– جامعة قاصدي مرباح –ورقلة–
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم المناجمنت

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني
في ميدان: العلوم الاقتصادية والتسيير والعلوم التجارية
فرع علوم التسيير، تخصص إدارة أعمال وإمداد

بعنوان:

أثر الأمن السيبراني على تحسين أداء سلاسل التوريد

دراسة حالة عينة من المؤسسات الجزائرية

من إعداد الطالبتان:

- خولة خراز
- سارة كانوري

نوقشت و أجيزت بتاريخ: **2026/05/17**

أمام اللجنة المكونة من السادة:

أ. الطاهر بن عمارة.....(أستاذ محاضر "ب"، جامعة قاصدي مرباح ورقلة) رئيسا
أ. نهلة قادري .....(أستاذ محاضر"أ"، جامعة قاصدي مرباح ورقلة) مشرفا ومقررا
أ. مريم بلطرش.....(أستاذ محاضر"أ"، جامعة قاصدي مرباح ورقلة) مناقشا

السنة الجامعية: **2026/2025**

– جامعة قاصدي مرباح –ورقلة–
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم المناجمنت

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر مهني
في ميدان: العلوم الاقتصادية والتسيير والعلوم التجارية
فرع علوم التسيير، تخصص إدارة أعمال وإمداد

بعنوان:

أثر الأمن السيبراني على تحسين أداء سلاسل التوريد

دراسة حالة عينة من المؤسسات الجزائرية

من إعداد الطالبتان:

- خولة خراز
- سارة كانوري

نوقشت و أجيزت بتاريخ: **2026/05/17**

أمام اللجنة المكونة من السادة:

أ. الطاهر بن عمارة.....(أستاذ محاضر "ب"، جامعة قاصدي مرباح ورقلة) رئيسا
أ. نهلة قادري .....(أستاذ محاضر"أ"، جامعة قاصدي مرباح ورقلة) مشرفا ومقررا
أ. مريم بلطرش.....(أستاذ محاضر"أ"، جامعة قاصدي مرباح ورقلة) مناقشا

السنة الجامعية: **2026/2025**



اهداء

الحمد لله الذي أنار بصيرتي، ومنحني القوة لأتم هذا المسير.. حمداً يليق بجلال وجهه وعظيم سلطانه. واعترافاً بالفضل لأهله، وتقديراً لكل من شق لي طريقاً نحو النور، أضع بين أيديكم ثمرة غرسي

إلى من غمرتني بحبها ودعواتها الصادقة، أمي الغالية "فاطمة خيراني.."

إلى منبع الفخر ومن مهد لي طريق العلم بصبره، أبي العزيز "قدور خراز .."

إلى سندي وذخري في هذه الحياة، إخوتي الثلاثة وأختاي، وإلى عصافير بيتنا أبناء أختي الثلاثة..

إلى أحبائي وعائلتاي، وكل من كان لي عوناً وسنداً بكلمة أو دعاء طوال هذه الرحلة..

وإلى رفيقة الكفاح وشريكتي في هذا البحث "سارة.."

أهديكم جميعاً هذا النجاح، فبكم ومعكم يكتمل الفخر.

خولة



اهداء

إلى الذين جعلوا من المحال ممكناً، ومن التعب راحة، ومن الحلم واقعاً..

إلى القلوب التي نبضت معي في كل سطر من سطور هذا البحث..

إليكم، يا من تستحقون من الشكر أجزله، ومن الحب أصدقه، أهدي هذا النجاح".

بكل حب وفخر، أهدي ثمرة تخرجي إلى:

والديّ العزيزين: "فاطمة الزهراء بن ناصر" و"لحسن كانوري."

أختاي وإخوتي .. أنتم السند والضياء.

شريكة النجاح ورفيقة البحث "خولة".. تقديراً لجهودنا المشتركة.

كل من كان له أثر جميل في رحلتي الدراسية.

سارة

شكر وعرفان

قال تعالى: "رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ"

الحمد لله أولاً على جزيل فضله ونعمه، إنه ولي ذلك والقادر عليه.
قال رسول الله صلى الله عليه وسلم: "من اصطنع إليكم معروفاً فجازوه، فإن عجزتم عن مجازاته فادعوا له حتى تعلموا أنكم شكرتم، فإن الله يحب الشاكرين."

بعد رحلة بحث وجهد، يطيب لي أن أتقدم بجزيل الشكر وعظيم الامتنان إلى الأستاذة المشرفة: **قادري نهلة**، على ما قدمته لي من نصائح قيمة، وإرشادات سديدة، وتوجيهات طيلة فترة إنجاز هذا العمل، فكانت خير مرشد ومعين.

كما أتقدم بالشكر والتقدير إلى الأساتذة الكرام: **اميناش ليندة** و **بن عمارة الطاهر**، على مساهمتهم القيمة ودعمهم العلمي.

ويمتد شكري وتقديري إلى كافة مسؤولي وموظفي المؤسسات محل الدراسة، الذين فتحوا لنا الأبواب وسهلوا لنا مهام البحث، وساهموا بتعاونهم في إثراء الجانب التطبيقي لهذه المذكرة.

وأخيراً، أتوجه بالشكر إلى كل من كان له أثر في إتمام هذا المسار الدراسي، سائلة الله عز وجل أن يوفق الجميع لما يحب ويرضى.

ملخص:

تهدف الدراسة الى تحليل مدى تأثير الأمن السيبراني على تحسين أداء سلاسل التوريد في المؤسسات محل الدراسة، ولقد قمنا بدراسة ميدانية لعينة من المؤسسات الجزائرية، ولتحقيق هدف الدراسة اعتمدنا على المنهج الوصفي والتحليلي وأسلوب دراسة الحالة، حيث تم اعتماد الاستبيان كأداة رئيسية لجمع البيانات، وكانت الدراسة على عينة عشوائية متمثلة في100 موظفا، وتم استخدام عدد من الأساليب الإحصائية ومعالجتها ببرنامج SPSS.

وقد توصلت الدراسة إلى وجود أثر معنوي للأمن السيبراني ككل على تحسين أداء سلاسل التوريد، كما تبين أن البعدين التنظيمي والبشري لهما أثر دال إحصائياً، في حين لم يظهر أثر معنوي مستقل لكل من البعد التقني والبعد التعاوني ضمن نموذج الانحدار المتعدد.

الكلمات المفتاحية: أمن سيبراني، سلاسل توريد، بيئة رقمية، كفاءة تشغيلية، سياسات أمنية، أنظمة استباقية.

Abstract:

The study aims to analyze the extent to which cybersecurity contributes to improving supply chain performance in the institutions under study. A field study was conducted on a sample of Algerian institutions. To achieve the objective of the study, the descriptive and analytical approach, as well as the case study method, were adopted. The questionnaire was used as the main tool for data collection. The study was conducted on a random sample of 100 employees, and several statistical methods were used, with the data processed using SPSS.

The study found that cybersecurity, as a whole, has a significant effect on improving supply chain performance. It also showed that the organizational and human dimensions have a statistically significant effect, while no independent significant effect was found for the technical and collaborative dimensions within the multiple regression model.

Keywords: Cybersecurity, supply chains, digital environment, operational efficiency, security policies, proactive systems

فهرس المحتويات

اهداء II
اهداء III
شكر وعرفان IV
ملخص V
فهرس المحتويات VI
قائمة الأشكال VIII
قائمة الجداول IX
قائمة الرموز و الاختصارات X
قائمة الملاحق VI
مقدمة I
الفصل الأول:الأدبيات النظرية والتطبيقية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد 6
تمهيد 7
المبحث الأول: الأدبيات النظرية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد 8
تمهيد 8
المطلب الأول: الإطار النظري للأمن السيبراني 8
الفرع الأول: تعريف الأمن السيبراني 8
الفرع الثاني: أهمية الأمن السيبراني 9
الفرع الثالث: خصائص الأمن السيبراني 9
الفرع الرابع: أبعاد الأمن السيبراني في سلاسل التوريد 10
المطلب الثاني: الإطار النظري لسلاسل التوريد 19
الفرع الأول: تعريف سلسلة التوريد 19
الفرع الثاني: أهمية سلاسل التوريد 19
الفرع الثالث: نشأة سلاسل التوريد 20
الفرع الرابع: أبعاد سلاسل التوريد من منظور الأمن السيبراني 21
المبحث الثاني: الأدبيات التطبيقية لأثر الأمن السيبراني على كفاءة سلاسل التوريد 24
المطلب الأول: الدراسات السابقة 24
الفرع الأول: مقارنة بين الدراسات الحالية والدراسات السابقة 35

خلاصة الفصل 37
الفصل الثاني:الجانب التطبيقي..... 38
تمهيد..... 39
المبحث الأول: الطريقة والأدوات 40
المطلب الأول: مجتمع وعينة الدراسة..... 40
الفرع الأول: مجتمع الدراسة 40
الفرع الثاني: منهج الدراسة ومصادر جمع البيانات..... 42
المطلب الثاني: أدوات الدراسة..... 43
الفرع الأول: أدوات جمع البيانات 43
الفرع الثاني: الأدوات الإحصائية..... 44
الفرع الثالث: صدق وثبات الاستبيان 45
المبحث الثاني: نتائج الدراسة ومناقشتها 47
المطلب الأول: عرض نتائج الدراسة..... 47
الفرع الأول: الدراسة الإحصائية للمتغيرات الشخصية..... 47
الفرع الثاني: اختبار التوزع الطبيعي للعينة 53
الفرع الثالث: تحليل وتفسير قياس أثر الأمن السيبراني على تحسين أداء سلاسل التوريد 54
الفرع الرابع: دراسة أثر الأمن السيبراني على تحسين أداء سلاسل التوريد في المؤسسات عينة الدراسة 62
المطلب الثاني: مناقشة نتائج الدراسة ومقارنتها مع نتائج الدراسات السابقة 70
الفرع الأول: مناقشة نتائج تبني استراتيجيات الأمن السيبراني 70
الفرع الثاني: مناقشة نتائج الإطار النظري لسلاسل التوريد 71
خلاصة الفصل 73
الخاتمة..... 74
قائمة المراجع 80
الملاحق 84

قائمة الأشكال

الشكل رقم (1): نموذج الدراسة ..... ه
الشكل رقم (2): توزيع الموظفين حسب السن 47
الشكل رقم (3): توزيع الموظفين حسب المستوى التعليمي 48
الشكل رقم (4): توزيع الموظفين حسب سنوات الأقدمية 49
الشكل رقم (5): توزيع الموظفين حسب القسم 50
الشكل رقم (6): توزيع الموظفين حسب حجم المؤسسة..... 51
الشكل رقم (7): توزيع الموظفين حسب نوع المؤسسة 52
الشكل رقم (8): المدرجات التكرارية لقياس اعتدالية البيانات 54

قائمة الجداول

جدول رقم (1): خطوات الممارسات التعاونية مع توضيح كيفية تطبيقها وضمان فعاليتها 11
جدول رقم (2): أهم سياسات وأساليب الأمن السيبراني لتعزيز حماية سلاسل التوريد 12
جدول رقم (3): التقنيات الحديثة الداعمة لتعزيز أمن سلاسل التوريد 13
جدول رقم (4): احصائيات الاستبيانات الموزعة والصالحة 42
جدول رقم (**5**): يوضح متغيرات الدراسة 42
جدول رقم (6): درجات مقياس ليكارت في الاستبيان 44
جدول رقم (7): مجال المتوسط الحسابي المرجح لكل مستوى مقياس (ليكارت) 45
جدول رقم (8): نتائج ألفا كرونباخ 45
جدول رقم (9): توزيع الموظفين حسب السن 47
جدول رقم (10): توزيع الموظفين حسب المستوى التعليمي 48
جدول رقم (11): توزيع الموظفين حسب سنوات الأقدمية 49
جدول رقم (12): توزيع الموظفين حسب القسم 50
جدول رقم (13): توزيع الموظفين حسب حجم المؤسسة 51
جدول رقم (14): توزيع الموظفين حسب نوع المؤسسة 52
جدول رقم (15): نتائج اختبار Shapiro-Wilk 53
جدول رقم (16): متوسط إجابات الموظفين حول التنظيم 54
جدول رقم (17): متوسط إجابات الموظفين حول البعد التقني 55
جدول رقم (18): متوسط إجابات الموظفين حول البعد البشري 56
جدول رقم (19): متوسط إجابات الموظفين حول البعد التعاوني 57
جدول رقم (20): متوسط إجابات الموظفين حول بعد الكفاءة التشغيلية 58
جدول رقم (21): متوسط إجابات الموظفين حول بعد جودة الخدمة وخدمة العملاء 60
جدول رقم (22): متوسط إجابات الموظفين حول بعد الاستمرارية والمرونة 61
جدول رقم (23): العلاقة بين الأمن السيبراني وسلاسل التوريد 62
جدول رقم (24): العلاقة الارتباطية بين البعد التنظيمي وأداء سلسلة التوريد 62
جدول رقم (25): العلاقة الارتباطية بين البعد التقني وأداء سلسلة التوريد 63
جدول رقم (26): العلاقة الارتباطية بين البعد البشري وأداء سلسلة التوريد 63
جدول رقم (27): العلاقة الارتباطية بين البعد التعاوني وأداء سلسلة التوريد 64
جدول رقم (28): نتائج ملخص النموذج (**Model Summary**) 64
جدول رقم (29): نتائج ANOVA للانحدار الخطي 65
جدول رقم (30): نتائج معاملات الانحدار الخطي **Coefficients** 65
جدول رقم (31): نتائج الانحدار الخطي المتعدد 66

قائمة الرموز و الاختصارات

الرمز	الدلالة
SPSS	الحزمة الإحصائية للعلوم الاجتماعية (برنامج تحليل احصائي)
DDoS	هجمات حجب الخدمة الموزعة
NIST	المعهد الوطني للمعايير والتكنولوجيا
IoT	انترنت الأشياء
SCCRM	إدارة مخاطر سلسلة التوريد السيبرانية
AI	الذكاء الاصطناعي

قائمة الملاحق

الرقم	عنوان الملحق	الصفحة
1	الاستبيان	85
2	قائمة الأساتذة المحكمين	89
3	مخرجات SPSS	90

مقدمة

أ. توطئة

يشهد العالم تحولات رقمية متسارعة تعد من أهم التغيرات التي أثرت على كل من القطاعات الإقتصادية والخدماتية، حيث أوجبت هذه التحولات واقع قائم على الرقمنة الكاملة، وفي هذه البيئة الرقمية باتت سلسلة التوريد كركيزة أساسية يمتد دورها من نقل البضائع المادية إلى أن أصبحت سلسلة توريد معقدة تعتمد على التدفقات المعلوماتية والبيانات الهائلة التي تربط بين المؤسسة وشركائها في بيئة رقمية مفتوحة، وإن هذا الانتقال نحو رقمنة سلاسل التوريد جعل المؤسسات تطمح إلى إنتاجية أعلى بالوصول إلى أعلى مستويات الجودة والفعالية، لكن في جهة أخرى وضع المؤسسات في ظل تحديات أمنية غير معتادة، بحيث تستوجب إعادة النظر في تقنيات وإستراتيجيات الحماية التقنية.

إن أصل الاشكالية اليوم يتمثل في أن كفاءة سلسلة التوريد لم تعد بالتوصيل في الوقت المناسب والتكلفة المناسبة فقط بل أضحت مرتبطة بمدى صمود النظام السيبراني أمام الهجمات والتهديدات الرقمية المتزايدة وهو مايضمن مرونة سلسلة التوريد ويؤمن إستمراريتها، وعليه أصبح الأمن السيبراني الركيزة الأساسية لضمان استدامة سلسلة التوريد، بحيث تساهم وسائل ضمان سرية البيانات الحساسة دور فعال في الحماية وهذا يعد ميزة تنافسية، ومنه يعزز الثقة بين مكونات سلسلة التوريد، لأن في بيئة تتميز بدرجة عالية من التنافسية يعد فقدان القدرة على التحكم في المعلومات تهديد مباشر لهوية المؤسسة وموقعها في السوق .

إن صحة وسلامة التدفق المعلوماتي داخل سلسلة التوريد هو الأساس في الحد من الأخطاء اللوجيستية وسيرها بكل مرونة، إذ أن أي خلل في البيانات عن قصد أو دون قصد أو تلاعب يؤدي إلى إعاقة عملية التنبؤ سواء من ناحية التهديدات أو توقع الطلب والمخزون وهذا ما يعكس بالسلب على الكفاءة التشغيلية، ومن خلال هذا الإتجاه يتضح أن وجود الأنظمة الرقمية يمثل ضمان حتمي لحماية سلاسل التوريد من الإنقطاعات غير المتوقعة، إذ أن الهجمات السيبرانية تتسبب توقف في حركة تدفق المنتجات ماينتج عنه خسائر مالية تهدد استمرار جميع العمليات السيبرانية .

إذ تتميز البيئة الرقمية بالتعقيد وهذا ما يلزم المؤسسات الكبرى نحو دمج تقنيات الذكاء الإصطناعي والاعتماد على الأنظمة الإستباقية لتطوير عمليات التنبؤ بالهجمات قبل وقوعها الفعلي، وبإستخدام هذه التقنيات المتطورة تعزز الشفافية داخل السلسلة بالإضافة إلى تتبع الشحنات بدرجة عالية وهو ما يقلص وقت التشافي من الهجمات الرقمية، وذلك يمنح السلسلة المرونة في المواجهة للأزمات المفاجئة، فالتكامل بين الأمن الرقمي والتكنولوجيا يعكس قوة الأداء الفعال.

وفي ظل التغيرات العالمية المتسارعة تظهر ضرورة فحص الواقع المحلي للمؤسسات الإقتصادية الجزائرية سواء العمومية أو الخاصة أو الأجنبية، إذ أنها تواجه إلزامية الإندماج في التحول الرقمي وضرورة تأمين سلامة سلاسل التوريد السيبرانية، وتاتي هذه الدراسة لإحكام الإطار المفاهيمي للأمن السيبراني وأثر على كفاءة وفعالية سلاسل التوريد.

ب. طرح الإشكالية:

ما مدى تأثير الأمن السيبراني على تحسين أداء سلاسل التوريد في المؤسسات عينة الدراسة؟

بناء على الإشكالية الرئيسية المطروحة ومن أجل الإلمام بالموضوع يمكن صياغة الإشكاليات الفرعية كالتالي:

- ✓ ما أثر البنية والسياسات الأمنية على أداء سلسلة التوريد في المؤسسات محل الدراسة؟
- ✓ ما أثر التكنولوجيا والحماية الرقمية على أداء سلسلة التوريد في المؤسسات محل الدراسة؟
- ✓ ما أثر الوعي الأمني لدى الموظفين على أداء سلسلة التوريد في المؤسسات محل الدراسة؟
- ✓ ما أثر البعد التعاوني في الأمن السيبراني على أداء سلسلة التوريد في المؤسسات محل الدراسة؟

ج. الفرضيات

وللإجابة على الإشكالية الرئيسية يمكن صياغة الفرضيات التالية والتي تعتبر إجابة مبدئية للأسئلة الفرعية وهي على النحو التالي:

- ✓ يوجد أثر ذو دلالة إحصائية للبنية والسياسات الأمنية على أداء سلسلة التوريد.
- ✓ يوجد أثر ذو دلالة إحصائية للتكنولوجيا والحماية الرقمية على أداء سلسلة التوريد.
- ✓ يوجد أثر ذو دلالة إحصائية للوعي الأمني لدى الموظفين على أداء سلسلة التوريد.
- ✓ يوجد أثر ذو دلالة إحصائية للبعد التعاوني في الأمن السيبراني على أداء سلسلة التوريد

د. أهمية الدراسة:

تعد هذه الدراسة إضافة لمكتبة الأكاديمية من خلال دراسة أثر الأمن السيبراني بفعالية سلسلة التوريد، إذ هو مجال يحتاج إلى المزيد من التقصي في البيئة المحلية، بحيث تبرز قيمتها التطبيقية في مساهمتها للمؤسسات محل الدراسة رؤية استراتيجية حول كيفية تحويل الأمن السيبراني من تكلفة إلى محرك للأداء وميزة تنافسية، بحيث تساعد صناع القرار في المؤسسات على فهم طبيعة المخاطر الرقمية التي قد تؤدي إلى توقف التدفقات المادية، مما يساهم في تصميم استراتيجيات دفاعية استباقية.

ه. أهداف الدراسة:

وتتمثل في:

- ضبط الإطار المفاهيمي لكل من الأمن السيبراني مع إبراز كل من أهميته وخصائصه.
- التعرف على واقع استخدام الأمن السيبراني في المؤسسات محل الدراسة وتحديد مواطن الضعف التي قد تؤثر على عملياتها اللوجستية.
- قياس مدى تأثير تطبيق الأمن السيبراني على تحسين مؤشرات الأداء اللوجستي.
- محاولة رصد مدى استجابة المؤسسات محل الدراسة للتطور في مجال الأمن السيبراني.

و. مبررات اختيار موضوع الدراسة:

هناك جملة من الأسباب التي دفعت بنا إلى اختيار هذا الموضوع نذكر ما يلي:

- الرغبة في تعميق المعرفة في مجال إدارة الأعمال وإمداد من منظور تقني معاصر يواكب التطورات.
- ندرة الدراسات العربية التي تربط بين تكنولوجيا الأمن السيبراني وكفاءة الأداء التشغيلي لسلاسل التوريد.
- التوجه المتسارع للمؤسسات نحو رقمنة سلاسل التوريد، مما جعلها عرضة لمخاطر سيبرانية تهدد استمراريتها.
- المساهمة في تقديم نموذج عملي يساعد المؤسسات الاقتصادية على مواجهة التهديدات الرقمية وضمان تدفق السلع والخدمات بكفاءة.

ز. حدود الدراسة:

من أجل معالجة البحث تم تحديد الحدود في:

- **الحدود الموضوعية:**

تقتصر هذه الدراسة على تحليل أثر الأمن السيبراني بأبعاده (البعد التنظيمي، التقني، البشري، والتعاوني.) في تحسين كفاءة وفعالية سلاسل التوريد (التخطيط، إدارة المخزون، استمرارية التدفقات، والشفافية).

- **الحدود المكانية:**

تُطبق هذه الدراسة ميدانياً على مستوى المؤسسات محل الدراسة، والتي تم اختيارها لكونها تعتمد على أنظمة معلوماتية متكاملة في إدارة سلاسل التوريدها.

- **الحدود الزمانية:**

تغطي هذه الدراسة الفترة الزمنية الممتدة خلال الموسم الجامعي 2026/2025، وهي الفترة التي تم فيها جمع البيانات الأولية وتطبيق الاستبيان.

- **الحدود البشرية:**

تتمثل في عينة من الموظفين والإطارات العاملة في قسم المناجمنت، قسم التوريد، وقسم نظم المعلومات في المؤسسة، نظراً لاطلاعهم المباشر على العمليات اللوجستية والأنظمة الرقمية.

ح. منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي والتحليلي باعتباره يقدم ويصف جميع المعلومات للمستخدمة في البحث ويحللها ويفسرها لإفادة القارئ وإثراء رصيده المعرفي، إضافة إلى ذلك أسلوب دراسة الحالة في عرض المؤسسات محل الدراسة بالإضافة إلى منهج علاقات الارتباط في دراسة العلاقة بين المتغيرات، أما أدوات جمع البيانات تمثلت في الاستبيان؛ وسيتم الاعتماد على البرنامج الإحصائي SPSS في معالجة البيانات واعتمدنا على منهجية IMRAD في تنسيق الدراسة ككل.

ط. مرجعية الدراسة:

- المقالات.
- الكتب.
- الدراسات السابقة المتمثلة في الدكتوراه والمقالات.
- المواقع الإلكترونية.

ي. هيكل الدراسة:

بغرض تحقيق أهداف الدراسة وجب تقسيمها إلى فصلين، فصل نظري وآخر تطبيقي، بالإضافة إلى المقدمة والخاتمة، لذا تمثل هيكل الدراسة كما يلي:

الفصل الأول يختص بدراسة الإطار المفاهيمي المتغيرات الدراسة، وهو بدوره قسم إلى مبحثين الأول يختص بدراسة الأدبيات النظرية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد من مفاهيم وأهمية وأبعاد إضافة الى مفهوم سلاسل التوريد وأهميتها ونشأتها أبعادها أما المبحث الثاني فقد خصص العرض ومناقشة بعض الدراسات السابقة حسب تصنيف الأجنبي باللغة العربية اللغة الأجنبية وتحديد ما جاء فيها

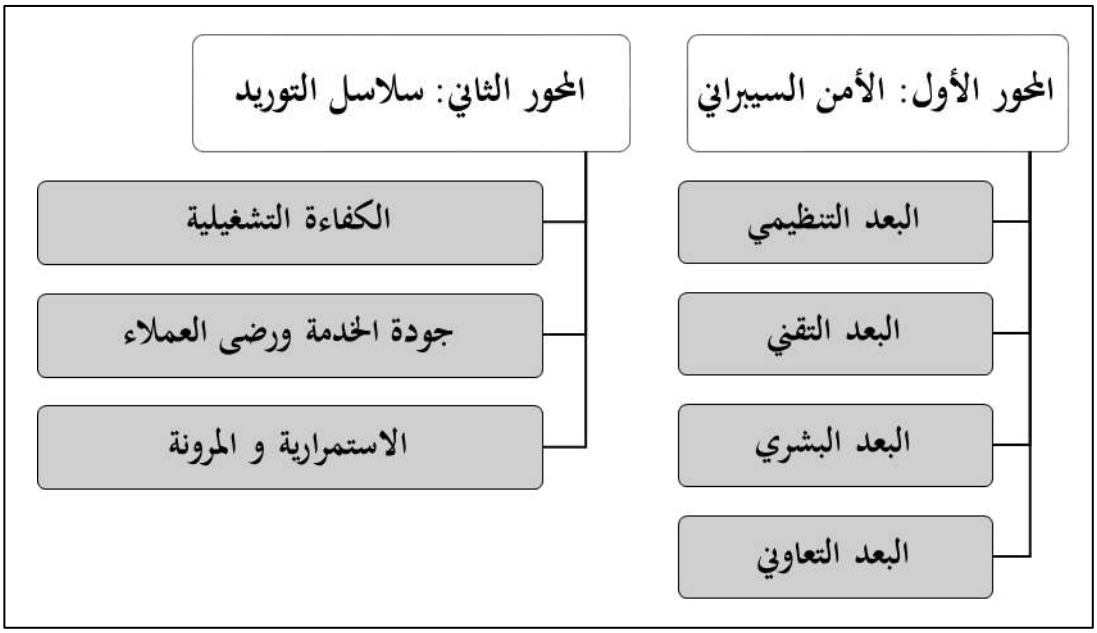
باختصار من أهداف ونتائج، إضافة إلى مقارنة الدراسة الحالية مع من سبقها من دراسات في نفس التوجه، أما الفصل الثاني تطرقنا فيه إلى الدراسة الميدانية للمؤسسات محل الدراسة من خلال مبحثين أيضا، بدءا بعينة وأدوات الدراسة في المبحث الأول، أما المبحث الثاني فيتعلق بعرض نتائج الدراسة ومناقشتها بنتائج الدراسات السابقة من أجل الإلمام بواقع موضوع الدراسة وحيثياته، وإلى آخر الدراسة تم عرض أهم النتائج المتوصل إليها، بالإضافة إلى جملة من التوصيات والاقتراحات.

