies on the sustainability of technology startups in the Kingdom of Saudi Arabia, by analyzing the relationship between cybersecurity practices and the level of sustainability of these projects in an evolving competitive environment. The study followed a descriptive-analytical methodology, with data collected through questionnaires directed to a sample of 155 participants working in technology startups. The results showed that adopting clear security strategies supported by senior management, in addition to updating security policies, training employees, and using advanced software, contribute significantly to protecting data, enhancing customer confidence, and improving the projects' reputation. The study also highlighted challenges such as the cost of implementing cybersecurity and the lack of specialized competencies, which necessitate the adoption of supportive solutions that include training and appropriate funding. Key recommendations include strengthening the role of senior management in supporting cybersecurity, developing ongoing training programs, streamlining security procedures to ensure business flexibility, and encouraging collaboration between government agencies and the private sector.

Keywords: cybersecurity, technology startups, project sustainability, security training, advanced software, specialized competencies, Saudi Arabia.

Midocean University
College of Management
Master's degree in Entrepreneurship



The Impact of Adopting Cybersecurity Strategies on the Sustainability of Tech Startups in the Kingdom of Saudi Arabia

Prepared by/

Yasser Hassan Al-Safadi

University ID/

243000055

Supervised by/

Ahmed Rajih

Year

2025