ك. صعوبات البحث:

- ✓ قلة المراجع الميدانية العربية التي تربط بين الأمن السيبراني وسلاسل التوريد بشكل مباشر، مما استلزم الاعتماد على مراجع أجنبية حديثة.
- ✓ تحفظ بعض أفراد العينة في المؤسسة محل الدراسة عن تقديم تفاصيل دقيقة حول الاختراقات أو الثغرات الأمنية لدواعٍ أمنية وتنافسية.
- ✓ محاولة التوفيق بين الجانب النظري المعمق والجانب التطبيقي الميداني في فترة زمنية محددة.
- ✓ صعوبة إعداد الاستبيان وتحديد محاوره وعباراته نظرا لحداثة الموضوع.

ل. نموذج الدراسة:

الشكل رقم (1): نموذج الدراسة



المصدر: من إعداد الطالبتين بناء على الدراسات السابقة.

الفصل الأول

الأدبيات النظرية والتطبيقية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد

تمهيد:

نعيش الأن في عصر الثورة التقنية المتسارعة بحيث تغيرت المفاهيم الاقتصادية التقليدية وأغدت سلسلة التوريد هي العصب الرئيسي لدوام المؤسسات في إطار سوق عالمية تمتاز بالتنافسية الفائقة، بحيث أصبح توجه المؤسسات نحو الرقمنة الشاملة لجميع العمليات اللوجستية ضرورة حتمية، لأن سلاسل التوريد لم تعد كما كانت تدفقات مادية فقط للسلع، بل أضحت شبكات معقدة من البيانات التي تتطلب إدارة متقنة لضمان كفاءتها.

وهذا الاعتماد المتصاعد على التكنولوجيا يفتح أفاق جديدة من المخاطر والتهديدات، مما يؤهل الأمن السيبراني الدرع الأساسي في تطبيق استراتيجيات التوريد الحديثة، فالحفاظ على أمن البيانات امتد ليضم بناء بنية وسياسات أمنية متينة، وتطبيق تكنولوجيا حماية رقمية مبتكرة، علاوة على ذلك دمج وتفعيل البعد التعاوني بين جميع أجزاء سلسلة التوريد للتصدي للتهديدات السيبرانية التي قد تهز ثبات المؤسسة وتعيق تدفقاتها المعلوماتية والمادية.

إن نواة هذه العلاقة يتمثل في مدى انعكاس التحصين السيبراني على أداء وكفاءة سلاسل التوريد، والحفاظ على أمن وسلامة المعلومات والأنظمة الرقيمة هما الأساس لتحقيق الكفاءة التشغيلية لضمان استمرارية سلسلة التوريد أمام الهجمات، وبدور هذا التكامل هو ما يترتب عنه جودة عالية في الخدمات ومنه رضا العملاء.

ومنه، سنقوم في هذا الفصل على الإلمام بمختلف الجوانب النظرية والتطبيقية لهذه الدراسة وذلك من خلال تقسيم الفصل إلى مبحثين:

المبحث الأول: الأدبيات النظرية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد.

المبحث الثاني: الأدبيات التطبيقية لأثر الأمن السيبراني على سلاسل التوريد.

المبحث الأول: الأدبيات النظرية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد

تمهيد

أحرز الأمن السيبراني اهتماما واسع في خضم التطور الرقمي المتسارع، بسبب ما له من أثر مباشر على استقرار جميع تدفقات سلسلة التوريد، وباعتبار أن أمن البيانات هي العامل الأساسي لتحقيق كفاءة الأداء اللوجيستي، ومنه سنتناول في هذا المبحث مفاهيم الأمن السيبراني وأهميته، بالإضافة إلى تفصيل أبعاده المحورية (البنيوية، التعاونية، التقنية) التي تمثل الاستراتيجيات التي تعد حصن سلسلة التوريد الرقمية.

المطلب الأول: الإطار النظري للأمن السيبراني

يعتبر الأمن السيبراني الدعامة الأساسية لحماية الأصول المعلوماتية وتأمين سلامة الأنظمة الرقمية في سلسلة التوريد، بحيث يقتضي لفهمه المعرفة الشاملة لنشأته وأهميته في التصدي للهجمات والتهديدات الرقمية. وبناء على ذلك، سنحرص في هذا المطلب إلى ضبط مفاهيم الأمن السيبراني، والعناصر الأساسية التي تساهم في وقاية سلسلة التوريد من الهجمات.

الفرع الأول: تعريف الأمن السيبراني

هناك الكثير من التعريفات والتي ذكرها المؤلفين عن الأمن السيبراني ومن بين هذه التعريفات ما يلي:

عرف على أنه " عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، والمستهلكين في الفضاء السيبراني. (الطالب، 2026)

يشكل الأمن السيبراني جزء أساسيا من أي سياسة أمنية وطنية فقد أصبحت الدول تصنف مسائل الدفاع السيبراني كأولوية في سياساتها الدفاعية كما خصصت أكثر من 130 دولة أقساما خاصة بالأمن السيبراني في فرقها الأمنية الوطنية، ويقصد بالأمن السيبراني مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية التي تهدف إلى حماية الفضاء السيبراني الوطني كما تركز على حماية بيانات الأفراد ومؤسسات الدولة من الاستخدام غير المصرح به أو أي أذى يلحق بشبكة. (عسيري، 2026)

وعرفه أيضا المشرع الأردني من خلال قانون الأمن السيبراني الأردني بكونه" مجموعة من الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبرانية والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الاجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك (المادة الثانية من قانون الأمن السيبراني الأردني)

ويعني مجموع الإجراءات الواجب اتخاذها من قبل الأجهزة الأمنية أو الأخرى غيرها ذات العلاقة، للمحافظة على سرية المعلومات الإلكترونية، ومنع الاختراقات الفيروسية من أجل ضمان وصول المعلومات

الحاسوبية إلى الجهات المختصة في الوقت المناسب، وضمان عدم وقوعها في أيدي الأعداء أو الأصدقاء على حد سواء خصوصا بعد الثورة الهائلة في عالم الاتصالات و التداولات الإلكترونية، حيث شكل هذا النوع من الأمن هاجسا استراتيجيا للقوى العالمية و المتمثلة في الولايات الأمريكية المتحدة و الصين وروسيا، إذ تدور في وقتنا الحالي حرب إلكترونية بين هذه القوى من أجل اختراق المعلومات و التأثير على أسعار البورصة و العملات وغيرها من المنشآت. (الشمري، 2021)

بناء على الزخم المعرفي الذي تم عرضه من خلال التعريفات السابقة للأمن السيبراني، ومنه نقدم تعريفا إجرائيا تلخيصا لما سبق:

هي باقة متكاملة من الإجراءات التقنية (مثل أنظمة التشفير) بالإضافة إلى الإجراءات التنظيمية (مثل سياسات الاستخدام) التي تساعد على تحصين البنية التحتية للبيانات والحيز الرقمي من أي اختراق أو وصول غير مصرح به، والحفاظ على سرية البيانات وتوفرها الآمن بشكل مستمر، مما يؤدي إلى انخفاض المخاطر الرقمية والحفاظ على استمرارية العمل بأمان.

الفرع الثاني: أهمية الأمن السيبراني:

تتجلى أهمية الأمن السيبراني في مجموعة من النقاط التالية: (أحمد و علي، 2022)

- قدرته على مقاومة التهديدات المعتمدة وغير المعتمدة والاستجابة.
- التخلص من الأضرار الناجمة عن تعطيل أو اتلاف تكنولوجيا المعلومات والاتصالات أو بسبب إساءة استخدامها.
- تم اعتماده من طرف العديد من الدول على قمة أولوياتها وخصيصا بعد الحروب الالكترونية.
- يعد الأمن السيبراني إشارة صريحة إلى نهاية عصر الحروب التقليدية التي تعتمد على الأسلحة الثقيلة، والإعلان عن بداية عهد جديد من الحروب الالكترونية.

الفرع الثالث: خصائص الأمن السيبراني

يتميز الأمن السيبراني بمجموعة من الخصائص حسب ما قدمته الهيئة الوطنية للأمن السيبراني (أحمد و علي، 2022) وهي كالتالي:

- **تأمين الوصول المنطقي:** عبر حماية الأصول التقنية والمعلوماتية لمؤسسة، وردع الوصول غير المصرح عن طريق تقييد صلاحية الدخول تماشيا مع ما يستلزم مصلحة العمل.
- **تحصين البنية التحتية والأنظمة:** تشمل الإمكانية على تأمين أجهزة معالجة البيانات، أجهزة المستخدمين، إلى جانب حماية البريد الإلكتروني من الهجمات السيبرانية.

- **إدارة أمن الشبكة:** إمداد بيئة اتصالات آمنة يشمل سلامة تدفق المعلومات وصد محاولة اختراق شبكات المؤسسة.
- **ضمان أمن الأجهزة الذكية:** من حماية الحواسيب، اللوائح الذكية، وحتى الهواتف، مع ضمانة التخزين والنقل الآمن للمعلومات الحساسة، خاصة عند استعمال الجهاز الشخصي لصالح العمل.
- **بلوغ المبادئ الأمنية:** وتتمثل في ضمان سلامة البيانات والحفاظ على السرية، وتوافرها الدائم حسب السياسات التنظيمية المعتمدة.

الفرع الرابع: أبعاد الأمن السيبراني في سلاسل التوريد

يتعدى الأمن السيبراني في سلسلة التوريد على الجانب التقني البحت، بل يمتد ليضم منظومة متكاملة من الأبعاد لتضم الجانب التقني والتنظيمي بين الشركاء، وسنسعى في الآتي لإلقاء الضوء على أبعاده الجوهرية المعتمدة في هذا البحث التي تتشمل في: البنية والسياسات الأمنية، التكنولوجيا والحماية الرقمية، البعد التعاوني.

1. **البنية والسياسات الأمنية (البعد التنظيمي):** تُعدّ البنية والسياسات الأمنية حجر الزاوية في بناء أي نظام إلكتروني يهدف إلى حماية الأصول والأنظمة الرقمية داخل المؤسسات، حيث لا يمكن تحقيق أداء فعّال دون وجود إطار تنظيمي واضح وقوانين تحكم هذا المجال. (Wallis & Dorey, 2024)

و لم يعد الأمن السيبراني خياراً ثانوياً، بل أصبح ضرورة حتمية في ظل التحول الرقمي المتسارع، فقد أظهرت دراسة لكل من Nazar Hlynskyy وOksana، استناداً إلى استطلاع أجرته Reuters Events، أن التحول الرقمي في سلاسل التوريد يُمثل أولوية عالية لدى 48% من المؤسسات الأوروبية. (Hlynskyy, Dovhun, & Pochopień, 2025)

وبناءً على ذلك، أصبحت تدابير الأمن السيبراني لحماية الأنظمة من الاختراق ومواجهة التهديدات تمثل أولوية استثمارية ضمن استراتيجيات التحول الرقمي، كما اتجهت العديد من الشركات إلى تبني سياسات مثل قانون تبادل معلومات الأمن السيبراني، الذي يدعم تبادل المعلومات حول التهديدات والهجمات بين القطاعين العام والخاص(Sadiku, Chukwu, & Sadiku, 2023) .

إضافة إلى ذلك، يتم تعزيز هذا التوجه من خلال برامج التوعية بالأمن السيبراني، مثل البرامج الوطنية التي تهدف إلى رفع مستوى الوعي لدى المؤسسات بمخاطر التهديدات السيبرانية وسبل مواجهتها. (Sadiku, Chukwu, & Sadiku, 2023)

يبين الجدول أدناه أن تطبيق برامج حماية الأنظمة يسهم في تحويل الأمن من إطار نظري قائم على السياسات والتشريعات إلى ممارسة تشاركية قائمة على التفاعل والتكامل بين الفاعلين.

كما يعكس الجدول خطوات الممارسات التعاونية البعد التنظيمي والتشاركي للأمن السيبراني، والذي يُعد عنصرًا أساسيًا في تأمين سلاسل التوريد، حيث يتطلب ذلك تنسيقًا مستمرًا وتبادلًا للمعلومات بين مختلف الأطراف.

جدول رقم (1): خطوات الممارسات التعاونية مع توضيح كيفية تطبيقها وضمان فعاليتها

تأسيس فضاء الممارسات التعاونية	يتم تحديد سبب انشاء مساحة الممارسة، مع عرض التحديات أو المشكلات المراد معالجتها بوضوح.
تجميع المجموعة	يتم جمع الأفراد المعنيين ودعوتهم لطرح وجهات نظر متنوعة حول القضية، بهدف إثراء العمل بتعدد الآراء والخبرات.
تحديد أرضية مشتركة للتعاون	يتم وضع قواعد واضحة للمشاركة والتفاعل، بما يضمن بيئة عمل تعاونية فعالة.
تطوير رؤية مشتركة	يتم بناء رؤية موحدة بين الأعضاء، مع تحديد سياق الممارسة والأهداف المراد تحقيقها.
التعرف على أعضاء المجموعة	يتم التواصل مع الأعضاء والتعرف على خبراتهم ومعارفهم وكفاءاتهم، وتشجيعهم على المشاركة الفعالة مع توضيح الهدف العام.
مرحلة التركيب (التكامل)	يتم تبادل وتحليل الخبرات والممارسات بهدف بناء معرفة جديدة، وتوسيع الآفاق، ومعالجة الثغرات.
مراجعة الانتاج المشترك	يتم تقييم ومناقشة المخرجات بشكل جماعي خلال الاجتماعات، بهدف تطوير الأفكار وتحسين النتائج.
تحويل المعرفة إلى ممارسات تطبيقية	يتم العمل على ترجمة النتائج إلى إرشادات قابلة للتنفيذ، خاصة في مجال تحسين الأمن السيبراني في سياق سلاسل التوريد.
تعزيز المشاركة والالتزام	يشارك الأعضاء في توجيه اللأنشطة واتخاذ القرار، مما يعزز الدافعية والانخراط في العمل.
تحديد الأولويات ودعم المجموعة	تقوم المجموعة بتحديد أولوياتها ومخرجاتها، مع توفير التيسير والدعم من قبل المنسقين دون فرض توجيه مباشر.

المصدر: (Wallis & Dorey, 2024)

ومن خلال ما سبق، يتضح أن السياسات الأمنية لم تعد فردية، بل أصبحت تُبنى ضمن إطار تشاركي تعاوني يعزز الفعالية والاستدامة.

وبالاطلاع على دراسة (الكندي و حور الكلباني ، 2025)، يتبين أنه تم التأكيد على مجموعة من عناصر البنية والسياسات الأمنية، والتي تتقاطع مع ما ورد في جدول الممارسات التعاونية، وذلك من خلال:

- **الاستراتيجية:** حيث تم التأكيد على أهمية وجود استراتيجية شاملة تربط بين إدارة المخاطر والدفاع السيبراني.
- **الالتزام بالبروتوكولات الحكومية:** بما يضمن الامتثال للتشريعات والتنظيمات ذات الصلة بالأمن السيبراني.
- **الحماية الرقمية:** من خلال تأمين كافة حلقات سلسلة التوريد ضد التهديدات السيبرانية.

وهذا يعزز ما ورد في الجدول، حيث أن تحقيق هذه العناصر يتطلب تعاونًا وتنسيقًا مستمرًا بين مختلف الأطراف، مما يؤكد الطابع التشاركي للأمن السيبراني.

جدول رقم (2): أهم سياسات وأساليب الأمن السيبراني لتعزيز حماية سلاسل التوريد

الأساليب/ السياسات	الشرح
سياسة التفتيش (بعد تقني وتنظيمي)	هي عمليات دورية ومنتظمة لتقييم أمن الشبكة، تهدف إلى اكتشاف الثغرات الأمنية ومعالجتها قبل استغلالها.
سياسة التحديث والتحقق (البعد التقني)	تتمثل في الالتزام بالتحديث المستمر والآلي للأنظمة والبرمجيات عبر جميع مراحل دورة حياة سلسلة التوريد، لضمان الحماية من الثغرات المعروفة.
سياسة التحكم في الوصول (بعد تقني + تنظيمي)	تعتمد على تطبيق بروتوكولات صارمة للتحكم في الوصول إلى الأنظمة، مثل المصادقة متعددة العوامل (MFA)، للحد من الهجمات القائمة على سرقة بيانات الاعتماد.
سياسة التوعية الأمنية (بعد بشري)	تشمل برامج تدريبية موجهة للعاملين، تهدف إلى تقليل الأخطاء البشرية غير المتعمدة، والتي تُعد من أبرز أسباب الاختراقات الأمنية.
.سياسة الاستجابة السريعة للحوادث (بعد تقني + بعد تشغيلي)	تعتمد على استخدام تقنيات متقدمة، مثل انترنت الأشياء، لمراقبة الأصول والعمليات بشكل لحظي، والكشف المبكر عن التهديدات، مما يساهم في الاستجابة السريعة والفعالة للحوادث الأمنية.

المصدر: (الكندي و حور الكلباني ، 2025)

تعكس هذه السياسات الأبعاد المختلفة للأمن السيبراني، حيث تجمع بين الجوانب التقنية والتنظيمية والبشرية، وهو ما يعزز من قدرة سلاسل التوريد على مواجهة التهديدات السيبرانية بشكل متكامل.

في ضوء ما سبق من عرض للسياسات الأمنية وتصنيفها وفقًا (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) **ننتقل من التركيز على الإجراءات التنظيمية إلى تناول الجانب التطبيقي، من خلال تحليل كيفية توظيف التكنولوجيا في بناء بنية أمنية حديثة وقادرة على مواجهة التهديدات السيبرانية، وذلك استنادًا إلى نفس الدراسة.**

جدول رقم (3): التقنيات الحديثة الداعمة لتعزيز أمن سلاسل التوريد

التقنية / الممارسة الرقمية	التوضيح
تكامل عمليات سلسلة التوريد	يُعد من الممارسات الحديثة التي تعزز مرونة وأمن سلسلة التوريد، من خلال دمج جميع المراحل بدءًا من التخطيط والانتاج، مروراً بالتخزين، وصولًا إلى التوزيع، ويساهم هذا التكامل في تقليل الثغرات الأمنية الناتجة عن ضعف التنسيق بين المراحل المختلفة.
التخطيط والتنبؤ الفعال	يمثل عنصراً أساسيًا في تحسين أداء سلسلة التوريد، حيث يتم الاعتماد على تقنيات الذكاء الاصطناعي وتحليل بيانات السوق للتنبؤ بالطلب بدقة، مما يساعد في تقليل المخاطر التشغيلية وتحسين الاستجابة، وبالتالي دعم الاستقرار والأمن العام للنظام.
الأتمتة	تُعد من التقنيات الحديثة في النقل والخدمات اللوجستية، حيث تُستخدم لتعزيز الكفاءة في عمليات التحميل والتفريغ والتوصيل، كما يتم توظيف أنظمة مثل تحديد المواقع (GPS) لمراقبة المنتجات وتتبعها، مما يتطلب تأمين هذه الأنظمة ضد التهديدات السيبرانية لضمان سلامة البيانات والعمليات.

المصدر: (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025)

وعلى الرغم من أن هذه التقنيات لا تُعد سياسات أمنية بحد ذاتها، إلا انها تلعب دوراً محورياً في دعم وتعزيز أمن سلاسل التوريد، خاصة عند دمجها ضمن إطار الأمن السيبراني.

من خلال دراسة بُعد البنية والسياسات الأمنية، يتضح أنه يقوم على تكامل مجموعة من العناصر التي تهدف إلى ضمان حماية الأنظمة والبرامج، وتحقيق استمرارية سلاسل التوريد حتى في ظل التهديدات السيبرانية.

وبناءً على ما سبق، يمكن استنتاج أن هذا البعد يرتكز على ثلاث دعائم أساسية:

أ. **الممارسات التعاونية:** كما ورد في دراسة (Wallis & Dorey, 2024)، والتي تقوم على إنشاء فضاء تشاركي يجمع مختلف الخبرات، بهدف تحليل الثغرات الأمنية ومعالجتها بشكل جماعي.

ب. **السياسات والإجراءات الأمنية:** (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025): والتي تعتمد على تطبيق أساليب التخفيف من المخاطر، من خلال الالتزام بسياسات التفتيش والتدقيق الدوري، إضافة إلى التحديث المستمر والرقابة الصارمة على الأنظمة.

ج. **التقنيات الداعمة:** والمتمثلة في تكامل عمليات سلسلة التوريد وأتمتة الانظمة، والتي تساهم في حماية المعلومات وتقليل الأخطاء البشرية، مما يعزز من كفاءة وأمن العمليات.

وعلى الرغم من أن هذا المحور يركز أساسًا على البعد التنظيمي للأمن السيبراني، إلا أن تحقيق فعاليته يتطلب تكاملًا مع الأبعاد الأخرى، خاصة البعد التقني والبشري، وهو ما سيتم التطرق إليه في المحاور اللاحقة.

2. **التكنولوجيا والحماية الرقمية (البعد التقني):** يمثل بُعد التكنولوجيا والحماية الرقمية الامتداد التطبيقي للبعد التنظيمي، حيث يركز على توظيف التقنيات الحديثة كوسيلة لتنفيذ السياسات الأمنية، من خلال حماية الأنظمة والبرمجيات، وتأمين تدفق البيانات والعمليات عبر مختلف مراحل سلسلة التوريد في مواجهة التهديدات السيبرانية.

وينقسم البعد التقني للأمن السيبراني إلى قسمين: يتمثل الأول في الأدوات التقنية الأساسية التي تشكل خط الدفاع الأول لحماية الأنظمة، بينما يتمثل الثاني في التقنيات المتقدمة التي تعتمد على الذكاء والتحليل لتعزيز القدرة على التنبؤ بالتهديدات والتصدي لها.

أولا: الأدوات التقنيات المتقدمة في الحماية الرقمية

يرتكز الأمن السيبراني في سلسلة التوريد على توليفة متكاملة من الحلول التقنية التي تتباين بين التقنيات الذكية المتطورة والأدوات الدفاعية الرئيسية، ويتطلع إلى بناء خط دفاع يضمن آمن البيانات واستمرارية التدفقات اللوجستية ضد المخاطر، ومنه نبرز هذه الوسائل التقنية المتقدمة وصولا لأدوات البرمجة التي تعد حصن الدفاع عن أصول المؤسسة الرقمية والمادية معا.

أ. **تقنية سلسلة الكتل (Blockchain)** : تضمن نظام أمن وشفاف في التعامل مع التهديدات، وتعتبر هذه التقنية من التقنيات الحديثة تقوم على قاعدة بيانات سحابية ضخمة تتكون من مجموعة من الكتل متصلة فيما بينها كل كتلة لها بصمة خاصة تسمى(Hash) ، تقوم على أساس اللامركزية بحيث توزع السجلات في

جميع الأجهزة، لا يمكن التعديل في أي سجل فمن خلال طبيعة التوزيع التي تقوم عليها البلوكشين يجعل من الاختراق أمر شبه مستحيل، وإمكانية الوصول واسترجاع المعلومات بشكل آمن. (تكليت، 2022)

وفي مجال الحماية الرقمية في الأمن السيبراني أكدت دراسة (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) أن هذه التقنية تقدم سجلات شفافة من خلال عدم توفر خاصية التعديل أو المسح كما هو موضح في المفهوم أعلاه، من خلال معرفة الشخص القائم بالعملية ومتى قام بها والحرص على تتبع وتسجيل كافة العمليات الرقمية لسلاسل التوريد، مما يمكن المؤسسة من التصدي لكلي تغيير في البيانات.

ب. **الذكاء الاصطناعي (Artificial Intelligence):** يقدم كشف عن التهديدات من خلال قدرة التنبؤ والاستجابة السريعة لأي تهديد.

ج. **أنترنت الأشياء (IOT)**: هي نظام من الأجهزة المترابطة فيما بينها، تقوم بتبادل المعلومات دون التدخل البشري، تستخدم تقوم على برامج، أجهزة لمعالجة البيانات، أجهزة الاستشعار والمشغلات واتصال الشبكات ببعضها. (صادوق و نيل، 96-110)

أشار (الكندي و حور الكلباني ، 2025) في دراسته إلى أنها تقنية متقدمة تزيد من كفاءة وفعالية الأمن الرقمي، حيث تقوم على جمع البيانات الفعلية و تحليلها للتنبؤ بأي تهديدات من خلال المراقبة للأصول والعمليات عبر أجهزة الاستشعار(IOT).

وأشارت دراسة (Hlynskyy, Dovhun, & Pochopień, 2025) أيضا إلى بعض من التقنيات المتقدمة، كل من التعلم العميق وأساليب دمج البيانات كونها تقنيات أساسية لنظام محصن.

د. **التعلم العميق(Artificial Intelligence)**: استخدمت هذه التقنية لزيادة المرونة السيبرانية اذ هو فعال في اكتشاف التهديدات في الوقت المناسب وضمان أمن الاتصالات.

ه. **أساليب دمج البيانات:** حسب ماورد في دراسة (Hlynskyy, Dovhun, & Pochopień, 2025) فإن الأنظمة تحتاج إلى تجميع بيانات، بحيث يتم الاعتماد على هذه الاساليب من خلال تجميع عدة معلومات التي تساهم في معرفة أمان الأنظمة ومنه اكتشاف أي تهديدات وتغطية الثغرات الأمنية.

ثانيا: أدوات ومنظومات الحماية التقنية: تعد هذه الأنظمة الحصن الرقمي للبيانات للتصدي لأي عمليات مشبوهة قد تصد عمل سلسلة التوريد.

أ. **التشفير (Encryption Systems)** : يقصد بالتشفير تلك الطريقة التي تعتمد على الخوارزميات الرياضية الذكية التي تسمح لمن يمتلك مفتاحا سريا أن يحول رسالة مقروءة لرسالة غير مقروءة أو العكس (حزام، 2020)، فهو يؤمن وصول الأطراف المعنية فقط إلى البيانات.

وهذا ما أكدته دراسة (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) بأنه إجراء تقني أساسي لحماية البيانات وزادا تأكيدا عن تشفيرها أثناء عملية الإرسال أو النقل لعرقلة أي اختراق.

ب. **الجدار الناري (Firewalls)** : هو مجموعة أنظمة توفر سياسات أمنية بين الإنترنت والشبكة الخاصة لتصبح جميع عمليات العبور إلى الشبكة أو الخروج منها تمر من خلال الجدار الناري الذي يصد المستعملين غير المرغوب فيهم. (حزام، 2020) أي هو تصد أي تدخل غير مصرح به.

ج. **أنظمة كشف التسلل(IDS)**: تم التطرق لأنظمة كشف التسلل من خلال مهامها الرئيسية:

الدور الأساسي لهذه الأنظمة هو الوقاية، إذ تعد إجراء أساسي لحماية المعلومات الحساسة والتأكد من آمانها حتى خلال حركة ونقل البيانات (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025).

تعتمد في عملها على (**packet sniffers**) التي هي تقوم بمراقبة حركة جميع أنواع عمليات البيانات، ومنه يسهل عملية التصدي لأي اختراق في الوقت الفعلي. (حزام، 2020)

تقوم بكشف عمليات الاختراق التي تتمثل على شكل برامج خبيثة وملفات مشبوهة، فلها القدرة على إزالتها قبل الوصل إلى غرض الاختراق في النظام. (حزام، 2020)

د. **المصادقة متعددة العوامل (MFA)**: تضمن تقنية المصادقة على حصر صلاحية الوصول للبيانات من خلال الأشخاص المؤهلين لها فقط . و تشدد (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) على ضرورة تنفيذ هذه التقنية في الأنظمة الحساسة، إذ هي فعالة في التصدي للهجمات مثل محاولة سرقة كلمة المرور.

تعمل المصادقة دائما على التحقق من هوية الرقمية للمستخدم قبل أي عملية دخول، وتعمل على هذا من خلال الاستعانة بالجدران النارية. (حزام، 2020)

غياب نظام فعال مثل نظام المصادقة، يعرض بيانات سلسلة التوريد إلى الاستعمال من أشخاص غير شرعيين ومنه عرقلة استمرار عمليات سلسلة التوريد. (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025)

إضافة على كل الأدوات السابقة أشارت في دراسة سابقة (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) إلى أن سلاسل التوريد تستخدم نظام(**GPS**)كونه تقنية تكنولوجية متقدمة لمراقبة سلع و أصول المؤسسة من السرقة خلال الحركة وتعزيز صلابة الأمن السيبراني.

3. **الوعي والتطبيق في الأمن السيبراني(البعد البشري)**: يتمثل في:

- **الإدراك الأمني هو العمود الفقري لحماية سلاسل التوريد:** يصنف الوعي الأمني أحد أهم دعائم الأمن السيبراني في المؤسسات، حيث لا يمكن لأي نظام تقني أن يحد الخطاء البشرية بالكامل، أي توفر أدوات حماية ليس بالضرورة أن المؤسسة محصنة ضد الهجمات، بالأخص غياب الوعي لدى الموظفين، وبسبب طبيعة سلسلة التوريد المترابطة يمتد هذا الوعي ليشمل كل من الموردين وموردو الموردين، أي نقص الوعي في حد ذاته ثغرة أمنية تستغل لإختراق الأنظمة، وهذا مايؤكد أن الأمن السيبراني مسؤولية مشتركة لجميع عناصر سلسلة التوريد.

- **تناسق العنصر البشري والإجرائي في الإستراتيجية الدفاعية:** العنصر البشري يمثل نقطة الانطلاق في كل من استراتيجيات الدفاع السيبراني، بحيث الأمن الداخلي لأيقل أهمية عن الأمن الخارجي، لأن الموظف هو أول من يتعامل مع البيانات الحساسة، بحيث أي تسريب للبيانات سواء بقصد أو بدون قصد، من أبرز المخاطر التي تشكل خطرا على أمن سلسلة التوريد، مما يؤكد أن العنصر البشري له دور فعال في التصدي للهجمات. (Sadiku, Chukwu, & Sadiku, 2023)

ومن هذا الانطلاق، يستوجب تحديد مسؤليات الموظفين داخل المؤسسة، مع الحد من الوصول إلى المعلومات الحساسة لغير المؤهلين.

- **الوعي كجزء من بنية النظام السيبراني:** يرتكز النظام السيبراني على ثلاث أسس رئيسية (العمليات، الأفراد، التقنيات)، وفي أغلب الأحيان يكون الموظف هو الحلقة الأولى المستهدفة، بحكم المسؤلية المباشرة عن التعامل مع المعلومات، بحث تعزيز مستوى الوعي لدى الموظف وإدراكه لطبيعة المخاطر يساعد بشكل ملحوظ في الحد من الأخطاء غير المقصودة.

في إطار توجه المؤسسات نحو التحول التكنولوجي، بحيث يمثل هذا التحول أولوية للعديد من المؤسسات الأوروبية، وهو أهم مجالات الإستثمار، تتنامى الحاجة إلى تعزيز الأمن السيبراني بشكل أساسي لإستمرارية سلسلة التوريد، ومنه يعتبر التدريب والتعليم أداة لرفع كفاءة الموظفين، وهي ما تهدف إلى قدرة الموظف على التعرف على التهديدات بشكل استباقي.

ومنه، البعد البشري العنصر المحوري في إحراز فعالية الأمن السيبراني، أي نجاح السياسات التنظيمية والأدوات التقنية يظل تابع بوعي الموظفين وقدرتهم على التطبيق السليم.

4. البعد التعاوني في الأمن السيبراني: أيا كانت كفاءة الأنظمة التقنية في المؤسسة، إذ أن الأمن السيبراني لا يتحقق إلا من خلال تضافر الجهود لجميع أطراف سلسلة التوريد، بحيث أن الوعي المتبادل بين المؤسسات والموردين و الموردين الفرعيين يشكل حجر الزاوية في حماية سلسلة التوريد من أي تهديد أو اختراق سيبيران (Wallis & Dorey, 2024)، ويتم ذلك عبر التالي:

- **الشراكة والتضامن الأمني:** تسند مسؤولية الأمن السيبراني إلى كافة أصحاب العلاقة، مما يضم المؤسسات، البنية التحتية، الحكومات، الموردين، تقوم هذه الشراكة على ضمان توحيد الإجراءات الأمنية وتبادل المعلومات حول الهجمات المرجحة، على نحو يجعل كل طرف مدرك لمسؤولياته فيما يخص حماية سلسلة التوريد.

- **الوعي الجماعي والتطبيق المشترك:** يحتوي البعد التعاوني لنمط استباقي في التصدي للتهديدات، بحيث توجه جميع الأطراف لرفع الوعي بالهجمات السيبرانية، واعتماد إجراءات موحدة لحماية حلقات سلسلة التوريد، وهذا ما يضمن فشل أي اختراق محتمل للنظام.

- **التقدير المسبق للتهديدات:** التنبؤ بالهجمات هو أحد العناصر الأساسية للبعد التعاوني، بحيث يقوم المشاركون بجمع البيانات والخبرات لرصد المخاطر المحتملة، مع وضع خطط مضادة لها، يساهم هذا النهج في رفع قدرة سلسلة التوريد على التصدي للاختراقات قبل وقوعها مع استمرارية العمليات.

استنادا على ما تم التطرق إليه من المنطلق النظري وأبعاده المتعددة للأمن السيبراني، يتاح لنا بلورة رؤية تحليلية بالاعتماد على النقاط المحورية الموضحة أدناه:

- **التحول المنهج للشمولية التنظيمية:** إن الأمن السيبراني لم يبقى محصورا في كونه درع تقني لأمن المعلومات أي الوقاية التقنية، بل تحول إلى عنصر أساسي من النظام الإداري لسلاسل التوريد، مما يحوله إلى العمود الفقري لحماية الأصول الرقمية والمادية للمؤسسة معا.

- **الأمن المشترك:** نستخلص أن أمن سلسلة التوريد الرقمية هي مسؤولية تشاركية عابرة للحدود التنظيمية، وانطلاقا من قاعدة السلة بمتانة أضعف حلقاتها، يتبين أن هشاشة الوعي لدى أي طرف منها (سواء مورد أو عامل أو حتى مورد المورد) يمكن ان يعصف أمن السلسلة بالكامل.

- **المرونة كقدرة تنافسية:** أن الترابط بين التكنولوجيا المتطورة (مثل البلوكشين والذكاء الاصطناعي) والإدراك البشري لا يقتصر هدفه لمنع الهجمات، وإنما لبناء ما يعرف بالمرونة السيبرانية التي تعتبر القدرة على التنبؤ بالتهديد والاستجابة السريعة له، وهذا ما يعد كونه ميزة تنافسية تضمن استمرارية العمليات اللوجيستية حتى في أوج الأزمات الرقمية.

ومنه نصل إلى أن الأمن السيبراني هو الدعامة المركزية الذي يضمن تدفق المعلومات والسلع بأمان، وهو ما يستدعي ممارسات تتعدى الحلول البرمجية إلى بناء ثقافة أمنية متجذرة في جميع حلقات سلسلة التوريد.

المطلب الثاني: الإطار النظري لسلاسل التوريد

يعد الإطار النظري لسلاسل التوريد الأساس المفاهيمي لتنظيم تدفقات القيمة من المورد إلى المستهلك، حيث يهدف إلى تحقيق التكامل الاستراتيجي بين الشركاء لرفع الكفاءة وتقليل الهدر. كما يركز على تعزيز المرونة والميزة التنافسية من خلال تبني الابتكار والرقمنة لمواجهة تغيرات السوق.

الفرع الأول: تعريف سلسلة التوريد

تعتبر سلسلة التوريد نظام شامل للأنشطة الوظيفية (مثل التخزين، الشراء والنقل) التي تسد الفجوات المكانية والزمانية عند تحويل المواد الخام إلى منتجات نهائية ذات قيمة ملموسة للعميل، بحث تشمل التدفقات الأمامية (من المنتج إلى العميل)، والتدفقات العكسية المرتبطة بإعادة إصلاح المنتجات المتقادمة، ومنه تمثل السلسة دورة حياة المنتج الكاملة التي تنطلق من مصادر التوريد حتى التخلص النهائي من المنتج. (غازي، 2022)

هي حلقة الوصول للموارد والعمليات والتي تبدأ بمصدر الموارد الخام وتمتد خلال توصيل أو تسليم المنتجات التامة إلى العميل النهائي، ويشمل ذلك التجار والتسهيلات الصناعية، والقائمين على نظم التوريد ومراكز التوزيع الداخلية والموزعين وأي كينونات أخرى تمهد السبيل إلى قبول ورضا العميل النهائي. (الرفاعي، 2016)

جميع الأنشطة المتعلقة بتدفق وتصنيع المنتجات من خلال الموردين إلى المستهلك النهائي، إضافة إلى تدفق المعلومات، وكلا التدفقين يتم الموردين إلى العملاء و العكس. (مصاروة، 2019)

هي عملية إدارة تدفق المواد والمنتجات التامة من الموردين إلى المستهلكين، وهذا يتضمن جميع مظاهر العمل من معالجة المبيعات، الانتاج، إدارة المخزون، توريد المواد، التوزيع، الشراء، التخمين، خدمة، العملاء، مجالات أخرى متعددة. (عزوز، 2018)

وبناء على تعدد زوايا النظر في مفهوم سلاسل التوريد، يمكننا تبني التعريف الإجرائي التالي:

تعد سلاسل التوريد بأنها النسق الديناميكي المتكامل الذي يوصل بين الحلقات المترابطة في الهدف والمستقلة وظيفا، التي تقوم بتزامن التدفقات المتداخلة (ماليا، معلوماتيا، وماديا) انطلاقا من مصدر التوريد الأولي وصولا إلى المستهلك النهائي وما بعد ذلك من اللوجستيات العكسية، **وتتجلى إجرائيا في القدرة على تحويل المدخلات إلى مخرجات مولدة للقيمة من خلال العمليات المترابطة (كالتوزيع، التخزين، الانتاج، الشراء) القابلة لقياس كفاءتها بمدى تحقيق المرونة في الاستجابة، بالإضافة إلى الحد من الفجوات المكانية والزمنية، وتحقيق استمرارية التدفق تحت تنوع الظروف البيئية.**

الفرع الثاني: أهمية سلاسل التوريد

يمكن أيجاز أهم الفوائد التي يمكن تحقيقها من إدارة سلاسل التوريد فيما يلي: (غازي، 2022)

- ✓ زيادة الاستجابة للزبائن.
- ✓ الاستجابة في الأوقات السليمة.
- ✓ وقت انتظار قصير لإشباع الطلبات.
- ✓ تخفيض تكاليف الاحتفاظ المخزون.
- ✓ تحسين معدل استخدام الموجودات.
- ✓ تخفيض تكلفة شراء المواد.
- ✓ جودة عالية المنتجات.
- ✓ الحسين القدرة على مواجهة الحوادث غير المتوقعة.
- ✓ السرعة في تطوير المنتجات.

الفرع الثالث: نشأة سلاسل التوريد

تبلور مفهوم سلسلة التوريد على امتداد مراحل زمنية مختلفة من النشأة (1956-1965) التي انصب اهتمامها على مدخل النظم، بالمرور على فترة الاختبار (1965-1970)، ومع فترة الأزمات (1970-1978)، أوجبت محاور جديدة فرضاتها التقلبات الاقتصادية التي تنصب على التخطيط الوقائي، مفضيا إلى التكامل الشامل (منذ 1980) التي نسقت التدفقات بين كل من المستهلك والمورد وجعلت منه أسلوب حتمي لرفع الكفاءة التشغيلية والتخفيض من التكاليف. (غازي، 2022)

1) **بداية ظهور وتبلور مفهوم سلسلة التوريد (1956–1965)**: بدأ مفهوم التوريد يظهر كنشاط متكامل خلال هذه الفترة، نتيجة عدة عوامل :

- **تطور مفهوم التحليل الكلي لعناصر التكلفة:** تحليل تكاليف الأنشطة المرتبطة معًا للوصول لأقل تكلفة إجمالية ممكنة، حتى لو كانت بعض التكاليف الفرعية مرتفعة، مثل ارتفاع تكلفة النقل مقابل انخفاض تكلفة التخزين .

- **تطور مدخل النظم (Systems Approach)**: النظر إلى المنظمة كنظام متكامل من أنظمة فرعية مترابطة (التسويق، التمويل، الانتاج)، ما ساعد على توحيد أنشطة التوريد تحت إطار إداري واحد .

- **الاهتمام بالخدمة المقدمة للمستهلك:** تحول التركيز من مجرد تحليل التكاليف إلى تقديم أفضل مستوى خدمة للعملاء بأقل تكلفة ممكنة .

- **تنظيم قنوات التوزيع:** توحيد الجهود في تدفق السلع الواردة والصادرة وتقليل ازدواج الجهود والتكاليف .

2) **فترة الاختبار(1965–1970)**: تم اختبار المفاهيم الأساسية للإمداد المتكامل، وظهرت إدارة التوزيع المادي وادارة المواد كنشاطات مرتبطة بالتوريد، وبدأت الشركات في إدراك الفوائد التشغيلية لتطبيق هذا المفهوم .

3) **فترة ظهور أولويات جديدة(1970–1978)**: تميزت بتقلبات اقتصادية وسياسية مثل **حرب أكتوبر(1973)** وارتفاع أسعار الطاقة، ما أثر على تكاليف الانتاج والمواد وأدى ذلك إلى تغييرات في أولويات إدارة التوريد: التركيز على **توفير احتياجات المشروع بأقل تكلفة واستخدام الطاقة بكفاءة**، وتطوير أساليب التخطيط طويل الأمد لتجنب نقص المواد.

4) **نحو تكامل انشطة التوريد (1980– حتى الان)**:

- أصبح التركيز على **تحقيق الترابط والتكامل بين إدارة المواد والتوزيع المادي** لضمان تلبية احتياجات التشغيل وتحقيق أهداف المشروع.
- المزايا: تقليل الجهود المكررة، تخفيض التكاليف، رفع الكفاءة التشغيلية، وتوحيد الرقابة والاتصال بين الانشطة.
- الإدارة المتكاملة أصبحت الأسلوب الإداري السائد لتحقيق تنسيق بين الانتاج والتسويق وضمان فعالية تدفق المواد من المورد إلى المستهلك النهائي.

الفرع الرابع: أبعاد سلاسل التوريد من منظور الأمن السيبراني

تمثل كفاءة سلاسل التوريد الحديثة رهينة بقدرتها على توحيد الحلول التقنية مع الأطر الأمنية المتطورة، بحيث لم يعد الأداء اللوجيستي ينحصر على سرعة التدفقات المادية فحسب، وإنما توسع ليشمل حصانة التدفقات المعلوماتية، وتتكون أبعاد هذا الأداء من خلال منظومة متكاملة تضم بين الكفاءة التشغيلية لضمان استغلال الموارد، وجودة الخدمات لتعزيز موثوقية العميل، ليصل إلى الاستمرارية والمرونة في مواجهة التحديات، وكل ذلك ينبني على قاعدة صلبة من استراتيجيات الحماية الرقمية التي تحول التهديدات السيبرانية إلى فرص للبروز والتفوق التنافسي.

1) **الكفاءة التشغيلية**: تعكس الكفاءة التشغيلية في سلسلة التوريد الإلكترونية قدرة المؤسسة على الاستفادة من الموارد المتاحة بشكل أمثل وتأمين استمرارية العمليات الانتاجية واللوجستية بأدنى هدر ممكن، وقد شارك تطبيق الأمن السيبراني في الحد من الأخطاء في العمليات اللوجستية وتعجيل عمليات التوريد، إلى جانب الحد من الانقطاعات وتوقف العمليات وتحسين استخدام الموارد. (Hlynskyy, Dovhun, & Pochopień, 2025)

وتشير المؤشرات العملية لهذه الكفاءة مقدار قدرة النظام المدعوم بالذكاء الاصطناعي والأمن السيبراني على أتمتة الرؤية الشاملة لكافة حلقات سلسلة التوريد، مع توفير الموارد والوقت، والتوقع بالتهديدات الممكنة قبل الوقوع لضمان استمرارية العمليات. (Claudia، Federico، و Antonella، 2026)

2) **جودة الخدمة ورضا العملاء:** يدل بعد جودة الخدمة على إمكانية سلسلة التوريد على توفير توقعات العملاء وتقديم خدمات عالية الجودة. نتجلى عن تطبيق الأمن السيبراني إلى تعزيز رضا العملاء من خلال تأمين حماية معلوماتهم الحساسة وتعزيز الثقة بين كل من الشركاء والموردين والمؤسسة. (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025) كما ساهم الأمن السيبراني على الحفاظ على امن العمليات اللوجستية .

3) **الاستمرارية والمرونة:** تكمن أهمية هذا البعد في قدرة سلسلة التوريد على مواجهة كل المخاطر النشأة فجأة ولاستشفاء من التهديدات بسرعة، بحث الأمن السيبراني أحدث تأثيرا على أمن استمرار العمليات أثناء الهجمات والتكيف مع التحديات المتغيرة. (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025)

4) **استراتيجيات الحماية الرقمية والوقاية التقنية:** تؤدي هذه الاستراتيجيات دورا أساسيا في تقوية أمان سلسلة التوريد، من أهمها تحديث الأنظمة بشكل دوري، بما يتضمن كلمات السر، لضمان سلامتها، (حزام، 2020) ويعتبر توحيد الموردين في هذه الاستراتيجيات ضرورة لتعزيز صلابة الأمن السيبراني داخل سلسلة التوريد، حيث تعد المصادقة المتعددة العوامل(MFA) أداة جوهرية لضمان الوصول المصرح به وحماية المعلومات، بينما يلعب توظيف نظام تحديد الموقع (GPS) دورا فعال في تتبع السلع أثناء النقل، بحيث يحد من مخاطر الاختراق والسرقة، ومنه دعم سلامة البيانات. (Said Al-Kindi, Alkalbani, Al-Hinai, & Ramadan, 2025)

ومنه نستنتج مما سبق أن تحقق هذه الأبعاد تكامل بنيوي بين التحصين السيبراني والكفاءة اللوجستية، بحيث استدامة التدفقات المعلوماتية والمادية بواسطة رؤية استباقية تستند التقنيات الحديثة للتنبؤ بالمخاطر والتصدي للانقطاعات، كذلك يقرن أمن البيانات وجودة الخدمة لجعل الحماية الرقمية معيار للموثوقية التنافسية، وهذا ما يؤكد الانتقال من مرحلة الصمود إلى المرونة والتشافي السريع من الأزمات.

وكخلاصة لهذا المبحث نستمد بناء على ما سبق أن الأمن السيبراني انتقل من حصن تقني إلى دعامة استراتيجية تحقق استدامة سلسلة التوريد في العصر الرقمي، فمن خلال انسجام أبعاده (كل من البشرية، التقنية، التنظيمية) لم يعد الغرض صد الهجمات فقط، وإنما بناء مرونة سيبرانية تعزز الكفاءة التشغيلية، وتضمن جودة الخدمة، وتعزز قدرة السلسلة على الاستجابة السريعة للأزمات.

وختاما، فإن صلابة سلسلة التوريد باتت تقاس بمدى تحصين التدفقات المعلوماتية، مما يجعل الحماية الرقمية عامل رئيسي للمصداقية والتنافسية اللوجستية.

المبحث الثاني: الأدبيات التطبيقية لأثر الأمن السيبراني على كفاءة سلاسل التوريد

عقب الفراغ من الجانب المفاهيمي لمتغيرات الدراسة، سنقوم في هذا الجزء باستعراض جملة من الدراسات السابقة باللغة الأجنبية التي عالجت موضوع الأمن السيبراني في سياق سلاسل التوريد. تم اختيار هذه الدراسات بناءً على حداثتها وصلتها المباشرة بمتغيرات البحث، حيث اعتمدنا في عرضها على الترتيب الزمني التنازلي (من الأحدث إلى الأقدم) للفترة ما بين 2020 و2026، ويهدف هذا الاستعراض إلى تمهيد الطريق لإجراء مقارنة دقيقة بين ما توصلت إليه هذه الأدبيات الأجنبية وما تسعى الدراسة الحالية للتحقق منه.

بعد التطرق إلى الجانب المفاهيمي لمتغيرات الدراسة، فلابد من الاطلاع على مجموعة من الدراسات التي عالجت الأمن السيبراني في سلسلة التوريد، وتم الاعتماد على هذه الدراسات بناء على حداثتها وصلتها المباشرة بمتغيرات الدراسة الحالية، وقمنا بعرضها حسب الترتيب الزمني التنازلي من الأحدث إلى الأقدم بهدف تمهيد الطريق لوضع أهم الفروقات بين هذه الدراسات الأجنبية وما تسعى له دراستنا الحالية.

المطلب الأول: الدراسات السابقة

1) دراسة (Aikaterin & Costas, 2026)

مقال بعنوان: إدارة المخاطر في سلسلة التوريد السيبرانية: من التهديدات إلى المعالجة– قسم النظم الرقمية، جامعة بيريوس، اليونان، 2026، عدد 25، رقم 40، 2026.

هدفت الدراسة إلى عرض إطار شامل لإدارة مخاطر سلاسل التوريد السيبرانية (C-SCRM)، والتركيز على تحديد التهديدات والثغرات الأمنية الناجمة على الاعتماد المتصاعد على مصادر تكنولوجيا المعلومات الخارجية، وتم استخدام المنهج الوصفي التحليلي من خلال مراجعة نظامية للأدبيات العلمية، واتخذت الدراسة المراجعة المنهجية كأداة للبحث، بالإضافة إلى تحليل المحتوى النوعي للوثائق التقنية الموثقة في نهاية 2025، وحللت البيانات بالأسلوب الإستنتاجي المنطقي إنشاء نموذج مقترح لمعالجة المخاطر السيبرانية، والنتائج المتوصل إليها كانت كالتالي:

- تتمثل الفجوة الأمنية الكبرى في نقص الرؤية لدى المؤسسات تجاه الخدمات أو المنتجات المشتراة من الموردين الخارجين.
- ضرورة اعتماد المعالجة الشاملة التي تنطلق من إختيار الموردين، ومراقبة الأصول، وصولا إلى الاستجابة لحوادث السيبرانية.
- أسهمت جائحة كوفيد-19 وخاصة في مراحلها اللاحقة، في الزيادة الحادة للمخاطر السيبرانية لسلسلة التوريد، بسبب التسارع في تبني الرقمنة.

2) دراسة (Alqudhaibi, et al., 2026)

مقال بعنوان: الأمن السيبراني الاستباقي في الصناعة 4.0:مسح لمنهجيات التنبؤ بالتهديدات السيبرانية في أنظمة التصنيع ،قسم هندسة الحاسوب الشبكات ،جامعة كرانفليد البريطانية وجامعة أم القرى ،بريطانيا و السعودية؛ العدد 14؛ الرقم 25؛ 2026.

هدفت لتحليل منهجيات التنبؤ بالتهديدات السيبرانية لحماية أنظمة التصنيع في عصر الصناعة 4.0، وتم استخدام المنهج الوصفي التحليلي من خلال مراجعة أدبيات الفترة (2010-2025)، وتم تحليل المنهجيات باستخدام التصنيف النوعي للفجوات البحثية والحلول الذكية المقترحة.

وتم التوصل إلى النتائج الاقتصادية التالية:

- حتمية الانتقال من الدفاع التقليدي إلى الأمن الاستباقي للتنبؤ بالهجمات قبل تأثيرها.
- فاعلية تقنيات تعلم الآلة والذكاء الاصطناعي في كشف التهديدات المعقدة في بيئات إنترنت الأشياء الصناعي.
- دعت الدراسة إلى تعزيز الوعي الأمني للموظفين ومعالجة تحديات دمج أنظمة المعلومات (IT) مع الأنظمة التشغيلية (OT).

3) دراسة (Modarress-Fathi, Ansari , & Ansa, 2026)

مقال بعنوان :المخاطر على سلاسل التوريد المستدامة واللوجستيات _قسم الأعمال والاقتصاد ،جامعة ستايل ، واشنطن الولايات المتحدة الأمريكية.

هدفت إلى التعرف على طبيعة العلاقة بين المخاطر النظامية العالمية (مثل الكوارث الطبيعية ،الأزمات الجيوسياسية ،والجرائم السيبرانية) وبين الضغوط الممارسة على سلاسل التوريد و الأنظمة اللوجستية المستدامة ، حيث تم استخدام المنهج الوصفي التحليلي والمنهج الكمي للجانب التطبيقي، واعتمدت الدراسة على بيانات ثانوية ضخمة تم جمعها من تقارير دولية للفترة ما بين (2000-2024)، وتم استخدام أداة مؤشر ضغط سلسلة التوريد العالمية (GSCPI) كمعيار قياس أساسي، مع معالجة البيانات إحصائياً بواسطة برنامج (SPSS) عبر اختبارات الانحدار المتعدد والارتباط، وتوصلت الدراسة للنتائج التالية:

- وجود علاقة ارتباطية موجبة وقوية ذات دلالة إحصائية بين زيادة التهديدات الخارجية (خاصة السيبرانية) وارتفاع مؤشرات الاضطراب في سلاسل التوريد العالمية.
- أثبتت الدراسة أن الجرائم السيبرانية والهجمات الإلكترونية تُعد المتنبئ الأول والأكثر خطورة بحدوث تأخيرات وتكاليف غير متوقعة في اللوجستيات الرقمية.
- حقق نموذج الدراسة قدرة تفسيرية عالية جداً بلغت 92%، مما يعني أن العوامل المدروسة تفسر معظم التغيرات الحاصلة في أداء سلاسل التوريد.

4) دراسة (Ahi, Agrawal, & Valizadeh, 2026)

مقال بعنوان :مخاطر قابلية التوسع في الذكاء الاصطناعي الوكيل و أمن سلسلة التوريد ،قسم أبحاث الذكاء الاصطناعي و الأمن السيبراني ،الولايات المتحدة الأمريكية؛العدد112؛ الرقم 8 ؛2026.

هدفت للتعرف على المخاطر الأمنية الناتجة عن توسع استخدام النماذج اللغوية (LLMs) والذكاء الاصطناعي الوكيل، واستخدمت المنهج الوصفي التحليلي لمراجعة 70 ورقة بحثية، وتم تحليل البيانات عبر مؤشر LSRI لتقييم مخاطر النشر، وغطت المدة الزمنية (2025/2018)وتوصلت للنتائج التالية:

_الرقمنة المعتمدة على الـــ LLM ضاعفت تهديدات البرمجيات الخبيثة وهجمات عبر أتمتها على نطاق واسع.

_أثبتت النماذج اللغوية كفاءة فائقة في كشف الثغرات بنسبة 91% مقارنة بالطرق التقليدية.

_أكدت الدراسة ضرورة حماية سلسلة توريد النماذج عبر التوقيعات المشفرة لضمان سلامتها من التلاعب.

_دعت إلى تبني "التعلم الفيدرالي" والذكاء الاصطناعي القابل للتفسير لتعزيز الخصوصية والامتثال القانوني.

5) دراسة (Ghasemshirazi , Shirvani, Ranjbar Tavakoli , Ghaedi, & Amin Langarizadeh, 2026)

مقال بعنوان: تطبيق بنية الثقة الصفرية لتعزيز الأمن والمرونة في سلسلة توريد الأدوية _قسم الكيمياء الطبية كلية الصيدلة، جامعة كرمان للعلوم الطبية، إيران؛ العدد 12؛ الرقم 04؛ 2026.

هدفت إلى تحليل فعالية نموذج (الثقة الصفرية) في حماية سلاسل التوريد الأدوية من الهجمات السيبرانية، وضمان سلامة المنتجات الصيدلانية وتتبعها رقمياً، تم الاعتماد على المنهج الوصفي التحليلي مع تطبيق دراسة الحالة، حيث تم تصميم إطار عمل تقني يربط بين الأمن السيبراني والعمليات اللوجستية للأدوية الحساسة ، بحيث كانت المدة الزمنية لهته الدراسة (2026/2024) ، وتم التوصل من خلال الدراسة التالية الى مجموعة من النتائج الاقتصادية:

- أثبتت الدراسة أن الانتقال إلى نموذج يساهم في تقليص مساحة الهجوم السيبراني بنسبة كبيرة في الأنظمة اللوجستية المرتبطة رقمياً.
- يؤدي تطبيق الثقة الصفرية إلى تعزيز الشفافية وقابلية التتبع، مما يضمن وصول الأدوية الأصلية للمرضى ويحمي البيانات الحساسة من الاختراق.
- ضرورة تبني معايير موحدة للأمن السيبراني بين جميع أطراف سلسلة التوريد (مصنعين، موزعين، مقدمي رعاية صحية) لضمان الامتثال التنظيمي والرقابي الصارم.

6) (Afifi Mohamed Afifi , Abd Eltawab Hashem, & Abulsaoud Ahmed Younis, 2026)

مقال علمي بعنوان: مراجعة نظامية لإدارة مخاطر سلسلة التوريد السيبرانية–قسم إدارة الأعمال ،جامعة القاهرة ،مصر؛ العدد1151؛ الرقم ؛ 2026.

هدفت إلى تقديم مراجعة نظامية وتقييم مفاهيمي شامل لإدارة مخاطر سلسلة التوريد السيبرانية (C-SCRM)، بهدف سد الفجوة المعرفية وتوحيد التعريفات المتداخلة لتعزيز استدامة المنظمات وقدرتها على الصمود، تم استخدام المنهج الوصفي التحليلي من خلال أسلوب "المراجعة النظامية للأدبيات" (SLR)، وجمعت البيانات من قاعدة البيانات العالمية Web of Science، شملت عينة الدراسة 175 مقالاً علمياً محكماً منشورة في الفترة (2014-2025)، ومن أجل معالجة النتائج تم اختيار البرنامج الإحصائي VOSviewer، وتوصلت الدراسة للنتائج التالية:

- إن الإدارة الفعالة لمخاطر سلسلة التوريد السيبرانية تؤثر بشكل إيجابي ومباشر على الأداء المالي والعملياتي للمؤسسات.
- يعتبر الخوف من المخاطر الرقمية وغياب الأطر الموحدة من العوامل الرئيسية التي تعيق الممارسين عن التطبيق الفعلي لهذا المفهوم.

7) دراسة (Ciceri, Caniato, & Moretto, 2026)

مقال بعنوان: دمج قدرات الذكاء الاصطناعي في إدارة مخاطر الأمن السيبراني لسلسلة الامداد، قسم اللوجستيات والتسويق، كلية الإدارة، جامعة البوليتكنيك في ميلانو، إيطاليا؛ العدد 01؛ الرقم 56؛ 2026

هدفت إلى تحليل الكيفية التي تعزز بها قدرات الذكاء الاصطناعي (AI) كقدرات ديناميكية عمليات إدارة مخاطر الأمن السيبراني في سلاسل الإمداد (SCCRM)، اعتمدت الدراسة على المنهج الكيفي الاستكشافي عبر استراتيجية دراسة حالة متعددة شملت 24 مقابلة معمقة مع خبراء تقنيين واستشاريين، استغرقت فترة الدراسة الميدانية وجمع البيانات ومعالجتها مدة زمنية ممتدة (2025/ 2026)، وتم التوصل للنتائج التالية:

- الذكاء الاصطناعي يكتشف التهديدات السيبرانية المعقدة أسرع من الأنظمة التقليدية.
- تؤدي أتمتة الأمن الرقمي إلى تقليل الأخطاء البشرية و رفع كفاءة أداء المؤسسة.
- أكدت الدراسة أن نجاح هذه الأنظمة يعتمد بشكل كبير على جودة وحكمة البيانات.

8) دراسة (Anurag, 2025)

مقال بعنوان: سلاسل التوريد الرقمية والأمن السيبراني– استراتيجيات الحماية وتخفيف المخاطر– قسم المعلومات التطبيقية، كلية غورو كريبا، الهند، عدد 13 إصدار 1، 2025، صفحات 10–18.

هدفت هذه الدراسة إلى استقصاء تقاطع سلسلة التوريد مع الأمن السيبراني، والتركيز على الصعوبات الناتجة عن التحول الرقمي وعرض تحليل معمق للإستراتيجيات الكفوءة لتخفيف المخاطر وحماية البيانات، وتم استخدام المنهج الوصفي التحليل من خلال تدقيق متكامل للأدبيات العلمية والتقنيات الناشئة، والأدوات التي اعتمدها الدراسة للبحث هي كل من المسح المرجعي والتحليل النوعي للتقارير التقنية وإطارات العمل الأمنية المتقدمة، بينما تمثلت عينة الدراسة في تحليل أنماط شبكات التوريد العالمية المتصلة بانترنت الأشياء(IoT) الأنظمة المعتمدة على البلوكشين والحوسبة السحابية، فتصلت هذه الدراسة إلى النتائج التالية:

- يؤمن البلوكشين السجلات من التلاعب من خلال ضمان المصداقية والشفافية لحركة السلع عبر مراحل التوريد المتعددة.
- إن تقنيات الذكاء الإصطناعي في الكشف الاستباقي للتهديدات عبر تدقيق وتحليل الأنماط غير المألوفة في تدفق البيانات.
- تؤكد الدراسة على ضرورة الإعتماد على التشفير ما بعد الكم لتأمين البيانات الحساسة.

9)دراسة (Boyes, 2025)

مقال بعنوان: الأمن السيبراني وسلاسل التوريد ذات المرونة السيبرانية– قسم الهندسة، جامعة كارلتون، المملكة المتحدة، أفريل 2025، عدد 5، إصدار 4، صفحات 28–34.

هدفت إلى استكشاف قضايا المرونة السيبرانية في سلسلة التوريد، تم الاعتماد على المنهج الوصفي التحليلي المبني على مراجعة الأدبيات النظرية، واستعانت الدراسة بتحليل المحتوى وسداسي باركيريان كأدوات للبحث، احتوت العينة على تحليل حوادث اختراق فعلية بالإضافة على أنظمة فيزيائية سيبرانية في الفترة الزمنية لأبريل 2015، وأجري تحليل البيانات بواسطة التحليل النوعي الاستنتاجي لوصل التهديدات بالنقاط الهشة، والنتائج المتوصل إليها كالتالي:

- إلزامية تبني نماذج أمنية شاملة تتعدى السرية لتشمل الفائدة.
- نقاط الاتصال مع الموردين الخارجيين تعد من أبرز الثغرات حرجا في سلسلة التوريد.
- يستلزم الأمن السيبراني نهج شامل يكامل بين العمليات والأفراد والانظمة.

10) دراسة (Hlynskyy, Dovhun, & Pochopień, 2025)

مقال بعنوان: الرقمنة والأمن السيبراني في الشركات وسلاسل التوريد – التحديات والفرص– قسم الإدارة والأعمال ، جامعة لفيف للفنون التطبيقية، أوكرانيا، 2025، عدد 29 إصدار 1، صفحات 53–59.

هدفت هذه الدراسة إلى تحليل واقع الأمن السيبراني والرقمنة في الشركات وسلاسل التوريد، ورصد التحديات والفرص المرتبطة بها لتعزيز المرونة السيبرانية لمجابهة التهديدات الرقمية المتصاعدة، وتم استخدام المنهج الوصفي التحليلي، بحيث جمعت البيانات الأولية بواسطة دراسة مسحية (استبيان) احتوت عينة مكونة من 60 شركة تنشط في قطاعات اقتصادية متنوعة (النقل، اللوجستيك، تكنولوجيا المعلومات، الطاقة، والتسويق) خلال الفترة الزمنية الممتدة من جانفي إلى فيفري 2024، وتم استخدام أسلوب تحليل البيانات الإحصائية والمصادر العلمية لتعزيز دقة النتائج المتوصل إليها، والتي هي كالتالي:

- الأمن السيبراني أولوية استراتيجية لـــ 49% من المنظمات الأوروبية، بالأخص في مجال حماية سلسلة التوريد من الاختراقات الرقمية والبيانية.
- بينت النتائج مستويات عالية من التحول الرقمي في الشركات التي شملها البحث، وبلغت نسبة الرقمنة العالية 63.3%، وبلغت نسبة الرقمنة العالية جدا 23.3.%
- إن أكثر التدابير الفعالية في الأمن السيبراني المستخدمة في المؤسسات هي: جدران الحماية بنسبة تقدر73.3%، برامج مكافحة الفيروسات 71.7 %، ثم أنظمة مراقبة الشبكات 68%.
- أهم التحديات التي تعرقل تأمين سلاسل التوريد سيبيرانيا: افتقار للخبرات الكافية والموظفين المؤهلين 66.7 %، القيود المالية 51.7 %، تقص البرامج التدريب وتوعية الموظفين.

11) دراسة (Dr. Pushpendu, 2024)

مقال بعنوان: أثر مقاييس الأمن السيبراني المعتمدة من قبل مؤسسات إدارة سلسلة التوريد في نافي مومباي– مجلة التكنولوجيا الناشئة والبحوث الابتكارية ، الهند، جوان 2024 عدد 11 إصدار 6، صفحات ب 10 – ب 17.

هدفت هذه الدراسة إلى فهم كيفية تأثير تدابير الأمن السيبراني على كفاءة إدارة سلاسل التوريد في نافي مومباي بالهند، تعيين المخاطر السيبرانية الناشئة وتأثيرها على العمليات اللوجستية، تم استخدام المنهج الوصفي التحليلي باستخدام أسلوب البحث النوعي، واعتمد في جمع بياناته إلى المراجعة المنهجية للتقارير الصناعية والبيانات الثانوية المتعلقة بالمؤسسات اللوجستية في المنطقة المستهدفة، وضمت عينة الدراسة قطاع مؤسسات إدارة سلاسل التوريد التي في منطقة نافي مومباي في الهند، بينما الفترة الزمنية، حيث ركزت جهودها على تحليل البيانات

والتهديدات السيبرانية المسجلة في المرحلة بعد الجائحة(2021، 2022، 2023)، حيث قدمت تصور حديث لتطور الهجمات السيبرانية، ومن خلالها قدمت النتائج التالية:

- أظهرت أن هناك علاقة طردية بين الاستثمار في الأمن السيبراني ومرونة سلسلة التوريد في كفاءتها على الاستجابة على الأزمات التقنية.

- إلزامية دمج بروتوكولات الأمن السيبراني في جوهر العمليات اللوجيستية اليومية دون التعامل معها كإجراء ثانوي.

- أبرزت الدراسة بأن السلوك التنظيمي والمورد البشري هما الحلقة الهشة في نظام الأمن السيبراني، لأن أغلب الاختراقات سببها نقص الوعي الأمني لكل الموظفين.

12) دراسة (Constance, Okpala, & Nkemakonam , 2024)

مقال بعنوان: تعزيز سلاسل التوريد التصنيع الذكية من خلال تدابير الأمن السيبراني– المجلة الدولية للاختراعات الهندسية (IJEI)، نيجيريا، ديسمبر 2024، عدد 13 إصدار 12، صفحات 01-06.

هدفت الدراسة لتحليل الدور المحوري للأمن السيبراني في تأمين سلسلة التوريد التصنيع الذكي، مع ايلاء اهتمام خاص على دمج تقنيات انترنت الأشياء (IoT)، سلاسل الكتل (Block Chain)، الذكاء الاصطناعي لمواجهة الهجمات الرقمية المتصاعدة، وتم استخدام المنهج الوصفي التحليلي استنادا إلى إجراء مراجعة أدبية ومنهجية تضم الأدبيات العلمية والأطر التقنية المعاصرة، حرصا على تقديم استراتيجيات دفاعية استباقية تحتوي على مرونة الأنظمة اللوجستية في 4.0، تكونت الدراسة من قطاع أنظمة التصنيع الذكي والعمليات اللوجيستية الرقمية ذات الصلة بها، ركزت جهود الدراسة في استقراء البيانات وتحليلها على الاهتمام بالتهديد السيبراني والتطور التقني الموثق في الفترة الزمنية من سنة 2018 إلى غاية سنة 2024 ، وكانت أهم النتائج المتوصل إليها من خلال هذه الدراسة كالتالي:

- أكدت الدراسة بأن إدماج الذكاء الاصطناعي يساهم بفاعلية في إكتشاف التهديدات بشكل مبكر من خلال تحليل البيانات اللوجستية الهائلة في الوقت الفعلي.
- توصلت الدراسة إلى أن انترنت الأشياء ساهمت في رفع سطح الهجوم، بحيث أن أصبحت سلسلة التوريد أكثر عرضة للتجسس الصناعي والهجمات.
- شددت الدراسة على المخاطر المترتبة عن الطرف الثالث تعتبر ضعف جوهري، بحيث أي ضعف أمني سيبيراني مورد واحد فقط قد يترتب عليه تعطيل المنظومة اللوجيستية كليا.

13)دراسة (Fahed Al-Khatib, Yousef Ibrahim, & Alnadi, 2024)

مقال بعنوان: ممارسات الأمن السيبراني وأداء سلسلة التوريد: حالة البنوك الأردنية _قسم إدارة الأعمال؛ كلية الأعمال؛ جامعة فيلادلفيا؛ المملكة الأردنية الهاشمية؛ العدد 1؛ الرقم 24 ؛2025.

هدفت هذه الدراسة إلى تحليل أثر ممارسات الأمن السيبراني كمتغير مستقل بأبعاده الثلاثة (السرية، السلامة، والتوافر) على أداء سلسلة التوريد كمتغير تابع في القطاع المصرفي الأردني. تم اتباع المنهج الوصفي التحليلي، حيث أجريت الدراسة الميدانية خلال الفترة الممتدة من أكتوبر 2024 إلى ديسمبر 2024، وشملت العينة 290 مستجيباً؛ جُمعت البيانات بواسطة استبيان إلكتروني خضع لاختبارات الصدق والثبات، بينما تمت المعالجة الإحصائية باستخدام برنامج SPSS.وتم التوصل للنتائج التالية

- أثبتت الدراسة وجود أثر إيجابي ذو دلالة إحصائية لممارسات الأمن السيبراني على أداء سلسلة التوريد المصرفية مما يساهم في تعزيز مرونة العمليات وجودتها.
- دعت الدراسة إلى ضرورة الاستثمار في تدريب الموظفين وتحديث أنظمة التشفير لضمان أمن المعلومات المصرفية وحماية سلاسل التوريد من التهديدات السيبرانية المتزايدة.

14) دراسة (Boyens, et al., 2024)

مقال بعنوان: ممارسات إدارة مخاطر سلاسل التوريد للأمن السيبراني للأنظمة والمنظمات– المعهد الوطني للمعايير والتكنولوجيا، وزارة التجارة الأمريكية، الولايات المتحدة الأمريكية، 2024.

هدفت الدراسة إلى طرح توجيهات تقنية واستراتيجية للمؤسسات حول كيفية إدارة مخاطر الأمن السيبراني خلال مراحل سلسلة التوريد، وتم استخدام المنهج الوصفي التحليلي التطوري، والأدوات المستخدمة في هذه الدراسة هي تحليل النظم وتكامل معايير الأمن الدولية، بحيث اهتمت بتطوير أطر العمل الخاصة بحماية تكنولوجيا المعلومات والاتصالات لغاية نوفمبر 2024، وحللت البيانات بأسلوب النمذجة الهيكلية لهجمات والمخاطر وتعيين الثغرات، والنتائج المتوصل لها كانت كالتالي:

- ضرورة انشاء قنوات خاصة لتبادل معلومات الهجمات السيبرانية لزيادة مستوى الحماية الجماعية بين جميع الفاعلين في سلسلة التوريد.
- إلزامية تبني نهج تقييم المخاطر المعتمد على دورة الحياة للحرص على أمن وسلامة المنتجات منذ التصميم إلى غاية التشغيل.
- أشارت الدراسة بزيادة مخاطر الموردين والأطراف الثالثة وهذا ما يستوجب فرض رقابة صارمة للتحقق المستمر من الأمني.

15) دراسة (Sylwi & Zbigniew, 2024)

مقال بعنوان: الهجمات السيبرانية كالتهديد في سلسلة التوريد– قسم المنطق الدولي، جامعة بوزنان للاقتصاد والأعمال، بولندا،2024، عدد 27، إصدار 3، صفحات 778-796.

هدفت الدراسة إلى تقصي طريقة تقييم التهديدات السيبرانية في سلسلة التوريد، مع إعطاء أهمية لتقييم المنفعة من خرائط التهديدات كأدوات لهذا الغرض، وتم استخدام المنهج الوصفي التحليلي بواسطة إجراء تحليل ببلومتري لبيانات قاعدة خاصة بالأبحاث الموثقة خلال الفترة الزمنية من 2019-2024، وتم الاعتماد على المسح المرجعي للبيانات الثانوية (statista) ودراسة استطلاعية بواسطة أداة خرائط التهديد كأدوات للبحث، وحللت البيانات نوعيا للوصل بين أنواع الهجمات بمدى تأثير القطاعات الإقتصادية، وكانت النتائج المتوصل إليها كالتالي:

- تنعكس الهجمات السيبرانية على سمعة المؤسسات، وتدفق بياناتها ومرونة عملياتها اللوجيستية بشكل مباشر.
- إلزامية تحسين النماذج الإدارية لتقييم الهجمات والمخاطر السيبرانية.
- توصلت الدراسة إلى أن البيانات التي توفرها خرائط التهديد متضاربة، وبتالي تصبح أدوات غير شاملة لرصد الحوادث الفعلية بشكل كلي.

16) دراسة. (Valentina Clavijo Mesa, Elena Patino-Rodriguez, & Jesus Guevara Carazas, 2024)

مقال بعنوان: الأمن السيبراني في المجال البحري :مراجعة مرجعية لأثار الهجمات السيبرانية و اليات الدفاع في سلاسل التوريد البحرية _قسم الهندسة الصناعية ،كلية الهندسة الميكانيكية بالجامعة الوطنية كولومبيا؛ عدد 11؛ الرقم 15؛ 2024.

هدفت الدراسة إلى معرفة المخاطر السيبرانية في سلاسل التوريد البحرية وتطوير تصنيف علمي للهجمات باستخدام المنهج الوصفي التحليلي (أسلوب المراجعة المنهجية لـــ 110 دراسة محكمة)، وغطت الفترة الزمنية ما بين (2024/2011) وتلخصت أهم نتائجها في:

- تضاعف التهديدات السيبرانية (مثل هجمات DDoS والانتحال) نتيجة تسارع التحول الرقمي وتقنيات الصناعة 4.0.
- ضرورة تبني استراتيجيات دفاعية استباقية وبرامج تدريبية متخصصة لرفع الوعي الأمني لدى العنصر البشري.
- حتمية الامتثال للأطر الدولية (مثل معايير NIST) لضمان تكامل أمن الشبكات اللوجستية والقدرة على التعافي.

17) دراسة (Sadiku, Chukwu, & Sadiku, 2023)

مقال بعنوان: الأمن التوريد– قسم الهندسة الكهربائية وهندسة الحاسوب، جامعة برايري فيو أيه اند إم، الولايات المتحدة الأمريكية.

هدفت هذه الدراسة لتقديم إطار نظري كامل حول الأمن السيبراني في سلاسل التوريد، مع تسليط الضوء على أمن تدفق المعلومات، المنتجات، والخدمات من المؤسسة للمستهلك النهائي ضد الاختراقات الرقمية المتزايدة، وتم استخدام المنهج الوصفي التحليلي من خلال مراجعة الأدبيات العلمية المنشورة، وتم الاستعراض للممكونات الرئيسية لأمن سلاسل التوريد بما في ذلك البرمجيات، الشبكات ،أنظمة تكنولوجيا المعلومات، بالإضافة على تحليل المخاطر السيبرانية الناتجة عن التعقيد الشديد لسلسلة التوريد، ومنه النتائج التي توصلت إليهم الدراسة كالتالي:

- سلسلة التوريد هي أبرز الأهداف الجذابة للهجمات السيبرانية لكونها تتيح منافذ دخول متعددة للمهاجمين من خلال الشركاء الخارجيين والموردين.
- الأمن السيبراني خيار استراتيجي لا غنى عنه لضمان استمرارية العمليات في هذا العصر الرقمي.
- إن أبرز تحديات الأمن السيبراني داخل سلسلة التوريد يكمن في ضعف الرؤية الشاملة للعمليات، بالإضافة إلى الاعتماد المتزايد على الأنظمة المترابطة التي ترفع من احتمالية التعرض للاختراقات.
- استنتجت هذه الدراسة أن ضم الذكاء الإصطناعي وأنترنت الأشياء هو عنصر جوهري فعال لتحديث أنظمة مؤهلة للتنبؤ بالهجمات السيبرانية وتسييرها بكفاءة.

18) دراسة (Solfa, 2022)

مقال بعنوان: تأثير الأمن السيبراني ومخاطر سلسلة التوريد على العمليات الرقمية: أدلة من صناعة الأدوية في الإمارات العربية المتحدة– جامعة لابلاتا الوطنية، الأرجنتين، 2022، عدد 2، إصدار 2، صفحات 18–31.

هدفت الدراسة إلى قياس أثر الأمن السيبراني ومخاطر سلاسل التوريد على العمليات الرقمية في مجال صناعة الأدوية في الإمارات، وتم استخدام المنهج الوصفي التحليلي ذو التصميم الاستنباطي، والأدوات التي استخدمت في الدراسة هي الاستبيان، وضمت العينة 243 موظف من أصل14 شركة لتصنيع الأدوية خلال سنة 2022. وتمت معالجة البيانات بأسلوب التحليل الإحصائي أي الارتباط والانحدار، وتوصلت للنتائج التالية:

- إلزامية تعزيز التحول الرقمي داخل المؤسسات التي تعتمد على العملاء لرفع قدرتها على إدارة الموردين بآمان.
- تبين أن هناك ارتباط إجابي معنوي ذو دلالة إحصائية مابين كفاءة العمليات الرقمية ومستوى الأمن السيبراني.

- أوضحت النتائج المتوصل إليها إلى أن الإستثمار في البنية التحتية السيبيراينة يحد من احتمالية انقطاع سلسلة االتوريد الدوائية.

19) دراسة: (Mohd, Nurul , Nik , & Zuraimi , 2021)

مقال بعنوان: الأمن السيبراني في إدارة سلاسل التوريد: مراجعة منهجية، قسم إدارة الأعمال، جامعة ماليزيا كيلانتان، ماليزيا، 2021، عدد 17 إصدار 1، صفحات 49-57.

هدفت هذه الدراسة إلى مراجعة مكتبية شاملة ومنهجية للأدبيات السابقة للأمن السيبراني في إدارة سلاسل التوريد، لتحديد الثغرات البحثية في هذا المجال، وتم استخدام المنهج الوصفي التحليلي بواسطة أسلوب المراجعة المنهجية (Systematic Literature Review)، وفق بروتكول PRISMA، وضمت الدراسة تحليل وفحص المقالات العلمية المنشورة في قواعد البيانات العالمية (Scopus Science ,Web of) خلال الفترة الممتدة من سنة 2011 إلى غاية 2020، وتم استخدام أسلوب تحليل لتصنيف المواضيع الأكثر بحثا، والنتائج التي توصلت لها هذه الدراسة:

- أكدت النتائج أن أغلب الأبحاث التي ركزت على تكنولوجيا المعلومات بأنها أداة تأمين بنسبة 25%، وإدارة الأمن السيبراني بنسبة 20%، وهو ما يستوجب لتوازن أكبر بين الجانب الإداري والتقني.
- تم التوصل إلى أن هناك فجوة في الدراسات التي تدرس الأمن السيبراني ومرونة سلسلة التوريد في صد الأزمات، مما يجب تكثيف البحوث .
- أبرزت الدراسة بأن حماية سلسلة التوريد تتصف بالتعقيد نظرا لتعدد الأطراف الفاعلة، وما يستوجب اعتماد حلول تكنولوجيا متقدمة (كالذكاء الاصطناعي وانترنت الأشياء) لإستمرارية سلسلة التوريد.

20) دراسة (Abhijeet, Maximilian, Nigel, & Richard, 2020)

مقال بعنوان: إدارة المخاطر السيبرانية في سلسلة التوريد : مراجعة وأجندة بحثية– مركز إدارة اللوجستيات وسلسلة التوريد، جامعة هيريوت وات، المملكة المتحدة، 2020، عدد 25، إصدار 2، صفحات 223-240.

هدفت الدراسة إلى تحليل طبيعة المخاطر السيبرانية في سلسلة التوريد وإيضاح إطار عمل كامل لإدارتها، وتم استخدام المنهج الوصفي التحليلي المبني على المراجعة المنهجية للأدبيات، ومن أدوات البحث المعتمدة في البحث: المسح الببليوغرافي وتحليل 113 مقال علمي من قواعد بيانات عالمية، لفترة زمنية ممتدة ما بين 2000 إلى غاية 2019، وحللت البيانات بواسطة الأسلوب التحليلي الموضوعي والاستنباطي، وكانت نتائج الدراسة كالتالي:

- العمل على تطوير المرونة السيبرانية لأنها تضمن استعادة نشاط سلسلة التوريد بشكل أسرع بعد الوقوع الفعلي للهجمات.

- إلزامية الانتقال من النهج التقني البحت والتحول إلى نهج جداري شامل يشرك جميع المؤسسات في سلسلة التوريد.
- أظهرت هذه الدراسة ثلاث أبعاد رئيسية للتهديدات والمخاطر السيبرانية في سلسلة التوريد: مخاطر سمعة المؤسسة، المخاطر الاستراتيجية، المخاطر التشغيلية.

الفرع الأول: مقارنة بين الدراسات الحالية والدراسات السابقة

استنادا إلى القيمة المعرفية المستخلصة من الدراسات السابقة التي تم عرضها، سنحاول إبراز أهم الفروقات وجوانب التشابه بينها وبين الدراسة الحالية، بالإضافة إلى استعراض ما قدمته من إثراء ودعم الدراسة الحالية، وذلك على النحو التالي:

من حيث الهدف: تباينت أهداف الدراسات السابقة إذ ركّزت بعض الدراسات على الجوانب التقنية فقط للأمن السيبراني، في حين هدفت دراسات أخرى إلى تحليل واقع الأمن السيبراني بصفة عامة، بينما أولت دراسات أخرى اهتمامًا ببناء أطر نظرية لإدارة المخاطر، أمّا الدراسة الحالية فقد سعت إلى الإحاطة بمختلف هذه الجوانب مجتمعة، فضلًا عن التطرّق إلى أثر الأمن السيبراني على أداء وفعالية سلسلة التوريد ميدانيًا.

من حيث العينة والمجتمع: اختلفت العينة من دراسة لأخرى، هناك من اعتمدت كعينة لها مؤسسات التصنيع الذكي، ومنها من استهدفت قطاع الأدوية وبعض الدراسات اختارت عينات مختلفة القطاعات، أما الدراسة الحالية فقد استهدفت عينة من موظفي قسم اللوجستيك والأمن السيبراني في المؤسسات محل الدراسة.

من حيث متغيرات الدراسة: تناولت معظم الدراسات السابقة تحليل متغيرات الأمن السيبراني بناء على نماذج تقنية متنوعة، في حين قامت دراسات اخرى بدارسة أبعاد تخفيف المخاطر، بينما تميزت الدراسة الحالية بربطها بين متغير الأمن السيبراني وفعالية الأداء لسلاسل التوريد.

من حيث زمن ومكان الدراسة: اختلفت الدراسات السابقة من حيث البعد الزمني، إذ انجزت بعض الدراسات بعد جائحة كوفيد-19، في حين أُجريت دراسات أخرى قبل أزمة سلسلة التوريد العالمية، وعلى خلاف ذلك فان الدراسة الحالية تُجرى خلال السداسي الأول من سنة 2026، بهدف تحليل أثر الأمن السيبراني على سلسلة التوريد، أمّا من حيث البعد المكاني فقد تنوّعت الدراسات السابقة بين دول آسيوية وأوروبية، في حين تركّز الدراسة الحالية على البيئة الجزائرية.

من حيث القطاع: احتوت الدراسات السابقة مجموعة من القطاعات (الطبية، التقنية، الصناعية، الخدماتية)، وهو حال دراستنا الحالية كل المؤسسات عينة الدراسة مؤسسات اقتصادية في قطاعات مختلفة.

من حيث أداة الدرلسة والمعالجة الإحصائية: تتشابه الدرلسات السابقة مع الدرلسة الحالية في أدوات البحث، حيث يُعدّ الاستبيان الأداة الرئيسية لجمع البيانات وتُعالج البيانات بلستخدام برنامجSPSS من خلال تطبيق الاختبارات الإحصائية المناسبة لتحديد طبيعة العلاقات بين المتغيرات.

وبالتالي يمكننا التأكيد على أن تم اختيار الدراسات السابقة بعناية عالية، بما يحقق على نحو يضمن تلاؤمها مع أهداف درلستنا ودورها في الإحاطة بأبعاد الموضوع، بحيث يظهر بشكل ملحوظ التقاطع الذي بينها وبين الدراسة الحالية، بالأخص على مستوى الهدف، أيا كان بشكل كلي أو جزئي، بينما تمحورت جميعها ضمن مجال الأمن السيبراني وسلاسل التوريد، مع ذلك أظهرت مختلف الدراسات تطابق ملحوظ لأدوات جمع البيانات من استبيان الذي يتصف بسهولة التطبيق، والأبرز من ذلك بانها درست الأمن السيبراني كخيار إستراتيجي لصد الهجمات الرقمية المتزايدة.

الفرع الثاني: مجال الاستفادة من الدراسات السابقة: اعتمادًا على مراجعة الدراسات السابقة، تم تحديد مجموعة من النقاط التي أسهمت في بناء مجال الاستفادة، والتي تمثّلت فيما يلي:

- أمّنت الدراسات السابقة دعمًا معرفيًا للدراسة الحالية، عبر إتاحة الاطلاع على الموضوع من زوايا تحليلية متعددة ومتمايزة.
- الاستعانة بالدراسات السابقة كمصادر أساسية لإثراء الإطار الجانب النظري بالمعارف العلمية الراهنة.
- لسهمت الدرلسات السابقة بشكل فعّال في تحديد المتغيرات محلّ الدرلسة، والتي تم اعتمادها كمنطلق أساسي للدراسة الحالية.
- إن إنشاء نموذج لستشرافي لأمن سلسلة التوريد في إطار التقنيات الحديثة (مثل الذكاء الاصطناعي)، من شأنه أن يُسهم في تعزيز مرونة الاستجابة اللوجستية، وهذه الأخيرة تُعدّ عاملًا حاسمًا في تحسين أداء سلسلة التوريد.
- تُسهم الدراسات السابقة في دعم النتائج المتوصل إليها، كونها تمثل مرجعًا تُقارن من خلاله نتائج الدراسة الحالية بالنتائج السابق.

على إثر ذلك وعند مقارنة الدراسات السابقة، تبيّن وجود فجوة بحثية سعت الدراسة الحالية إلى معالجتها، حيث ركّزت معظم الدراسات السابقة على الجوانب التقنية فقط للأمن السيبراني، في حين تميّزت هذه الدراسة بالربط المباشر بين الأمن السيبراني واستمرارية سلسلة التوريد، كما تتجلّى خصوصية الدرلسة الحالية في إسقاط هذه المفاهيم على واقع المؤسسات وهو ما يُمثّل إضافةً نوعيةً للمكتبة الأكاديمية، من خلال تعزيز الدراسات الميدانية الحديثة التي تتناول أثر الهجمات الرقمية على مرونة واستمرارية سلسلة التوريد.

خلاصة الفصل

تم التطرق في هذا الفصل إلى كل ما يتعلق بمتغيرات الدراسة من أدبيات نظرية وتطبيقية، حيث استعرض في بدايته مبحث خاص بالإطار المفاهيمي للدراسة، بدأنا بمتغير الأمن السيبراني من ناحية المفهوم والأهمية وأبعاده الأساسية، كما تم التطرق لمتغير سلاسل التوريد اعتمادا على ضبط المفاهيم وعرض أهميته ومراحل نشأته، وصولا إلى الأبعاد التي تبرز أدائها وفعاليتها في ظل التحديات الراهنة، إضافة إلى الإجراءات التي تعزز مرونة واستمرارية سلسلة التوريد.

وفيما يتعلق بالدراسات السابقة تم التطرق إليها وإبرازها في المبحث الثاني، حيث توضح لنا وجود حرص متزايد من طرف الباحثين بدراسة تقاطعات الأمن السيبراني مع كفاءة أداء العمليات اللوجستية، وكما يتضح تنوع المجالات واختلافها من دراسة لأخرى، ومع هذا التنوع أثبت وجود علاقة تأثيرية وترابطية بين متغيرات الدراسة، وهو ما يشكل إضافة مميزة لمكتبة الأكاديمية تصبو لإثراء الرصيد المعرفي بدراسات ميدانية حديثة، والتي سوف تختبر ميدانيا من خلال الدراسة التطبيقية في الفصل الثاني.

الفصل الثاني

أثر الأمن السيبراني على تحسين أداء سلاسل التوريد لعينة من المؤسسات الجزائرية

تمهيد:

بعد الإحاطة بالأدبيات النظرية والتطبيقية لمفاهيم الأمن السيبراني وسلاسل التوريد، وتحليل الأطر الفكرية الناظمة للعلاقة بين الأمن السيبراني وتحسين كفاءة سلاسل التوريد، واستناداً إلى ما خلصت إليه الدراسات السابقة في هذا المجال؛ تأتي هذه الدراسة الميدانية لاستكمال الجانب التطبيقي. تهدف الدراسة إلى قياس أثر آليات الأمن السيبراني في عينة من المؤسسات (عمومية، خاصة وأجنبية) بمختلف أحجامها، وتقييم دورها الجوهري في تحصين سلاسل التوريد ضد الأزمات الرقمية وضمان استمرارية أدائها. وسنفصل في ذلك من خلال المبحثين التاليين:

المبحث الأول: الطريقة وأدوات الدراسة

المبحث الثاني: مناقشة نتائج الدراسة ومقارنتها مع نتائج الدراسات السابقة

المبحث الأول: الطريقة والأدوات

يعتبر هذا المبحث مدخلا إلى الدراسة الميدانية لأثر الأمن السيبراني على تحسين أداء سلاسل التوريد، حيث سيتم عرض المنهج المتبع ومجتمع وعينة الدراسة وأدوات جمع المعلومات، إضافة إلى مختلف البرامج والأدوات والأساليب الإحصائية التي تم من خلالها التوصل إلى نتائج الدراسة.

المطلب الأول: مجتمع وعينة الدراسة

سنتناول في هذا المطلب عرض للطريقة المتبعة في الدراسة من خلال التعرف على المنهج المتبع من توضيح أسلوب الدراسة، مجتمع الدراسة وعينة الدراسة ومختلف الأدوات الإحصائية المستعملة

الفرع الأول: مجتمع الدراسة

تمثل مجتمع الدراسة في مؤسسات (عمومية، خاصة وأجنبية) بمختلف أحجامها، أين تم استهداف فئة مسئولي وموظفي المؤسسات محل المناقشة، بصفتهم الأقرب لمعرفة المعايير المعمول بها داخل المؤسسة سواء من جانب الأمن السيبراني أم من الجانب اللوجستي، اشتملت عينة الدراسة على عدة مؤسسات منها مؤسسات عمومية مثل: ALGERIE TELECOM، ENAFOR، SARPI، ENAC، Direction des Équipements Publics

ومؤسسات خاصة: BAYAT CATERING،

إضافة لمؤسسات أجنبية: Halliburton،

أولا: المؤسسات العمومية (Secteur Public)

1. **اتصالات الجزائر (ALGERIE TELECOM)**: تأسست بموجب قانون خصخصة قطاع البريد والمواصلات سنة 2002 كشركة أسهم (SPA) مملوكة للدولة. تعد الفاعل الأساسي في قطاع الاتصالات بالجزائر، حيث تتولى إدارة وتطوير الشبكة الوطنية للاتصالات والإنترنت. تلعب دوراً محورياً في توفير البنية التحتية الرقمية، مما يجعلها ركيزة أساسية عند دراسة حماية تدفق البيانات. (Algeria Telecom, 2026)
2. **المؤسسة الوطنية للتنقيب (ENAFOR)**: هي شركة فرعية تابعة لمجمع سوناطراك بنسبة 100%، تأسست عام 1966 واستقلت كفرع في 1981، مقرها الاجتماعي بحاسي مسعود (ولاية ورقلة). تختص في حفر وصيانة الآبار النفطية والغازية. تدير سلاسل التوريد لوجستية معقدة تتطلب حماية سيبرانية عالية نظراً لحساسية العمليات الميدانية والبيانات. (ENAFOR, 2026) (ENAC, 2026)
3. **المؤسسة الوطنية للقنوات (ENAC)**: تأسست عام 1978، وهي فرع مملوك بالكامل لمجمع سوناطراك. تتخصص في هندسة وبناء خطوط أنابيب نقل المحروقات (Pipelines) والمنشآت التابعة لها. تمثل نموذجاً للمؤسسات التي تعتمد على أنظمة رقمية لمراقبة تدفق الإمدادات عبر مسافات جغرافية شاسعة.

4. **الشركة الجزائرية لإنجاز المشاريع الصناعية (SARPI) :تأسست** عام 1992 كشركة مختلطة، وهي حالياً مملوكة بالكامل لمجمع سوناطراك. تختص في الهندسة والمشتريات والبناء (EPC) والصيانة الصناعية الكبرى. تدير عمليات توريد دولية واسعة لتأمين المعدات الحساسة، وتعتمد على أنظمة إدارة متكاملة (ERP) لتنسيق مشاريعها الصناعية الضخمة. (SARPI, 2026)

5. **مديرية التجهيزات العمومية لولاية ورقلة (Direction des Équipements Publics – DEP)**: هيئة إدارية تابعة لوزارة السكن والعمران والمدينة، وتعمل تحت وصاية ولاية ورقلة. تتولى مهام الإشراف والمتابعة لإنجاز المشاريع العمومية الكبرى في الولاية. تعتمد المديرية على الرقمنة في إدارة الصفقات العمومية ومتابعة وتيرة الإنجاز مع المقاولين، مما يجعل أمن معلوماتها جزءاً لا يتجزأ من كفاءة أدائها الإداري. (MHUV, 2026)

ثانيا: المؤسسات الأجنبية

1. **شركة هاليبرتون (Halliburton)**: شركة عالمية أمريكية وتعد من كبرى شركات الخدمات النفطية في العالم. تنشط في الجزائر كقطاع أجنبي خاص، وتقدم حلولاً تكنولوجية متقدمة لقطاع الطاقة. تتميز بسلسلة توريد عالمية وتطبق معايير صارمة لتأمين بياناتها وعملياتها الميدانية، مما يجعلها مرجعاً للممارسات التكنولوجية العالمية. (halliburton, 2026)

ثالثا: المؤسسات الخاصة

1. **مؤسسة بايات للإطعام (Bayat Catering)**: شركة جزائرية خاصة (SPA) رائدة في خدمات الفندقة والإطعام والتموين للمواقع النفطية والصناعية (Base de Vie). تعتمد في أدائها على سلسلة توريد لوجستية مكثفة تشمل توريد المواد الغذائية والخدماتية وتوزيعها في بيئات صحراوية صعبة، وتوظف الحلول الرقمية في إدارة المخازن والطلبيات. (Bayat Catering, 2026)

عينة الدراسة

أجريت الدراسة الحالية على عينة عشوائية من مجتمع الدراسة وهم الموظفين بالمؤسسات العمومية والخاصة والأجنبية عينة الدراسة أي الموظفين والمسؤولين بهذه المؤسسات على اختلاف درجاتهم، وقد تم توزيع 100 إستبيانا إلكترونيا، وتم استرجاعها كاملة، وبالتالي تم معالجة 100 استبيانا وهي العينة النهائية التي طبقت عليها الدراسة، والجدول التالي يوضح توزيع الاستبيانات.

جدول رقم (4): احصائيات الاستبيانات الموزعة والصالحة

	الموزعة	المسترجعة	الملغاة	الصالحة
العدد	100	100	0	100
النسبة المئوية	%100	%100	% 0	% 100

المصدر: من اعداد الطالبتين

متغيرات الدراسة

ومن خلال موضوع البحث قمنا بتحديد المتغير التابع والمتغير المستقل وكل المتغيرات تم الاعتماد في تحليلهما على معطيات المؤسسات محل الدراسة ويمكن توضيحها في الجدول التالي:

جدول رقم (5): يوضح متغيرات الدراسة

المتغيرات		الأبعاد
المتغير المستقل	الأمن السيبراني	البعد التنظيمي
		البعد التقني
		البعد البشري
		البعد التعاوني
المتغير التابع	سلاسل التوريد	الكفاءة التشغيلية
		جودة الخدمة ورضا العملاء
		بعد الاستمرارية

المصدر: من اعداد الطالبتين

الفرع الثاني: منهج الدراسة ومصادر جمع البيانات

أولا: منهج الدراسة

من أجل تحقيق أهداف الدراسة وللإجابة على الإشكالية المطروحة، وجب اختيار منهج يحدد الخطوات التي يتبعها الباحثين من أجل الوصول إلى الغاية التي بني من أجلها البحث ونظرا لطبيعة موضوع هذه الدراسة قمنا باستخدام المنهج الوصفي التحليلي لتوضيح مدى تبني المؤسسات لمفهوم الأمن السيبراني في تحسين أداء سلاسل التوريد، وهو ما يتلاءم مع أغراض الدراسة، لأنه يعتبر الأسلوب الأنسب للدراسة.

ويعرف هذا المنهج بأنه يعطي وصف وتفسير علمي منظم للظاهرة المدروسة ويجسد الواقع كما هو، حيث يعمل على توفير فرص للحصول على أكبر حصيلة من المعلومات مما يسهل الوصول إلى نتائج واضحة وذات مصداقية عالية

ثانيا: مصادر جمع البيانات

البيانات المختلطة بالدراسة تم الاعتماد على مصدرين أساسيين هما:

1. **المصادر الثانوية:** لإثراء الجانب المفاهيمي في الجزء النظري للدراسة، اعتمدنا على المصادر الثانوية المتمثلة في المقالات الأجنبية، إلا انه من الدراسات التي نعتبرها دراسات مرجعية هي الدراسات التالية دراسة ياسمين عفيفي مراجعة نظامية لإدارة مخاطر سلسلة التوريد السيبرانية

2. **المصادر الأولية:** المعالجة الجانب التطبيقي للدراسة، تم اللجوء إلى الاستبيان كأداة أساسية للدراسة

المطلب الثاني: أدوات الدراسة

تتطلب عملية إنجاز البحوث والدراسات توفر مجموعة من الأدوات البحثية والوسائل المناسبة التي تستخدم لجمع المعلومات والتي تمكن الباحث من الوصول إلى البيانات اللازمة، حيث يستطيع من خلالها معرفة واقع أو ميدان الدراسة ولأن أدوات جمع البيانات متعددة ومتنوعة، فإن طبيعة الموضوع الخاضع للدراسة وخصوصيته تفرض انتقاء الأدوات المناسبة على جمع البيانات والأساليب الإحصائية لتحليل تلك البيانات.

الفرع الأول: أدوات جمع البيانات

في موضوع بحثنا هذا سيتم الاعتماد على الاستبيان بشكل كبير كوسيلة لجمع البيانات المختلطة بالدراسة

أولا: الاستبيان

يمثل الاستبيان مجموعة من الأسئلة تم تصميمها بناء على الدراسات السابقة المماثلة لموضوع أثر الأمن السيبراني في تحسين أداء سلاسل التوريد.

الجزء الأول: يحتوي على البيانات الأساسية للموظفين بالمؤسسات محل الدراسة (السن، المستوى التعليمي، عدد سنوات الخبرة، الوظيفة، حجم المؤسسة، نوع القطاع).

الجزء الثاني: يتعلق بقياس أثر الأمن السيبراني على تحسين أداء سلاسل التوريد، ويحتوي على 29 عبارة ومكون من جزأين:

_جزء لعرض قياس أبعاد الأمن السيبراني والمكون من 16 عبارة والمكون من 04 أبعاد

- ✓ البعد التنظيمي المكون من 04 عبارات؛
- ✓ البعد التقني المكون من 04 عبارات؛
- ✓ البعد البشري المكون من 04 عبارات؛
- ✓ البعد التعاوني في الأمن السيبراني والمكون من 04 عبارات.

الجزء الثالث: متعلق بأداء سلسلة التوريد

والمكون من 13 عبارة وتتكون من 03 أبعاد؛

- ✓ بعد الكفاءة التشغيلية والمكون من 05 عبارات؛
- ✓ بعد جودة الخدمة ورضى العملاء والمكون من 04 عبارات؛
- ✓ بعد الاستمرارية والمرونة والمكون من 04 عبارات.

الفرع الثاني: الأدوات الإحصائية

من أجل تحليل البيانات التي تم جمعها من خلال قوائم الاستبيان تمت عملية تفريغ البيانات في برنامج 2007 اكسل والاستعانة ببرنامج SPSS للمعالجة، حيث تم الاعتماد على مجموعة من الأساليب الإحصائية وذلك على النحو التالي:

- معامل الفاكرونباخ.
- المتوسط الحسابي والانحراف المعياري.
- معامل الارتباط برسون؛
- الإنحدار الخطي البسيط.
- الانحدار الخطي المتعدد.

كما تم استخدام مقياس ليكارت الخماسي لتقييم إجابات الموظفين، بحيث تم إعطاء رقم لكل درجة من المقياس من اجل تسهيل عملية معالجتها كالآتي:

جدول رقم (6): درجات مقياس ليكارت في الاستبيان

أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
5	4	3	2	1

المصدر: من إعداد الطالبتين

لتحديد قيم المتوسط الحسابي تم كذلك كالآتي:

1. **حساب المدى:** المدى قيمة –أقل قيمة أي 5-1= 4
2. **يقسم المدى على عدد الفئات:** 5/ 4 = 0,8
3. **يضاف (0,8) للحد الأدنى للمقياس.** فتصبح كالتالي

جدول رقم (7): مجال المتوسط الحسابي المرجح لكل مستوى مقياس (ليكارت)

المتوسط المرجح	المستوى
من 1 الى 1,80	منخفض جدا (غير موافق بشدة)
من 1,81 الى 2,60	منخفض (غير موافق)
من 2,61 الى 3,40	متوسط (محايد)
من 3,41 الى 4,20	مرتفع (موافق)
من 4,21 الى 5	مرتفع جدا (موافق بشدة)

المصدر: من إعداد الطالبتين

الفرع الثالث: صدق وثبات الاستبيان

لقد تم إجراء عدد من الإجراءات على الاستبيان للتأكد من صحته وثباته مستخدما في ذلك تحكيم الاستبيان من خلال محكمين متخصصين في هذا الموضوع، بالإضافة للاختبارات اللازمة للتحقق من الصدق والثبات.

✓ **صدق المحكمين:**

ولغرض معرفة مدى وضوح أسئلة الاستبيان فقد تم تصميمه مع الأستاذ المشرف وعرضه على أساتذة متخصصين في هذا المجال، وبعد ذلك تم صياغة العبارات بشكل ملائم وأكثر وضوحا وبساطة لتظهر في شكلها النهائي

✓ **ثبات الاستبيان:**

يعبر عن مدى استقرار وثبات أدوات الدراسة المتمثلة في الاستبيان، بحيث يوضح ما إذا كانت الاستبيانات الموزعة ستعطي نفس النتائج إذا تم توزيعها مجددا على نفس أفراد العينة وفي نفس الظروف، وتم الاعتماد في ذلك على معامل الثبات "آلفا كرونباخ" بالاستعانة ببرنامج SPSS

جدول رقم (8): نتائج ألفا كرونباخ

المحور	عدد الفقرات	قيمة ألفا كرونباخ
أبعاد الأمن السيبراني	16	0,816
أبعاد سلاسل التوريد	13	0,681
المجموع	29	0،852

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من جدول رقم (8) نلاحظ أن قيمة ألفا كرونباخ لمحور أبعاد الأمن السيبراني بلغت **81,6%**وهي قيمة مرتفعة، أما محور أبعاد سلاسل التوريد فقد بلغت قيمة ألفا كرونباخ له **68,1%** وهي قيمة مقبولة، أما قيمة ألفا كرونباخ الإجمالية فقد بلغت **85,2%**وهي قيمة تعبر عن ثبات مرتفع جداً، لأنها أعلى من النسبة المقبولة في دراسات العلوم الإنسانية وهي **60%**؛ مما يعني أن أداة الدراسة تتمتع بدرجة عالية من الثبات مما يجعلها صالحة لاستيفاء متطلبات الدراسة الميدانية.

المبحث الثاني: نتائج الدراسة ومناقشتها

يهدف هذا البحث الى عرض النتائج التي توصلنا اليها من عمليات التحليل الاحصائي واظهار العلاقة بين متغيرات الدراسة بالاعتماد على مجموعة من الأدوات الإحصائية التي ذكرناها سابقا.

المطلب الأول: عرض نتائج الدراسة

يتضمن هذا المطلب على عرض كل ما جاء في الاستبيانات الموزعة على أفراد العينة بداية من البيانات الأساسية إلى إجاباتهم على عبارات محاور قياس أبعاد الأمن السيبراني وأداء تحسين سلسلة التوريد، إضافة إلى عرض نتائج دراسة مجموعة من الارتباطات، سيتضمن ذلك التعليق على كل ما توصلنا إليه

الفرع الأول: الدراسة الإحصائية للمتغيرات الشخصية

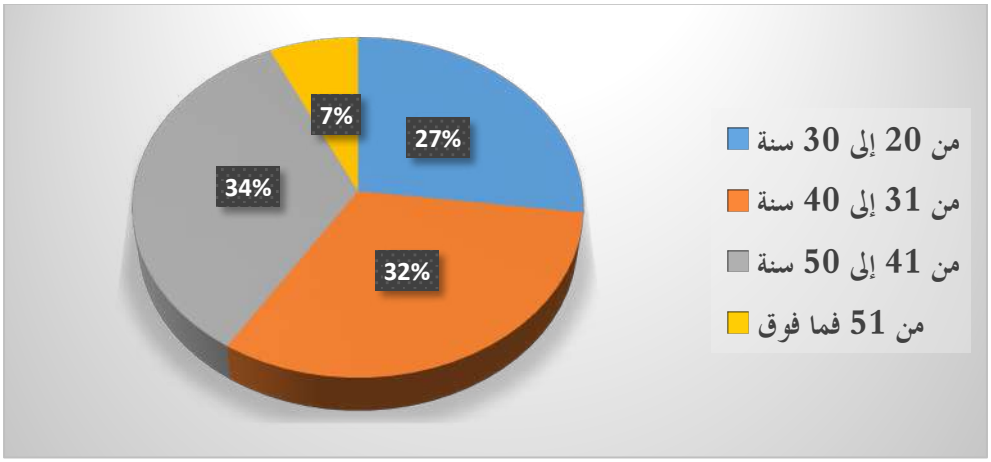
أولا: توزيع الموظفين حسب السن وهذا ما يوضحه الجدول التالي :

جدول رقم (9): توزيع الموظفين حسب السن

السن	التكرار	النسبة المئوية
من 20 إلى 30 سنة	27	27,0 %
من 31 إلى 40 سنة	32	32,0 %
من 41 إلى 50 سنة	34	34,0 %
من 51 فما فوق	7	7,0 %
المجموع	100	100,0 %

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

الشكل رقم (2): توزيع الموظفين حسب السن



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج excelوSPSS

من خلال استعراض بيانات جدول رقم (9) الذي يوضح توزيع أفراد عينة الدراسة حسب متغير السن، نلاحظ أن الفئة العمرية الأكثر تمثيلاً في عينة الدراسة هي الفئة التي تتراوح أعمارهم (**من 41 إلى 50 سنة**)، حيث بلغ عدد أفرادها **34** موظفاً بنسبة **34.0%**، تليها في المرتبة الثانية الفئة العمرية (**من 31 إلى 40 سنة**) بعدد **32** موظفاً وبنسبة **32.0%**، ثم جاءت الفئة العمرية (**من 20 إلى 30 سنة**)في المرتبة الثالثة بعدد **27** موظفاً وبنسبة **27.0%**، بينما جاءت فئة **51** سنة فما فوق في المرتبة الأخيرة بعدد **7** موظفين فقط وبنسبة **7.0%**؛ بحيث يُشير هذا التوزيع إلى تقارب في نسب الفئات العمرية الثلاث الأولى (**من 20 إلى 50 سنة**)، مما يعكس تنوعاً في الخبرات العملية داخل المؤسسات محل الدراسة، كما يُظهر تركز الغالبية العظمى من الموظفين (**أكثر من 66%**) في الفئة العمرية المتوسطة (**من 31 إلى 50 سنة**)، وهو ما يمنح النتائج موثوقية عالية، نظراً لأن هذه الفئة غالباً ما تكون هي الأكثر دراية بمتطلبات العمل الميداني وتحديات الأمن السيبراني في أداء سلاسل التوريد.

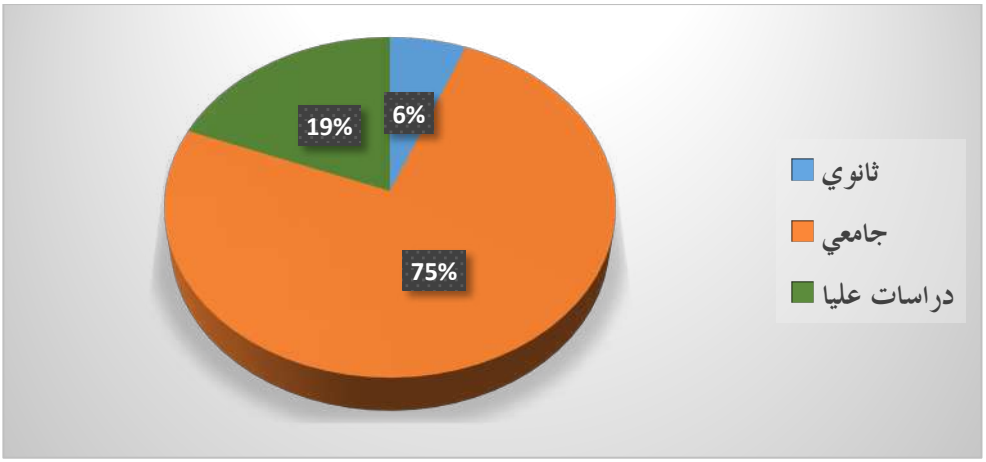
ثانيا: توزيع الموظفين حسب المستوى التعليمي يوضحه الجدول أدناه:

جدول رقم (10): توزيع الموظفين حسب المستوى التعليمي

المستوى التعليمي	التكرار	النسبة المئوية
ثانوي	6	6,0 %
جامعي	75	75,0 %
دراسات عليا	19	19,0 %
المجموع	100	100,0 %

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

الشكل رقم (3): توزيع الموظفين حسب المستوى التعليمي



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSSوexcel

يظهر الجدول أعلاه أن أغلب أفراد عينة الدراسة هم من ذوي المستوى الجامعي بنسبة بلغت **75%** (75 موظفا)، تليها فئة الدراسات العليا بنسبة **19%** (19 موظفا)، وهذا التركز الكبير للمستويات الجامعية والعليا يعكس بوضوح طبيعة الوظائف في المؤسسات محل الدراسة التي تشترط كفاءات علمية مؤهلة، مما يضمن لنا أن الموظفين يمتلكون الرصيد المعرفي الكافي لاستيعاب محاور الاستبيان والإجابة بدقة على الأسئلة المتعلقة بـــ الأمن السيبراني وسلاسل التوريد، بينما لم تتجاوز فئة المستوى الثانوي نسبة **6%** (6 موظفين).

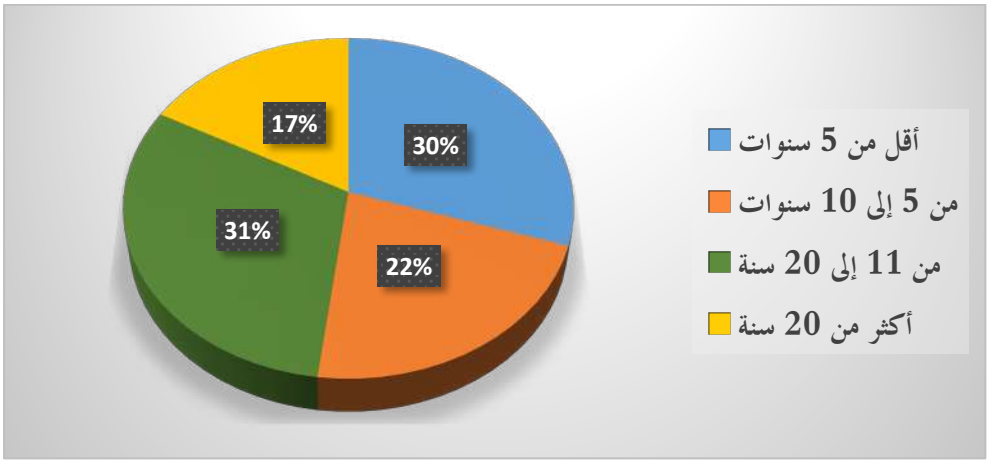
ثالثا: عدد سنوات الأقدمية: توزيع الموظفين حسب سنوات الأقدمية؛ وهذا ما يوضحه الجدول التالي:

جدول رقم (11): **توزيع الموظفين حسب سنوات الأقدمية**

الخبرة	التكرار	النسبة المئوية
أقل من 5 سنوات	30	30,0 %
من 5 إلى 10 سنوات	22	22,0 %
من 11 إلى 20 سنة	31	31,0 %
أكثر من 20 سنة	17	17,0 %
المجموع	100	100,0 %

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

الشكل رقم (4): **توزيع الموظفين حسب سنوات الأقدمية**



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS وexcel

يظهر الجدول أعلاه توزيع أفراد العينة حسب سنوات الأقدمية، حيث نلاحظ تقارباً في نسب الخبرات المهنية؛ إذ تصدرت الفئة ذات الخبرة من (**11 إلى 20 سنة**) المرتبة الأولى بنسبة **31%** (31 موظفا)، تليها مباشرة فئة أقل من **5** سنوات بنسبة **30%** (30 موظفا)، ثم فئة من(**5 إلى 10 سنوات**) بنسبة **22%** (22 موظفا)، وأخيراً فئة (**أكثر من 20 سنة**) بنسبة **17%** (17 موظفا)، هذا التوزيع ويعكس توازناً نوعياً في

عينة الدراسة بين أصحاب الخبرات المتراكمة القادرين على إدارة تعقيدات سلاسل التوريد، وبين ذوي المهارة العالية التي تمتلك سرعة التكيف مع متطلبات الأمن السيبراني الحديثة،

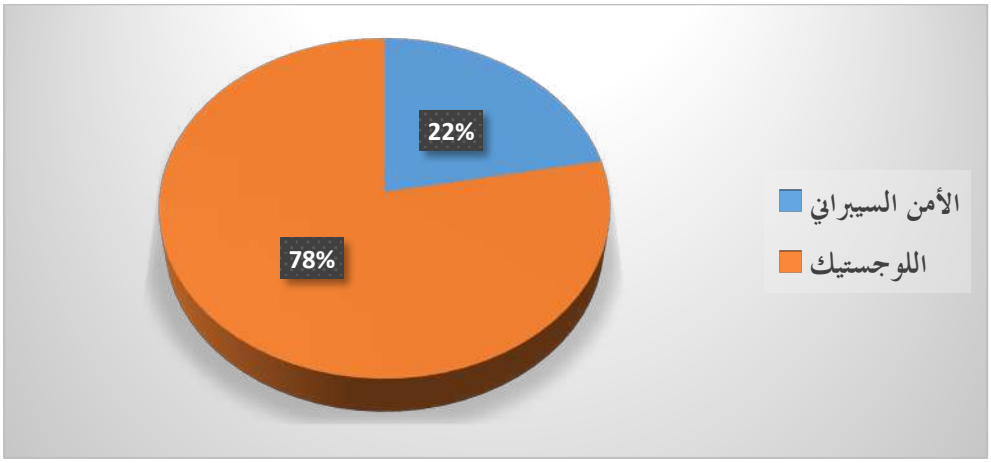
رابعا: توزيع الموظفين على حسب القسم؛ كما هو موضح:

جدول رقم (12): توزيع الموظفين حسب القسم

القسم	التكرار	النسبة المئوية
الأمن السيبراني	22	22,0 %
اللوجستيك	78	78,0 %
المجموع	100	100,0 %

المصدر: من اعداد الطالبتين بالاعتماد على نتائج برنامجspss

الشكل رقم (5): توزيع الموظفين حسب القسم



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSSوexcel

يوضح الجدول أعلاه توزيع أفراد العينة حسب القسم، حيث نلاحظ أن قسم اللوجستيك تصدر المرتبة الأولى بنسبة بلغت **78.0%** (78 موظفا)، في حين بلغت نسبة الموظفين في قسم الأمن السيبراني **22.0**% (22 موظفا)، ويعود سبب هذا التباين الواضح إلى أن النشاط اللوجستي يمثل العمود الفقري الأساسية للمؤسسات محل الدراسة، بينما لا يزال قسم الأمن السيبراني يُصنف كأحد التخصصات الل التي بدأت المؤسسات في تبنيها حديثاً لمواكبة التحول الرقمي.

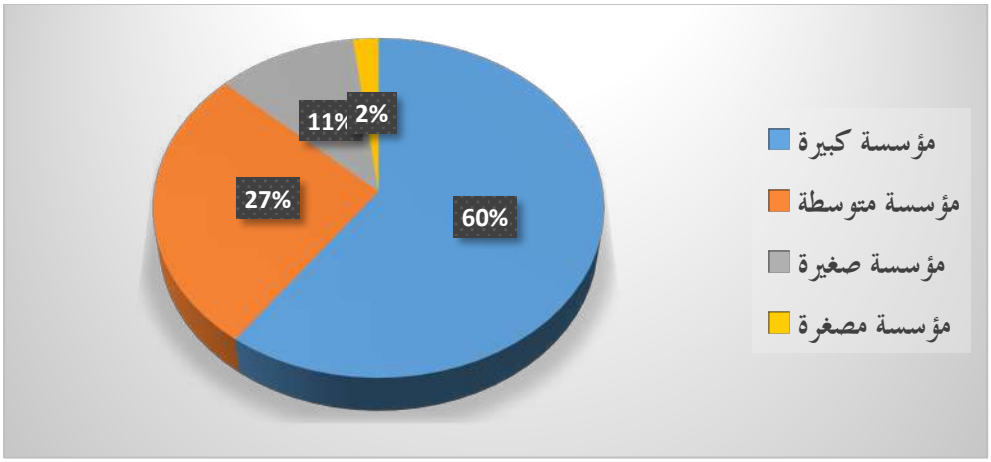
خامسا: توزيع الموظفين حسب حجم المؤسسة؛ وهذا ما يوضحه الجدول التالي:

جدول رقم (13): توزيع الموظفين حسب حجم المؤسسة

حجم المؤسسة	التكرار	النسبة المئوية
مؤسسة كبيرة	60	60,0 %
مؤسسة متوسطة	27	27,0 %
مؤسسة صغيرة	11	11,0 %
مؤسسة مصغرة	2	2,0 %
المجموع	100	100,0 %

المصدر: من اعداد الطالبتين بالاعتماد على نتائج برنامجspss

الشكل رقم (6): توزيع الموظفين حسب حجم المؤسسة



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج excelوSPSS

يوضح الجدول أعلاه توزيع أفراد العينة حسب حجم المؤسسة، حيث نلاحظ سيطرة المؤسسات الكبيرة على الحصة الأكبر بنسبة **60.0%** (60 موظفا)، تليها المؤسسات المتوسطة بنسبة **27.0%** (27 موظفا)، بينما بلغت نسبة الموظفين في المؤسسات الصغيرة والمصغرة **11%** و**2%** على التوالي، ويعكس هذا التركز الكبير في المؤسسات الكبيرة والمتوسطة واقع قطاع اللوجستيك والأمن السيبراني؛ كون هذه المؤسسات هي الأكثر استهدافاً وقدرة على تبني أنظمة الحماية الرقمية المعقدة.

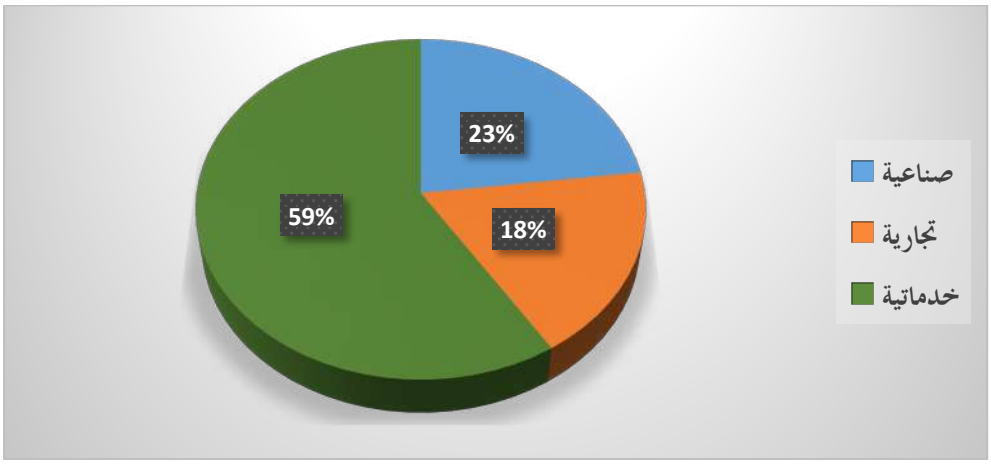
سادسا: **توزيع الموظفين حسب نوع المؤسسة**؛ وهذا ما يوضحه الجدول التالي:

جدول رقم (14): **توزيع الموظفين حسب نوع المؤسسة**

نوع القطاع	التكرار	النسبة المئوية
صناعية	23	23,0 %
تجارية	18	18,0 %
خدماتية	59	59,0 %
المجموع	100	100,0 %

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

الشكل رقم (7): **توزيع الموظفين حسب نوع المؤسسة**



المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSSوexcel

يوضح الجدول أعلاه أن نسبة الموظفين بالقطاع الخدماتي قد قدرت بـــ **59.0%** وهي نسبة كبيرة جداً، وهذا راجع لطبيعة نشاط المؤسسات محل الدراسة التي ترتكز بشكل أساسي على تقديم الخدمات اللوجستية، تليها فئة الموظفين بالقطاع الصناعي بنسبة **23.0%**، بينما بلغت نسبة الموظفين بالقطاع التجاري **18.0%** وهي النسبة الأقل في عينة الدراسة. ويعكس هذا التوزيع هيمنة الجانب الخدمي في بيئة الدراسة، وهو ما يتماشى مع التوجهات الحديثة التي تعتبر الخدمات اللوجستية الرقمية والمؤمنة سيبيرانيا الركيزة الأساسية لاستدامة العمليات؛ حيث إن المؤسسات الخدمية هي الأكثر اعتماداً على تدفق البيانات الحساسة عبر سلاسل التوريد.

الفرع الثاني: اختبار التوزع الطبيعي للعينة

يعد اختبار التوزع الطبيعي خطوة منهجية حاسمة لتحديد نوع الاختبارات الإحصائية المستخدمة في اختبار فرضيات الدراسة؛ حيث يتوقف استخدام الاختبارات المعلمية على مدى اقتراب توزيع بيانات العينة من المنحنى الاعتدالي. وللتحقق من ذلك، تم تطبيق اختبارات كولموجروف-سميرنوف (Kolmogorov–Smirnov) و شابيرو-ويلك (Shapiro–Wilk) على متغيرات الدراسة لعينة قوامها (100) مفردة، والجدول التالي يوضح النتائج:

جدول رقم (15): نتائج اختبار Shapiro–Wilk

المحور	الاختبار	الإحصاء	الدلالة الإحصائية Sig
الأمن السيبراني	Shapiro–Wilk	0.980	0.126
سلاسل التوريد	Shapiro–Wilk	0.980	0.137

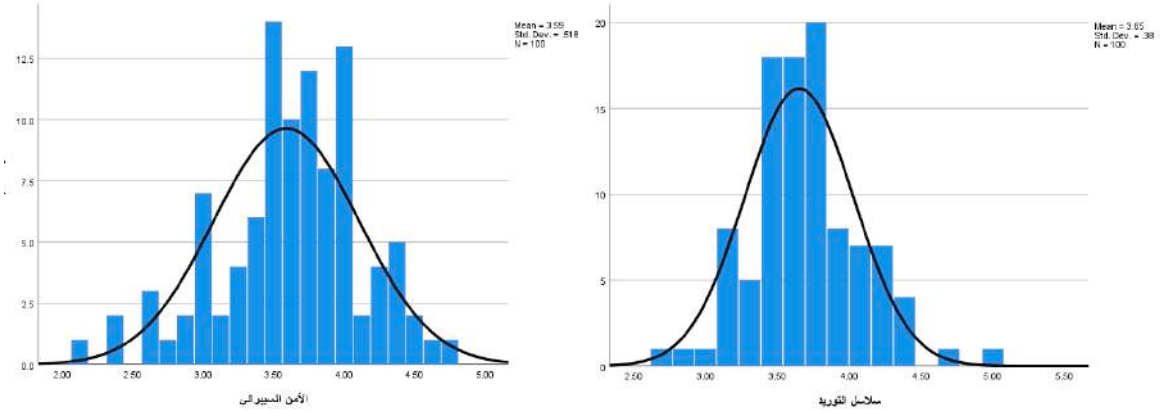
التعليق على النتائج وتفسيرها:

أظهرت نتائج اختبار (Shapiro–Wilk) الموضحة في الجدول أعلاه أن قيم مستوى الدلالة (Sig) لكل من محور (الأمن السيبراني) (**0.126**) ومحور (سلاسل التوريد) (**0.137**) هي أكبر من مستوى الدلالة المعياري (**0.05**)، ويشير ذلك إحصائياً إلى قبول الفرضية الصفرية التي تنص على أن البيانات تتبع التوزع الطبيعي.

الفحص البياني للاعتدالية (Visual Inspection):

لتعزيز الموثوقية النتائج، تم فحص التوزيع بيانياً عبر المدرجات التكرارية. أظهر الشكل البياني لمحور الأمن السيبراني، ومحور سلاسل التوريد، تمركز الاستجابات بوضوح حول المتوسطات الحسابية (3.59 و 3.65) على التوالي) واتخاذها شكل المنحنى الجرسي، إن التطابق البصري بين توزيع البيانات ومنحنى الاعتدالية في المخططات البيانية يؤكد أن البيانات تتسم بالاعتدالية الكافية، حيث تميل القيم للتجمع في المنتصف مع انخفاض تدريجي متوازن نحو الأطراف، وهو ما يدعم استخدام الاختبارات المعلمية.

الشكل رقم (8): المدرجات التكرارية لقياس اعتدالية البيانات



الخلاصة الإحصائية: بناءً على نتائج اختبار Shapiro–Wilk للمحاور الرئيسية والتدعيم البصري من خلال المخططات البيانية، ونظراً لكون حجم العينة (100) يحقق متطلبات قانون النهاية المركزية، فقد اعتمد خلال الدراسة على استخدام الاختبارات الإحصائية المعلمية مثل معامل ارتباط بيرسون والانحدار الخطي لقياس أثر أبعاد الأمن السيبراني على سلاسل التوريد.

الفرع الثالث: تحليل وتفسير قياس أثر الأمن السيبراني على تحسين أداء سلاسل التوريد

- **تحليل وتفسير أثر الأمن السيبراني**

- **البعد التنظيمي:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة بالبعد التنظيمي في المؤسسات محل الدراسة وهي كالتالي:

جدول رقم (16): متوسط إجابات الموظفين حول التنظيم

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
تلتزم الإدارة العليا بتوفير الموارد المالية اللازمة لتطبيق استراتيجية الأمن السيبراني.	4,23	0,908	1	مرتفع جدا
توجد سياسات أمنية واضحة ومصرح بها تحدد مسؤوليات الموظفين في حماية البيانات.	4,15	0,903	2	مرتفع
يقتصر التدقيق على الأنظمة الرقمية على الحالات الطارئة فقط مما يسمح بوجود ثغرات أمنية.	2,75	1,132	4	متوسط
يتعاون قسم تكنولوجيا المعلومات مع قسم اللوجستيك لتعزيز الأمن السيبراني.	4,00	0,910	3	مرتفع
المجموع	3,78	0,96	-	مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من الجدول أعلاه يظهر أن المتوسط الحسابي العام لإجابات الموظفين حول البعد التنظيمي بلغ (**3.78**) وبانحراف معياري (**0.96**)، وهو يقع في المجال المرتفع، وتشير قيم الانحراف المعياري إلى نسبية الوثوق بقيم المتوسط الحسابي المكونة لهذا البعد، وهذا يعني أن المؤسسات محل الدراسة تمتلك تنظيما جيدا ،ويعود هذا بالأساس إلى أن المؤسسات محل الدراسة تلتزم الإدارة العليا بتوفير الموارد المالية اللازمة لتطبيق استراتيجية الأمن السيبراني (وهو ما توضحه العبارة الأولى بمتوسط حسابي (**4.23**) وانحراف معياري(**0.908**) ، كما يعود ذلك إلى وجود سياسات أمنية واضحة ومصرح بها تحدد مسؤوليات الموظفين في حماية البيانات وهو ما تبينه العبارة الثانية بمتوسط حسابي (**4.15**) وانحراف معياري (**0.903**)، كما يتعاون قسم تكنولوجيا المعلومات مع قسم اللوجستيك لتعزيز الأمن السيبراني وهو ما تبينه العبارة الرابعة بمتوسط حسابي (**4.00**) وانحراف معياري (**0.910**)، أما بخصوص يقتصر التدقيق على الأنظمة الرقمية على الحالات الطارئة فقط مما يسمح بوجود ثغرات أمنية وهو ما توضحه العبارة الثالثة بمتوسط حسابي (**2.75**) وانحراف معياري (**1.132**).

وعليه نستنتج أن المؤسسات محل الدراسة تمتلك تنظيمياً أمنياً مدعوماً بالتزام الإدارة العليا وتنسيق فعال بين الأقسام، مع وجود سياسات واضحة لحماية البيانات؛ إلا أنها لا تزال تفتقر لآليات التدقيق الرقمي المستمر كإجراء استباقي.

- **البعد التقني:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة بالبعد التقني في المؤسسات محل الدراسة وهي كالتالي

جدول رقم (17): **متوسط إجابات الموظفين حول البعد التقني**

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
تتبنى المؤسسة إجراءات مشددة للمصادقة لمنع الوصول غير المصرح به للبيانات.	4,18	0,809	1	مرتفع
تفتقر أنظمة النسخ الاحتياطي للتلقائية مما يؤخر استعادة البيانات عند وقوع الهجمات السيبرانية	2,73	1,024	4	متوسط
تعتمد المؤسسة على تقنيات متقدمة (الذكاء الاصطناعي) للتنبؤ بالتهديدات السيبرانية المحتملة	3,28	1,181	3	متوسط
تعتمد المؤسسة على استراتيجية التحديث المستمر للأنظمة التشغيلية للحد من الثغرات الأمنية	3,91	0,986	2	مرتفع
المجموع	3,53	1,000		مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من الجدول أعلاه يظهر أن المتوسط الحسابي العام لإجابات الموظفين حول البعد التقني بلغ (**3.53**) وبانحراف معياري (**1.000**)، وهو يقع في المجال المرتفع، وتشير قيم الانحراف المعياري إلى نسبية الوثوق بقيم المتوسط الحسابي المكونة لهذا البعد، وهذا يعني أن المؤسسات محل الدراسة تمتلك تقنيات متقدمة ، ويعود هذا بالأساس إلى أن المؤسسات تتبنى إجراءات مشددة للمصادقة لمنع الوصول غير المصرح به للبيانات وهو ما توضحه العبارة الأولى بمتوسط حسابي (**4.18**) وانحراف معياري (**0.809**)، كما يعود كذلك إلى اعتماد المؤسسة على استراتيجية التحديث المستمر للأنظمة التشغيلية للحد من الثغرات الأمنية وهو ما تبينه العبارة الرابعة بمتوسط حسابي (**3.91**) وانحراف معياري (**0.986**)، كما تعتمد المؤسسة على تقنيات متقدمة (الذكاء الاصطناعي) للتنبؤ بالتهديدات السيبرانية المحتملة وهو ما توضحه العبارة الثالثة بمتوسط حسابي (**3.28**) وانحراف معياري (**1.181**)، وصولاً إلى أن أنظمة النسخ الاحتياطي تفتقر للتلقائية مما يؤخر استعادة البيانات عند وقوع هجمات سيبرانية وهو ما تبينه العبارة الثانية بمتوسط حسابي (**2.73**) وانحراف معياري (**1.024**).

وعليه نستنتج أن المؤسسات محل الدراسة تعتمد حلولاً تقنية متطورة لتأمين الوصول وتحديث الأنظمة، لكنها تفتقر إلى الاتمتة في عمليات النسخ الاحتياطي مما قد يعيق سرعة الاستجابة للأزمات.

- **البعد البشري:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة بالبعد البشري في المؤسسات محل الدراسة وهي كالتالي:

جدول رقم (18): متوسط إجابات الموظفين حول البعد البشري

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
يبدي الموظفون عدم التزام تام بتغيير كلمات المرور الخاصة بهم بشكل دوري.	2,73	1,162	4	متوسط
تحرص المؤسسة على التدريب الدوري المستمر لتطوير أداء الموظفين في التعامل مع المخاطر الرقمية	3,71	1,217	3	مرتفع
يساهم الموظف الواعي في تقليل مخاطر هجمات الهندسة الاجتماعية وأي بريد مشبوه	4,30	0,704	1	مرتفع جدا
يمتلك الكادر التقني المهارات اللازمة للتصرف السريع واحتواء الهجمات السيبرانية فور وقوعها	3,85	0,957	2	مرتفع
المجموع	3,65	1,010		مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من الجدول السابق يظهر أن المتوسط الحسابي العام لإجابات الموظفين حول البعد البشري بلغ (**3.65**) وبانحراف معياري (**1.010**)، وهو يقع في المجال المتوسط إلى المرتفع، وهذا يعني أن المؤسسات محل الدراسة تمتلك مهارات بشرية جيدة ، ويعود هذا بالأساس إلى إدراك أن الموظف الواعي يساهم في تقليل مخاطر هجمات الهندسة الاجتماعية وأي بريد مشبوه وهذا ما توضحه العبارة الثالثة .بمتوسط (**4.30**) وبانحراف معياري (**0,704**)، وامتلاك الكادر التقني المهارات اللازمة للتصرف السريع واحتواء الهجمات السيبرانية فور وقوعها وهذا ما توضحه العبارة الرابعة متوسط (**3.85**) وبانحراف معياري (**0,957**)،كما تحرص المؤسسة على التدريب الدوري المستمر لتطوير أداء الموظفين في التعامل مع المخاطر الرقمية وهذا ما توضحه العبارة الثانية .بمتوسط (**3.71**) وبانحراف معياري (**1,217**)، بينما يبدي الموظفون عدم التزام تام بتغيير كلمات المرور الخاصة بهم بشكل دوري وهذا ما توضحه العبارة الأولى .بمتوسط (**2.73**) وانحراف معياري (**1,162**)

وعليه نستنتج أن المؤسسات محل الدراسة تمتلك رصيداً بشرياً وتقنياً مؤهلاً لمواجهة التهديدات السيبرانية، مع وجود حاجة ملحة لتعزيز الثقافة الأمنية السلوكية فيما يتعلق بالالتزام الدوري بتغيير بيانات الوصول.

- **البعد التعاوني:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة بالبعد التعاوني في المؤسسات محل الدراسة وهي كالتالي

جدول رقم (19): **متوسط إجابات الموظفين حول البعد التعاوني**

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
تعتمد المؤسسة منصات رقمية موحدة مع الموردين والشركاء لإدارة ومراقبة المخاطر السيبرانية المشتركة.	3,65	1,038	2	مرتفع
تفرض المؤسسة معايير أمنية محددة على الموردين لتأمين سلامة سلسلة التوريد.	3,73	1,004	1	مرتفع
تتضمن الاتفاقيات مع الموردين عدم وضوح في إجراءات حماية وسرية البيانات المتبادلة.	2,70	1,049	4	متوسط
تبادل المعلومات بشكل فوري بين الشركاء بشأن التهديدات السيبرانية المحددة.	3,56	0,946	3	مرتفع
المجموع	3,41	1,009		مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من الجدول السابق يظهر أن المتوسط الحسابي العام لإجابات الموظفين حول البعد التعاوني بلغ (**3.41**) وبانحراف معياري (**1.009**)، وهو يقع في المجال المرتفع، وتشير قيم الانحراف المعياري إلى نسبية الوثوق بقيم المتوسط الحسابي المكونة لهذا البعد، وهذا يعني أن المؤسسات محل الدراسة تمتلك فرق تعاونية جيدة ، ويعود هذا بالأساس إلى أن المؤسسة تفرض معايير أمنية محددة على الموردين لتأمين سلامة سلسلة التوريد وهو ما توضحه العبارة الثانية بمتوسط حسابي (**3.73**) وانحراف معياري (**1,004**)، كما تعتمد المؤسسة منصات رقمية موحدة مع الموردين والشركاء لإدارة ومراقبة المخاطر السيبرانية المشتركة وهو ما تبينه العبارة الأولى بمتوسط حسابي **3.65**)وانحراف معياري (**1,038**)، بالإضافة إلى تبادل المعلومات بشكل فوري بين الشركاء بشأن التهديدات السيبرانية المحددة العبارة الرابعة بمتوسط (**3.56**) وانحراف معياري (**0.946**)، وصولاً إلى أن الاتفاقيات مع الموردين تتضمن عدم وضوح في إجراءات حماية وسرية البيانات المتبادلة (وهو ما تبينه العبارة الثالثة بمتوسط حسابي (**2.70**)وانحراف معياري (**1,049**).

وعليه نستنتج أن المؤسسات تنتهج سياسة تعاونية نشطة لتأمين سلاسل إمدادها عبر فرض معايير تقنية ومنصات مشتركة، إلا أنها تواجه تحديات قانونية تتعلق بوضوح بنود حماية البيانات في الاتفاقيات المبرمة مع الشركاء.

- **تحليل وتفسير أداء سلاسل التوريد**

- **بعد الكفاءة التشغيلية:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة ببعد الكفاءة التشغيلية في المؤسسات محل الدراسة وهي كالتالي

جدول رقم (20): متوسط إجابات الموظفين حول بعد الكفاءة التشغيلية

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
يساهم الأمن السيبراني في تقليص زمن توقف العمليات الناتجة عن الاختراقات.	4,20	0,636	1	مرتفع
تلعب سلامة البيانات دور مهم في دقة التنبؤ بالطلب المستقبلي في سلسلة التوريد.	4,17	0,711	3	مرتفع
يؤدي ضعف سلامة البيانات إلى عدم القدرة على تخفيض التكاليف اللوجستية الإضافية.	3,88	0,891	4	مرتفع
تساعد الأنظمة الآمنة في تحسين سرعة تدفق المعلومات بين جميع حلقات السلسلة.	4,18	0,770	2	مرتفع

تواجه المؤسسة عدم القدرة على استغلال مواردها المعلوماتية نتيجة ضعف الرقابة الأمنية.	3,56	1,008	5	مرتفع
المجموع	4,00	0,803		مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من خلال إبراز النتائج المتوصل إليها في الجدول أعلاه، يتبين أن المتوسط الحسابي للإجابات المتعلقة ببعد الكفاءة التشغيلية بلغ (**4,00**)، والذي يندرج في مجال (موافق) وهو المستوى المرتفع، وتدل القيمة (**0,803**) للانحراف المعياري على وجود تطابق وتوافق كبير في آراء المستجيبون، وهذا ما يعكس وعي عالي في المؤسسة بعلاقة متينة بين الحماية الأمنية والتمييز التشغيلي.

تحتل العبارة الأولى التي تنص على "يساهم الأمن السيبراني في تقليص زمن توقف العمليات الناتجة عن الاختراقات" على المرتبة الأولى بمتوسط حسابي (**4,20**) مع انحراف معياري (**0,636**)، إذ يعكس مدى إدراك المبحوثين بأن الحماية السيبرانية هي الضامن الأساسي لاستمرار تدفق العمليات، والحد من الأعطال المفاجئة التي تشل حلقات سلسلة التوريد، وتأتي العبارة الرابعة في المرتبة الثانية والتي تنص على" تساعد الأنظمة الآمنة في تحسين سرعة تدفق المعلومات بين جميع حلقات السلسلة" بمتوسط يقدر ب (**4,18**)، فيؤكد أن آمان البيئة الرقمية يعزز من سلاسة تدفق البيانات، مما يؤثر بالإيجاب على سرعة الاستجابة اللوجستية، وتليها العبارة الثانية التي تتحدث عن "تلعب سلامة البيانات دور مهم في دقة التنبؤ بالطلب المستقبلي في سلسلة التوريد" بمتوسط (**4,17**)، التي تدل على أن صحة البيانات الرقمية هي المرتكز الذي يبنى عليه التخطيط الاستراتيجي الفعال لسلسلة التوريد، ثم تأتي العبارة الثالثة في المرتبة ما قبل الأخيرة التي تتناول أثر ضعف سلامة البيانات على التكاليف اللوجستية، بحيث نجد المتوسط (**3,88**)، وهو ما يبقيها في مستوى مرتفع ، ويؤكد أن أي تلاعب بالبيانات يؤدي إلى هدر مالي غير مدروس، وفي الأخير نجد العبارة الخامسة التي تنص على ‘‘تواجه المؤسسة عدم القدرة على استغلال مواردها المعلوماتية نتيجة ضعف الرقابة الأمنية" بمتوسط (**3,56**) مع إنحراف معياري (**1,008**)، ويتبين هنا أن المعيار الإنحرافي تجاوز الواحد، فيدل على تفوت نسبي في آراء أفراد العينة حول درجة ملائمة الرقابة الأمنية في المؤسسات لبلوغ الاستغلال الأمثل للموارد المعلوماتية.

ومنه نستنتج أن صلابة البنية التحتية للأمن السيبراني هي جوهر وأساس الكفاءة التشغيلية في لسلاسل التوريد للمؤسسات نطاق الدراسة، أي كلما زادت قدرة الأنظمة على حماية سلامة البيانات، أدى ذلك إلى تقليص فترات الانقطاع، ومنه تعزيز دقة التنبؤ مما يحسن من الأداء التشغيلي العام.

- **بعد جودة الخدمة وخدمة العملاء:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة ببعد جودة الخدمة وخدمة العملاء في المؤسسات محل الدراسة وهي كالتالي

جدول رقم (21): متوسط إجابات الموظفين حول بعد جودة الخدمة وخدمة العملاء

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
يعزز ضمان سرية بيانات الزبائن في رفع مستويات الولاء للمؤسسة والثقة في خدماتها.	4,31	0,775	1	مرتفع جدا
ترفع الحماية السيبرانية موثوقية المؤسسة وتزيد من قدرتها على تسليم الطلبيات في الوقت المناسب.	4,17	0,779	2	مرتفع
تفتقر بعض الخدمات لعدم خلوها من التلاعب بالبيانات نتيجة ضعف سلامة الأنظمة.	2,46	0,958	3	منخفض
يسبب الضعف التقني عدم شفافية تتبع الشحنات عبر حلقات السلسلة.	2,17	0,842	4	منخفض
المجموع	3,28	0,838		متوسط

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من خلال الاطلاع على نتائج الجدول، يتضح أن المتوسط الحسابي العام لهذا البعد بلغ (**3,28**)، هي قيمة ضمن المستوى المتوسط لمقياس ديكارت الخماسي، بينما قيمة الانحراف المعياري قدرت ب(**0,838**)، وهذا ما يدل على وجود الانسجام في آراء أفراد العينة في هذا البعد، ونلاحظ أيضا تباين بسيط في الآراء حول بعض العبارات،

وباستقراء الإجابات، نجد أن العبارة الأولى حازت على المرتبة الأولى بمتوسط عالي (**4,31**) مع انحراف معياري (**0,775**) والتي تنص على "يعزز ضمان سرية بيانات الزبائن في رفع مستويات الولاء للمؤسسة والثقة في خدماتها"، وهذا ما يدل على الوعي المرتفع بأهمية الأمن السيبراني كحجر أساسي لبناء علاقة متينة مع العميل، وسجلت العبارة الثانية متوسط حسابي بقدر (**4,17**) التي تتحدث عن دور الحماية السيبرانية في تعزيز موثوقية المؤسسة والمساهمة في تسليم الطلبيات في الوقت المحدد، وأيضا نلاحظ انخفاض في المتوسطات الحسابية للعبارات التي تعكس جوانب سلبية، تليها العبارة الثالثة المتعلقة بتلاعب البيانات بمتوسط (**2,46**)، في حين العبارة الرابعة سجلت أقل متوسط حسابي قدره (**2,17**) والتي تنص على "يسبب الضعف التقني عدم شفافية تتبع الشحنات عبر حلقات السلسلة"، وهو ما يعكس بالإيجاب على ثقة الموظفين في الأنظمة التقنية للمؤسسة.

وعليه نستنتج بأن جودة الخدمة ورضا العميل يرتبطان ارتباطا وثيقا بمدى فعالية تدابير الأمن السيبراني في الحفاظ على الخصوصية واستمرارية العمليات.

- **بعد الاستمرارية والمرونة:** يظهر الجدول الموالي نتائج إجابات الموظفين المتعلقة ببعد الاستمرارية و المرونة في المؤسسات محل الدراسة وهي كالتالي

جدول رقم (22): متوسط إجابات الموظفين حول بعد الاستمرارية والمرونة

الفقرة	المتوسط	الانحراف المعياري	الترتيب	النتيجة
تمتع سلسلة التوريد بالقدرة على الاستمرارية حتى في ظل الهجمات الرقمية.	3,64	0,894	3	مرتفع
تساهم خطط الاستجابة السريعة في تقليل الزمن اللازم لعودة العمليات إلى طبيعتها بعد وقوع الأزمة السيبرانية.	4,13	0,720	1	مرتفع
يدعم دمج الحماية في العمليات في تقليص حجم الخسائر المالية الناجمة عن انقطاع التوريد.	4,10	0,785	2	مرتفع
يظهر أداء المؤسسة عدم القدرة على التكيف السريع مع المتغيرات الرقمية المفاجئة في السوق.	2,50	0,990	4	منخفض
المجموع	3,59	0,847		مرتفع

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

من خلال تحليل النتائج يتبين لنا أن المتوسط الحسابي العام لبعد الاستمرارية والمرونة قد بلغ (3,59) وهو ما يدل على ارتفاع مستوى الاستجابة، بالإضافة إلى الانحراف المعياري الذي سجل (0,847) وهو ما يعكس التوافق بين إجابات الموظفين حول قدرة المؤسسة على الصمود، ومن خلال التعمق في النتائج نجد أن العبارة رقم (2) التي تنص على "تساهم خطط الاستجابة السريعة في تقليل الزمن اللازم لعودة العمليات إلى طبيعتها بعد وقوع الأزمة السيبرانية" وتصنف في المرتبة الأولى بمتوسط قدره (4,13)، ثم بعدها العبارة رقم (3) بمتوسط قدره (4,1) وهذا ما يثبت أن حماية العمليات يساهم في الحد من الخسائر المالية التي تنتج عن انقطاع التوريد، وتليها العبارة رقم (1) المتعلقة مرونة السلسلة وقدرتها على الاستمرارية حتى في ظل الهجوم السيبراني وبلغ المتوسط الحسابي لها ب(3,64)، وفي الأخير سجلت العبارة رقم (4) التي تنص على "يظهر أداء المؤسسة عدم القدرة على التكيف السريع مع المتغيرات الرقمية المفاجئة في السوق" أدنى متوسط حسابي (2,50)، وهو يمثل مؤشر إيجابي يدل على مرونة أداء المؤسسة وقدرتها على التكيف عند المتغيرات المفاجئة.

وعليه نستنتج مما سبق أن تدابير الأمن السيبرانية تضمن استمرارية وتدفق سلسلة التوريد بالإضافة إلى المرونة في التصدي للتهديدات السيبرانية.

الفرع الرابع: دراسة أثر الأمن السيبراني على تحسين أداء سلاسل التوريد في المؤسسات عينة الدراسة

أولا: نتائج دراسة أثر لأمن السيبراني على تحسين أداء سلاسل التوريد في المؤسسات عينة الدراسة: والتي سوف نعالجها من خلال دراسة علاقة الارتباط باستخدام معامل الارتباط بيرسون.

1. دراسة مساهمة أثر الأمن السيبراني على تحسين سلاسل التوريد

لتحديد علاقة الارتباط بين متغيرات الدراسة تم الاستعانة بمعامل الارتباط بيرسون وكانت النتائج كما هي موضحة في الجدول التالي:

جدول رقم (23): العلاقة بين الأمن السيبراني وسلاسل التوريد

		قياس أبعاد الأمن السيبراني
أداء سلسلة التوريد	ارتباط بيرسون	0.602
	الدلالة الإحصائية	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يتبين من خلال الجدول رقم (23) أن هناك علاقة ارتباطية موجبة وذات دلالة إحصائية بين أبعاد الأمن السيبراني وأداء سلاسل التوريد، إذ بلغ معامل ارتباط بيرسون 0.602، وهي قيمة تعكس علاقة متوسطة تميل إلى القوة، كما أن قيمة الدلالة الإحصائية 0.000 أقل من 0.05 وهذا يدل على معنوية العلاقة، **أي أن تعزيز الأمن السيبراني داخل المؤسسة يرتبط بتحسن أداء سلسلة التوريد**

2. دراسة مساهمة أثر أبعاد الأمن السيبراني على تحسين أداء سلاسل التوريد:

جدول رقم (24): العلاقة الارتباطية بين البعد التنظيمي وأداء سلسلة التوريد

		البعد التنظيمي
أداء سلسلة التوريد	ارتباط بيرسون	0.498
	الدلالة الإحصائية	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يبين الجدول وجود علاقة ارتباطية موجبة ومتوسطة القوة بين البعد التنظيمي للأمن السيبراني وأداء سلسلة التوريد، حيث بلغ معامل الارتباط 0.498، مع دلالة إحصائية قدرها 0.000، وهي أقل من 0.05.

وهذا يدل على أن وضوح السياسات الأمنية، دعم الإدارة العليا، والتنسيق التنظيمي داخل المؤسسة يرتبط بتحسن أداء سلسلة التوريد، من خلال تعزيز حماية المعلومات وضمان استمرارية العمليات.

جدول رقم (25): العلاقة الارتباطية بين البعد التقني وأداء سلسلة التوريد

		البعد التقني
أداء سلسلة التوريد	ارتباط بيرسون	0.494
	الدلالة الإحصائية	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يُظهر الجدول رقم (25) وجود علاقة ارتباطية موجبة وذات دلالة إحصائية بين البعد التقني للأمن السيبراني وأداء سلاسل التوريد، حيث بلغت قيمة معامل ارتباط بيرسون r=0.494، وهي قيمة تدل على علاقة متوسطة القوة. كما بلغت قيمة الدلالة الإحصائية Sig=0.000، وهي أقل من مستوى الدلالة المعتمد 0.05، مما يؤكد أن هذه العلاقة معنوية وليست ناتجة عن الصدفة.

عليه نستنتج أن وهذا يدل على أن تحسين الجوانب التقنية للأمن السيبراني، مثل أدوات الحماية الرقمية، الأتمتة، والمراقبة المستمرة، يرتبط بتحسن أداء سلسلة التوريد من حيث حماية المعلومات، سرعة الاستجابة، واستمرارية العمليات.

جدول رقم (26): العلاقة الارتباطية بين البعد البشري وأداء سلسلة التوريد

		البعد البشري
أداء سلسلة التوريد	ارتباط بيرسون	0.548
	الدلالة الإحصائية	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يبين الجدول رقم (26) وجود علاقة ارتباطية موجبة ومتوسطة القوة تميل إلى القوة بين البعد البشري للأمن السيبراني وأداء سلاسل التوريد، حيث بلغ معامل الارتباط 0.548، مع دلالة إحصائية قدرها 0.000، وهي أقل من 0.05.

ومنه نستنتج أن تحسين أداء سلاسل التوريد لا يعتمد فقط على الوسائل التقنية، بل يرتبط بدرجة كبيرة بوعي العنصر البشري وانضباطه داخل المؤسسة، فكلما كان الموظفون أكثر التزامًا بالإجراءات الأمنية وأكثر وعيًا بالمخاطر السيبرانية، زادت قدرة سلسلة التوريد على حماية معلوماتها، تقليل الأخطاء، والاستجابة بمرونة أكبر للتهديدات الرقمية.

جدول رقم (27): العلاقة الارتباطية بين البعد التعاوني وأداء سلسلة التوريد

		البعد التعاوني
أداء سلسلة التوريد	ارتباط بيرسون	0.405
	الدلالة الإحصائية	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يبين الجدول رقم (27) وجود علاقة ارتباطية موجبة وذات دلالة إحصائية بين البعد التعاوني في الأمن السيبراني وأداء سلاسل التوريد، حيث بلغ معامل الارتباط 0.405، مع دلالة إحصائية قدرها 0.000، وهي أقل من 0.05.

ومنه نستنتج إلى أن التعاون الأمني الرقمي يرتبط إيجابيًا بأداء سلاسل التوريد، إلا أن قوة العلاقة المحدودة نسبيًا تشير إلى أن هذا التعاون يحتاج إلى دعم أكبر من خلال وضوح الاتفاقيات، تحديد مسؤوليات حماية البيانات، وتوحيد آليات الاستجابة للمخاطر السيبرانية المشتركة.

ثانيا: اختبار الفرضيات

-الفرضية الرئيسية: "يوجد أثر للأمن السيبراني على أداء سلسلة التوريد"

- **التحليل الاحصائي**: لاختبار الفرضية الرئيسية المتعلقة بأثر الأمن السيبراني على أداء سلسلة التوريد ننظر إلى نتائج الجداول الثلاث الأساسية والمتمثلة في: Model Summary، ANOVA، وCoefficients.

جدول رقم (28): نتائج ملخص النموذج (**Model Summary**)

Model Summary			
R	R مربع	R مربع معدل	الخطأ المعياراي
.602	0,362	0,356	0,30492

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يبين جدول Model Summary أن قيمة معامل الارتباط R = 0.602 تشير إلى وجود علاقة موجبة متوسطة بين الأمن السيبراني وأداء سلسلة التوريد، أي أنه كلما تحسن مستوى الأمن السيبراني تحسن أداء

سلسلة التوريد، ونلاحظ أن معامل التحديد بلغ ($R^2 = 0.362$) وهذا يدل على أن الأمن السيبراني يفسر حوالي 36.2% من التغيرات في أداء سلسلة التوريد، وهي نسبة مقبولة في الدراسات الاجتماعية والاقتصادية.

جدول رقم (29): نتائج ANOVA للانحدار الخطي

ANOVA					
النموذج	مجموع المربعات	الفرق	متوسط التربيع	قيمة F	الدلالة الإحصائية Sig
الانحدار	5,178	1	5,178	55,694	0.000
الباقي	9,111	98	0,093		
المجموع	14,289	99			

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يبين جدول ANOVA أن قيمة الدلالة الإحصائية Sig = 0.000 وهي أقل من 0.05، وهذا يعني أن نموذج الانحدار ككل دال إحصائيًا ضمن حدود عينة الدراسة، مما يدعم قبول الفرضية الرئيسية.

جدول رقم (30): نتائج معاملات الانحدار الخطي Coefficients

Coefficients					
	المعاملات غير المعيارية		المعاملات المعيارية	قيمة t	الدلالة الإحصائية Sig
	قيمة B	الخطأ المعياري	بيتا		
الثابت	2,065	0,215	-	9,611	0,000
الأمن السيبراني	0,442	0,059	0,602	7,463	0,000

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

وعليه يمكن بناء نموذج تفسيري للأمن السيبراني وسلاسل التوريد وهو كالتالي:

$$Y = 2.065 + 0.442X$$

حيث أن(Y) سلاسل التوريد، و(X) الأمن السيبراني.

يتضح من جدول معاملات الانحدار الخطي البسيط أن قيمة معامل الانحدار غير المعياري **B** للأمن السيبراني بلغت **0.442**، وهي قيمة موجبة وهذا يدل على وجود أثر طردي للأمن السيبراني على أداء سلاسل

التوريد، ويعني ذلك أن ارتفاع مستوى تطبيق الأمن السيبراني بوحدة واحدة يؤدي إلى تحسن أداء سلاسل التوريد بمقدار **0.442** وحدة، كما بلغت قيمة معامل الانحدار المعياري **Beta = 0.602**، وهي تشير إلى قوة تأثير معتبرة للأمن السيبراني في تفسير التغير في أداء سلاسل التوريد، وبما أن قيمة الدلالة الإحصائية بلغت **0.000** وهي أقل من مستوى المعنوية **0.05** فإن الأثر دال إحصائيًا.

بناءً على نتائج الجداول السابقة نقبل الفرضية الرئيسية التي تنص على:" يوجد أثر ذو دلالة إحصائية للأمن السيبراني على تحسين أداء سلسلة التوريد"

وذلك لأن جميع المؤشرات الإحصائية خاصة قيمة Sig في جدول Coefficients أكدت وجود هذا الأثر بشكل واضح.

- **التفسير الاقتصادي:** مما سبق نصل إلى أن تحسين مستوى الأمن السيبراني داخل المؤسسات يساهم في تعزيز كفاءة وأداء سلسلة التوريد، أي كلما كانت الأنظمة المعلوماتية أكثر حماية قلت المخاطر المرتبطة بالاختراقات أو فقدان البيانات، وهو ما يضمن استمرارية العمليات اللوجستية دون انقطاع.، أي أن الأمن السيبراني لا يمثل فقط جانبًا تقنيًا بل أصبح عنصرًا اقتصاديًا مهمًا يساهم في تحسين الأداء وتعزيز القدرة التنافسية للمؤسسات من خلال دعم فعالية سلسلة التوريد.

- **التحليل الاحصائي: لاختبار الفرضيات الفرعية ننظر إلى جدول Coefficients(الانحدار المتعدد)**

جدول رقم (31): **نتائج الانحدار الخطي المتعدد**

Coefficients					
	المعاملات غير المعيارية		المعاملات المعيارية	قيمة t	الدلالة الإحصائية Sig
	قيمة B	الخطأ المعياري	بيتا		
الثابت	2,093	0,218		9,589	0,000
البعد التنظيمي	0,126	0,063	0,218	2,007	0,048
البعد التقني	0,026	0,086	0,039	0,298	0,767
البعد البشري	0,181	0,063	0,332	2,882	0,005
البعد التعاوني	0,097	0,060	0,158	1,615	0,110

المصدر: من إعداد الطالبتين بالاعتماد على مخرجات برنامج SPSS

يمكن بناء نموذج تفسيري لأبعاد الأمن السيبراني وسلاسل التوريد وهو كالتالي:

$$Y=2.093+0.126X1+0.026X2+0.181X3+0.097X4$$

Y: أداء سلالسل التوريد

X1:البعد التنظيمي

X2: البعد التقني

X3: البعد البشري

X4: البعد التعاوني

- من خلال الجدول أعلاه والمتمثل في الانحدار الخطي المتعدد يمكن اختبار الفرضيات الفرعية الأربع:

1. **اختبار الفرضية الفرعية الأولى**: المتعلقة بأثر البنية والسياسات الأمنية على تحسين أداء سلسلة التوريد.

يظهر من خلال الجدول أن قيمة الدلالة الإحصائية $Sig = 0.048$ وهي أقل من مستوى المعنوية (0.05)، هذا يدل على أن البعد التنظيمي له أثر معنوي على أداء سلسلة التوريد، أي أن هذا الأثر ليس عشوائيًا بل يمكن الاعتماد عليه إحصائيًا.

ونلاحظ أن معامل الانحدار $Beta = 0.126$ يظهر موجبا، أي أن العلاقة طردية كلما تحسنت البنية والسياسات الأمنية داخل المؤسسة تحسن أداء سلسلة التوريد.

ومن خلال هذه النتائج نقبل الفرضية الفرعية الأولى والتي مفادها: "يوجد أثر ذو دلالة إحصائية للبنية والسياسات الأمنية على تحسين أداء سلسلة التوريد"

- **التفسير الاقتصادي للفرضية الفرعية الأولى**: مما سبق نصل إلى أن وجود سياسات أمنية واضحة وبنية تنظيمية جيدة داخل المؤسسة يساعد على تنظيم العمل بشكل أفضل وحماية المعلومات من الأخطار، بالتالي التقليل من المشاكل والتوقفات في سير العمليات داخل سلسلة التوريد، ووضوح السياسات الأمنية يجعل التنسيق بين مختلف الأطراف أسهل وأسرع، مما يساهم في تحسين تدفق المعلومات والسلع داخل السلسلة، أي تحسين الجانب التنظيمي للأمن السيبراني يؤدي إلى رفع كفاءة الأداء وتقليل الخسائر ما ينعكس إيجابيًا على أداء سلسلة التوريد.

2. اختبار الفرضية الفرعية الثانية: "يوجد أثر ذو دلالة إحصائية للتكنولوجيا والحماية الرقمية على تحسين أداء سلسلة التوريد.

يظهر من خلال الجدول أن قيمة الدلالة الإحصائية $Sig = 0.767$ وهي أكبر من مستوى المعنوية (0.05)، هذا يدل على أن البعد التقني ليس له أثر معنوي على أداء سلسلة التوريد، أي أن هذا الأثر ليس حقيقيا بل يمكن الاستغناء عليه إحصائيًا.

ونلاحظ أن معامل الانحدار $Beta = 0.026$ يظهر ضعيف جدا، أي أن العلاقة طردية ضعيفة جدا أي أن لا توجد علاقة ذات دلالة إحصائية للتكنولوجيا والحماية الرقمية على تحسين أداء سلسلة التوريد.

- **ومن خلال هذه النتائج نرفض الفرضية الفرعية الثانية التي تنص على أنه:" يوجد أثر ذو دلالة إحصائية للتكنولوجيا والحماية الرقمية على تحسين أداء سلسلة التوريد. (حسب العينة)**

- **التفسير الاقتصادي للفرضية الثانية:** مما سبق نستنتج أن استخدام التكنولوجيا والحماية الرقمية وحده لا يكفي لتحسين أداء سلسلة التوريد في المؤسسة محل الدراسة، وقد يرجع ذلك إلى أن هذه الأدوات قد لا تكون مستغلة بشكل فعال، أو أن تأثيرها يحتاج إلى تكامل مع عناصر أخرى مثل الوعي البشري أو التنظيم الإداري حتى يظهر أثرها بشكل واضح.

3. اختبار الفرضية الفرعية الثالثة: "يوجد أثر ذو دلالة إحصائية للوعي الأمني لدى الموظفين على تحسين أداء سلسلة التوريد".

يظهر من خلال الجدول أن قيمة الدلالة الإحصائية $Sig = 0.005$ وهي أقل من مستوى المعنوية (0.05)، هذا يدل على أن البعد البشري له أثر معنوي على أداء سلسلة التوريد، أي أن هذا الأثر ليس عشوائيًا بل يمكن الاعتماد عليه إحصائيًا.

ونلاحظ أن معامل الانحدار $Beta = 0.181$ يظهر موجبا، أي أن العلاقة طردية كلما كان تحسن في مستوى الوعي الأمني لدى الموظفين داخل المؤسسة تحسن أداء سلسلة التوريد.

- **ومن خلال هذه النتائج نقبل الفرضية الفرعية الثالثة التي تنص على أنه: " يوجد أثر ذو دلالة إحصائية للوعي الأمني لدى الموظفين على تحسين أداء سلسلة التوريد"**

- **التفسير الاقتصادي للفرضية الفرعية الثالثة:** مما سبق نستنتج أن ارتفاع مستوى الوعي الأمني لدى الموظفين يساهم بشكل مباشر في تحسين أداء سلسلة التوريد، ويظهر ذلك جليا من خلال إدراك العاملين

للمخاطر السيبرانية بشكل كبير واتباعهم سلوكيات صحيحة في التعامل مع المعلومات يؤدي هذا إلى تقليل حدوث الأخطاء والمشاكل مثل تسريب البيانات أو تعطّل الأنظمة، مما يساعد على استمرار العمل بشكل منتظم، أي أن العنصر البشري الواعي يعتبر عاملًا مهمًا في رفع كفاءة الأداء وتقليل الخسائر داخل سلسلة التوريد.

4. اختبار الفرضية الفرعية الرابعة: "يوجد أثر ذو دلالة إحصائية للبعد التعاوني في الأمن السيبراني على تحسين أداء سلسلة التوريد".

- يظهر من خلال الجدول أن قيمة الدلالة الإحصائية $Sig = 0.110$ وهي أكبر من مستوى المعنوية (0.05)، هذا يدل على أن البعد التعاوني ليس له أثر معنوي على أداء سلسلة التوريد، أي أن هذا الأثر عشوائيًا بل يمكن الاستغناء عليه إحصائيًا.
- ونلاحظ أن معامل الانحدار $Beta = 0.097$ يظهر موجبا، أي أن العلاقة طردية متوسطة أن لا توجد علاقة ذات دلالة إحصائية للبعد التعاوني على تحسين أداء سلسلة التوريد.

- **من خلال هذه النتائج نرفض الفرضية الفرعية الرابعة التي مفادها: " يوجد أثر ذو دلالة إحصائية للبعد التعاوني في الأمن السيبراني على تحسين أداء سلسلة التوريد".**

- **التفسير الاقتصادي للفرضية الفرعية الرابعة:** مما سبق نستنتج أن التعاون بين مختلف الأطراف داخل المؤسسة أو مع الشركاء الخارجيين في مجال الأمن السيبراني يساعد على تحسين التنسيق وتبادل المعلومات بشكل أفضل، لكن بما أن هذا البعد لم يظهر أثرًا معنويًا في النتائج، فهذا يعني أن هذا التعاون الموجود لا ينعكس بشكل واضح على أداء سلسلة التوريد، وقد يكون تطبيقه غير كاف أو غير منظم بالشكل الذي يسمح بتحقيق نتائج اقتصادية ملموسة.

نتيجة عامة: توضح النتائج أن نموذج الانحدار كان دال إحصائيا، وهذا يعني أن الأمن السيبراني ككل له تأثير حقيقي على أداء سلسلة التوريد وليس مجرد صدفة في البيانات، بالمقابل في الانحدار المتعدد عند تفصيل الأمن السيبراني إلى أبعاده يظهر أن بعض الأبعاد فقط هي التي تؤثر بشكل واضح بينما أبعاد أخرى لا يظهر لها تأثير معنوي، ويرجع ذلك إلى أن التأثير الكلي يتوزع بين هذه الأبعاد وبالتالي قد يضعف أثر بعضها عند تحليلها بشكل منفصل داخل نفس النموذج.

- **ومن خلال تحليل الانحدار الخطي البسيط والانحدار الخطي المتعدد نصل إلى أن تحسين أداء سلسلة التوريد يعتمد أساسًا على الجوانب التنظيمية والبشرية في الأمن السيبراني أكثر من الجوانب التقنية والتعاونية، فوجود سياسات أمنية واضحة ورفع وعي الموظفين يساهم في تقليل الأخطاء وضمان استمرارية العمل بشكل أفضل، بالمقابل ضعف تأثير الجانب التقني والتعاوني يشير إلى أنهما غير كافيين لوحدهما لإحداث تحسين اقتصادي واضح.**

ومنه نصل إلى أن فعالية الأمن السيبراني تظهر بشكل أكبر عندما يكون مرتبطًا بتنظيم جيد ووعي بشري داخل المؤسسة.

المطلب الثاني: مناقشة نتائج الدراسة ومقارنتها مع نتائج الدراسات السابقة

الفرع الأول: مناقشة نتائج تبني استراتيجيات الأمن السيبراني

أولا: نتائج البعد التنظيمي

بينت النتائج النظرية لدراستنا الحالية أن الأمن السيبراني تجاوز كونه حماية تقنية أساسية بل أصبح أولوية استراتيجية ألزمها التحول الرقمي، وتتوافق هذه النتيجة مع ما توصلت إليه الدراسة (Abhijeet, Maximilian, Nigel, & Richard, 2020) بحيث أكدت على ضرورة التحول من الأسلوب التقني البحث إلى الأسلوب الإداري المشترك، وهو أيضا ما توصلت إليه دراسة (Afifi Mohamed Afifi , Abd Eltawab Hashem, & Abulsaoud Ahmed Younis, 2026) بأن الحد من مخاطر سلسلة التوريد السيبرانية أضحى ضرورة إدارية تساهم في استمرارية سلسلة التوريد، لأن سلاسل التوريد الحديثة تعتمد على التدفقات الرقمية فأي اختراق يؤدي إلى توقف السلسلة ومنه خسارة مالية، بينما تختلف دراستنا مع دارسة (Mohd, Nurul , Nik , & Zuraimi , 2021) التي تسلط الضوء على الفجوة البحثية التي تربط بين الأن السيبراني ومرونة السلسلة ضد الأزمات، فالدراسة الحالية قدمت إطار نظري شامل يربط الأمن بالاستمرارية مع محاولة سد الفجوة المعرفية وتقوية العلاقة بين الحماية السيبرانية والاستمرارية.

ثانيا: نتائج البعد التقني

من نتائج الدراسة الحالية أن دمج كل من تقنية البلوك شين والذكاء الاصطناعي تعطي سلسلة التوريد القدرة على الدفاع الإستباقي عوضا عن رد الفعل، وهذا ما توافقنا فيه دراسة (Alqudhaibi, et al., 2026) التي صرحت بضرورة التحول من رد الفعل إلى الوقاية الاستباقية القائمة على التنبؤ لمنع توقف الإنتاج، ونتفق ايضا مع دراسة (Sadiku, Chukwu, & Sadiku, 2023) بأن توظيف الذكاء الاصطناعي هو أساس التنبؤ بالهجمات السيبرانية، ونجد اختلاف في التوجه البحثي الذي كان من نتائج دراسة (Mohd,

(Nurul , Nik , & Zuraimi , 2021 بأن 25% من الأبحاث تحصر دور التكنولوجيا كأداة التأمين البحث على خلاف الدراسة الحالية بأن التكنولوجيا نظام استباقي متكامل.

ثالثا: نتائج البعد البشري

توصلت الدراسة الحالية إلى أن العنصر البشري هو المحرك الأساسي عن نجاح المنظومة وغياب الوعي يعد ثغرة لا تسد بالحلول التقنية، وتتوافق هذه النتيجة مع دراسة (Abhijeet, Maximilian, Nigel, & Richard, 2020) بأن زيادة الوعي ضرورة حتمية لتعزيز المرونة السيبرانية، بينما اختلفت الدراسة الحالية عن دراسة (Sadiku, Chukwu, & Sadiku, 2023) التي ركزت على المكونات التقنية بينما أثبتت الدراسة الحالية نظريا أن تدريب سلوك الموظف ووعيه هما الأساس قبل الأنظمة التقنية، وهذا ما يبرر الموظفين يعتبرون الخط الأول للدفاع في الدراسة الحالية.

رابعا: نتائج البعد التعاوني

من النتائج المتوصل إليها أن أمن سلسلة التوريد هو مسؤولية جماعية تعتمد على التعاون وتدفق المعلومات بين جميع مكونات السلسلة، وهذا ما يتوافق مع ما أشارت إليه دراسة (Aikaterin & Costas, 2026) التي تشير بأن الفجوة الأمنية في نقص الرؤية تجاه الموردين والشركاء الخارجيين، بينما تختلف الدراسة الحالية مع دراسة (Abhijeet, Maximilian, Nigel, & Richard, 2020) التي صنفت التهديدات في السمعة والتشغيل والاستراتيجية، لكن الدراسة الحالية وسعت البعد التعاوني ليشمل المسؤولية القانونية التشاركية.

الفرع الثاني: مناقشة نتائج الإطار النظري لسلاسل التوريد

أولا: نتائج الكفاءة التشغيلية

من النتائج المتوصل إليها نظريا أن سلاسل التوريد أضحت نظام متفاعل يربط بين كل من التدفق المادي والمعلوماتي والمالي، بحيث يجب وجود رؤية شاملة وهذا ما ينتج عن تشابك سلسلة التوريد الحديثة ، بالإضافة إلى أن تحسين الخدمة يعد معيار للجودة والكفاءة، وهذا ما يتوافق تماما مع دراسة (Sadiku, Chukwu, & Sadiku, 2023) التي بينت إلزامية الحفاظ على أمان كل التدفقات لضمان وصول الخدمة للمستهل النهائي، ونجد دراسة (Aikaterin & Costas, 2026) وجدت أ، المخاطر في المنتجات المشترات فقط لكن يختلف مع الدراسة الحالية لأن المفهوم أوسع ويشمل اللوجستيات العكسية لأن في السلاسل الحديثة تميزت بأنها دائرية، فحماية البيانات والمنتجات عند الاسترجاع ضرورة حتمية لضمان جودة وكفاءة خدمة العميل ومنه رضا العميل.

ثانيا: المرونة الرقمية

كانت من النتائج المتوصل لها أن فعالية الأداء اللوجيستي مرتبطة بأمان التدفق المعلوماتي، بينما الأمن السيبراني هو أساس مرونة سلسلة التوريد التي تتميز بالتنبؤ للهجمات أو التعافي السريع منها، وتتوافق هذه الاخيرة

مع دراسة (Hlynskyy, Dovhun, & Pochopień, 2025) بأن ادارة المخاطر السيبرانية مع التحول الرقمي المتسارع هو شرط أساسي للاستمرارية، ونجد أيضا أن دراسة (Abhijeet, Maximilian, Nigel, & Richard, 2020) بينت أهمية المرونة لاستعادة نشاط السلسلة، بينما اختلفت دراستنا مع دراسة (Mohd, Nurul , Nik , & Zuraimi , 2021) التي أشارت على فجوة في دراسة المرونة أي وجود افتقار بحثي في دراسة المرونة بشكل كافي، أما في درايتنا الحالية أكدت على أن قوة أمان الأنظمة الرقمية يضمن وصول المنتجات في الوقت المناسب.

ثالثا: نتائج التنافسية والموثوقية

توصلت دراستنا إلى أ، دعم الذكاء الاصطناعي لأنظمة المؤسسة تحقق رؤية شاملة، وهذا ما يجعل الحماية الرقمية ليست مجرد آلية دفاعية فقط بل ميزة تنافسية تعزز ثقة الشركاء، وهذا ما يتطابق مع دراسة (Alqudhaibi, et al., 2026) في أن الذكاء الاصطناعي له القدرة على حماية الاستثمارات، وهذا ما يؤكد أن، التكنولوجيا وتقنياتها وسيلة تحقق الشفافية للعملاء والشركاء بالإضافة إلى أنها في الأصل أداة تحد من المخاطر، ونجد في دراسة (Sadiku, Chukwu, & Sadiku, 2023) بحيث تعتبر أن الأمن السيبراني مجرد برامج حماية، في حين تركز الدراسة الحالية على استغلال قوة الحماية في انشاء هوية تسويقية للمؤسسة وهي الأمان، وهذا بكل تأكيد ما يمكن المؤسسة من اكتساح السوق، لأن هذا السبب الأول في اختيار التعامل مع مؤسسة عن غيرها.

خلاصة الفصل

قمنا خلال هذا الفصل بدراسة في مختلف المؤسسات عبر ربوع الوطن بهدف تحليل ودراسة أثر الأمن السيبراني على تحسين أداء سلاسل التوريد، حيث قمنا بتوزيع استبيانات لتجميع البيانات مع الموظفين والإطارات بالمؤسسات وقمنا بتحليل الاستبيانات ومعالجتها اعتمادا على برنامج spss، حيث قمنا بعرض نتائج الدراسة، ثم اختبار فرضيات الدراسة ومناقشة نتائج الدراسة ومقارنتها مع نتائج الدراسات السابقة

خاتمة

الخاتمة

تعد سلسلة التوريد في العصر الرقمي الشريان الحيوي الذي يغذي الكيان الاقتصادي للمؤسسات، غير أن هذا الشريان بات عرضة لتهديدات سيبرانية متزايدة تتجاوز في خطورتها المخاطر اللوجستية التقليدية. لقد انطلقت هذه الدراسة من تأصيل نظري أكد أن الأمن السيبراني لم يعد مجرد خيار تقني تكميلي، بل استراتيجية جوهرية تهدف إلى حماية سلامة وسرية وتوافر المعلومات التي تتدفق عبر حلقات السلسلة. ففي بيئة أعمال تتسم بالتعقيد والترابط الرقمي، يصبح أي اختراق لمعلومات التوريد بمثابة شلل يصيب القيمة المضافة للمؤسسة، وهو ما جعلنا نتبنى رؤية شاملة تنظر إلى الأمن السيبراني كمنظومة متكاملة تضم السياسات التنظيمية، والوسائل التقنية، والوعي البشري، والجهود التعاونية المشتركة بين كافة الفاعلين.

إن المراجعة الأدبية والنظرية مكنتنا من استيعاب أن الأداء المتميز لسلاسل التوريد لم يعد يُقاس فقط بالسرعة والتكلفة، بل بمدى (المرونة السيبرانية) وقدرة السلسلة على الصمود أمام الهجمات الرقمية وضمان استمرارية الأعمال. وذلك من خلال تقليل مخاطر الانقطاع وتعزيز ثقة الشركاء. وبناءً على هذا الربط المنهجي بين أمن المعلومات وكفاءة العمليات، سعى الجانب الميداني للدراسة لاختبار مدى تحقق هذه الفلسفة النظرية على أرض الواقع في المؤسسات محل الدراسة.

أولا: النتائج

- ✓ تحول الأمن السيبراني من مجرد (حماية تقنية) إلى (أولوية استراتيجية) وإدارية تضمن استمرارية سلاسل التوريد.
- ✓ يُعتبر العنصر البشري المحرك الأساسي للمنظومة، ووعي الموظف هو خط الدفاع الأول الذي لا يمكن للحلول التقنية وحدها سد ثغراته.
- ✓ أمن السلسلة مسؤولية جماعية تتطلب تدفق المعلومات بين الشركاء وتتضمن "مسؤولية قانونية تشاركية".
- ✓ المرونة الرقمية: يرتبط الأداء اللوجيستي بـــ "أمان التدفق المعلوماتي"، حيث يضمن الأمن السيبراني قدرة السلسلة على "التعافي السريع" وضمان وصول المنتجات في وقتها.
- ✓ الحماية السيبرانية ليست مجرد أداة دفاعية، بل هي "ميزة تنافسية" تعزز ثقة الشركاء وتساهم في بناء "هوية تسويقية" آمنة للمؤسسة

- ✓ تعتمد المؤسسات محل الدراسة على نخبة من الكوادر ذات المستوى التعليمي العالي، مما يضمن وجود وعي مؤسساتي كافٍ للتعامل مع المفاهيم المعقدة للأمن السيبراني.
- ✓ تمتاز القوى العاملة في هذه المؤسسات بتوازن مثالي بين الخبرات الميدانية العريقة والطاقات الشابة، وهو مزيج ضروري لضمان استقرار العمليات اللوجستية مع سرعة التكيف مع التقنيات الرقمية الحديثة.
- ✓ يعكس التوزيع الوظيفي داخل المؤسسات حداثة تخصص الأمن السيبراني في الهياكل التنظيمية، حيث لا تزال هذه المؤسسات في مراحلها التأسيسية لدمج أنظمة الحماية الرقمية ضمن أنشطتها اللوجستية التقليدية.
- ✓ تتركز الدراسة بشكل أساسي في المؤسسات الكبيرة ذات الطابع الخدمي، وهي البيئات الأكثر احتياجاً لتأمين تدفق البيانات الحساسة عبر سلاسل التوريد نظراً لضخامة عملياتها وتعقيدها.
- ✓ تشير الخصائص العامة للمؤسسات محل الدراسة إلى أن النتائج المتوصل إليها تتمتع بمصداقية عالية، كونها نابعة من كفاءات بشرية مؤهلة مهنياً وعلمياً وتواجه التهديدات السيبرانية بشكل مباشر في بيئة عملها.

ثانيا: اختبار الفرضيات

- **الفرضية الأولى: نقبل الفرضية الفرعية الأولى والتي مفادها: "يوجد أثر ذو دلالة إحصائية للبنية والسياسات الأمنية على تحسين أداء سلسلة التوريد"** لأنه تبين لدى المؤسسات محل الدراسة وجود سياسات أمنية واضحة وبنية تنظيمية جيدة تساعد على تنظيم العمل بشكل أفضل وحماية المعلومات من الأخطار

- **الفرضية الثانية: نرفض الفرضية الفرعية الثانية التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية للتكنولوجيا والحماية الرقمية على تحسين أداء سلسلة التوريد"** وذلك راجع إلى أن هذه الأدوات قد لا تكون مستغلة بشكل فعال، أو أن تأثيرها يحتاج إلى تكامل مع عناصر أخرى مثل الوعي البشري أو التنظيم الإداري حتى يظهر أثرها بشكل واضح.

- **الفرضية الثالثة: نقبل الفرضية الفرعية الثالثة التي تنص على أنه: "يوجد أثر ذو دلالة إحصائية للوعي الأمني لدى الموظفين على تحسين أداء سلسلة التوريد".** ويظهر ذلك جليا من خلال إدراك الموظفين للمخاطر السيبرانية بشكل كبير واتباعهم سلوكيات صحيحة في التعامل مع المعلومات يؤدي هذا إلى تقليل حدوث الأخطاء والمشاكل مثل تسريب البيانات أو تعطّل الأنظمة.

- **الفرضية الرابعة: نرفض الفرضية الفرعية الرابعة التي مفادها: "يوجد أثر ذو دلالة إحصائية للبعد التعاوني في الأمن السيبراني على تحسين أداء سلسلة التوريد"**. فهذا يعني أن هذا التعاون الموجود في المؤسسات محل الدراسة لا ينعكس بشكل واضح على أداء سلسلة التوريد، وقد يكون تطبيقه غير كاف أو غير منظم بالشكل الذي يسمح بتحقيق نتائج اقتصادية ملموسة.

ثالثا: التوصيات

على ضوء نتائج الدراسة المتوصل إليها، يمكن طرح التوصيات الموالية، والتي تتمثل في بعض الإجراءات التي من شأنها أن تزيد من فاعلية تدابير الأمن السيبراني في تحسين أداء سلاسل التوريد:

- ✓ وضع برامج استراتيجية لتدعيم عملية استخدام التقنيات الحديثة والأنظمة الذكية في مراقبة وتأمين تدفقات السلع والمعلومات، مع تخصيص موازنات لتوفير الإمكانات المادية والبشرية اللازمة لحماية هذه البنية التحتية.
- ✓ الحرص على تقديم برامج تدريبية دورية لجميع الفاعلين في سلسلة التوريد (موظفين، موردين، وشركاء) حول ثقافة الأمن الرقمي، لمساعدتهم على الاستخدام الأمثل للبرامج والتقنيات اللوجستية وتنمية مهاراتهم في التصدي للاختراقات.
- ✓ خلق وظائف رشيقة ومستحدثة متخصصة في إدارة المخاطر السيبرانية اللوجستية وتطوير أنظمة دفاعية استباقية.
- ✓ الاستفادة من تجارب الدول المتقدمة في مجال (سلاسل التوريد الرقمية الآمنة)ومحاولة تكييف أفضل الممارسات العالمية بما يتوافق مع بيئة المؤسسات المحلية.
- ✓ نشر الوعي والثقافة الرقمية لدى جميع أطراف السلسلة، مما يساعد في اتخاذ قرارات سليمة مبنية على بيانات مشفرة ومحمية.
- ✓ تعزيز التعاون والشراكة مع الجامعات ومراكز البحث العلمي ومختبرات الأمن السيبراني لابتكار حلول تقنية محلية تساهم في حماية الأمن القومي الاقتصادي.

رابعاً: آفاق الدراسة

في ختام بحثنا هذا، وبناءً على النتائج المتوصل إليها، نقترح لكم بعض المواضيع التي من شأنها أن تكمل ما تم التوصل إليه في هذا البحث، وهي كالآتي:

- أثر تقنيات "البلوكشين" (Blockchain) في تعزيز موثوقية وأمن سلاسل التوريد.
- دور الذكاء الاصطناعي في التنبؤ بالهجمات السيبرانية قبل وقوعها في المؤسسات اللوجستية.
- نظام العمل عن بعد في الأقسام اللوجستية ودوره في زيادة الثغرات السيبرانية.
- أثر الاستثمار في الأمن السيبراني على القيمة السوقية والسمعة المؤسسية لشركات النقل والإمداد.

المراجع

قائمة المراجع

أولا: المراجع باللغة العربية

1. شويرب جيلالي / دمراد فائزة. (2023). مفهوم الحروب السيبرانية و الأمن السيبراني . *مجلة الحقوق والحريات* ، 164.
2. شيرين محمد غازي. (2022). *ادارة اللوجسيات وسلاسل الامداد* . رأس البر : المعهد العالي للادارة والحاسب الالي .
3. شريفة كلاع. (27 أفريل , 2022). الأمن السيبراني وتحديات الجوسسة والاختراقات الالكترونية للدول عبر الفضاء السيبراني.
4. ياسين مليح، و يونس مليح . (31 جويلية , 2021). الأمن السيبراني بالمغرب : الواقع والتحديات في ظل جائحة فيروس كورونا كوفيد -19.
5. بدر الحيمودي. (27 أفريل , 2023). الأمن السيبراني و حماية الأنظمة المعلوماتية . *مجلة شمال افريقيا للنشر العلمي* .
6. ماريا فالنتينا، و أيلينا باتينو رودريغيز فيماندو خيسوس كارمن . (6 نوفمبر , 2024). الأمن السيبراني في البحر : مراجعة أدبيات لتأثيرات الهجمات السيبرانية والدفاعات في سلالسل التوريد البحرية. صفحة 02.
7. نزار هلينسكي، و دوفون جولانتا بوشوبين أوكسانا . (15 جانفي , 2025). الرقمنة و الأمن السيبراني في الشركات و سلاسل التوريد :التحديات والفرص .
8. كلاوديا سيسيري، و كانياتو أنطونيلا موريتو فيديريكو . (10 جانفي , 2026). دمج قدرات الذكاء الاصطناعي في ادارة مخاطر الأمن السيبراني لسلاسل التوريد .
9. أيكاترينا لاتسيو، و لامبرينوداكيس كوستاس . (22 جانفي , 2026). ادارة مخاطر سلاسل التوريد السيبرانية :من التهديدات الى المعالجة.
10. ماثيو ن.أو .صادق، و جانيت صادق أوكاي سي تشوكو . (2023). الأمن السيبراني في سلاسل التوريد .
11. وداد بوطلاعة، و منال بوكورو. (26 ديسمبر, 2022). الهجمات السبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام. *مجلة حقوق الانسان و الحريات العامة*.
12. فاطمة على إبراهيم أحمد ، أ.د. رحاب يوسف، و عيد د. وليد. (2022). الأمن السيبراني والنظافة الرقمية. *المجلة المصرية لعلوم المعلومات*، 390-422.
13. ابراهيم أحمد، و فاطمة علي. (2022). الأمن السيبراني و النظافة الرقمية. *المجلة الرسمية لعلوم المعلومات*، 397_398.
14. عادل القضيب، ماجد البراك عبد المحسن الوسيل، عمرو منشي ثامر الشريف، و ساندیب جاجتاب كونستانتينوس سالونيتيس. (06 ديسمبر, 2026). الأمن السيبراني الاستبقائي في الصناعة : مراجعة لمنهجيات التنبؤ بالتهديدات السيبرانية في أنظمة التصنيع.

15.منار سعيد الكندي، و نصرة سبيح الهنائي ربيع رمضان حور الكلباني . (2025). أمن سلسلة التوريد في نظم المعلومات : دراسة مسحية.

16.تانيا واليس، و دوري بول. (03 جويلية, 2024). ممارسات التعاون من أجل الأمن السيبراني لسلاسل التوريد الخاصة بالبنية التحتية الحيوية.

17.فائزة دمراد، و جيلالي دشويب. (20 أفريل, 2023). مفهوم الحروب السيبرانية والأمن السيبراني.

18.جعفر سعدي. (2020). *ادارة سلاسل التوريد وأهميتها في تحسين أداء المؤسسة*. ورقلة: جامعة قاصدي مرباح ورقلة.

19.سليمان قطاف، و عبد الحليم بوقرين. (26 جويلية, 2023). الأليات الموضوعية والأجرائية المتبعة لتحقيق الأمن السيبراني (الجزائر نمذجا).

20.فتيحة حزام. (2020). *حماية الأنظمة الرقمية بين الآليات التقنية وأجهزة الحماية*. بومرداس: مجلة الحقوق و العلوم الأنسانية.

21.عوسات تكليت. (2022). تقنية البلوك تشين : دراسة في المفهوم والعناصر. *مجلة العلوم القانونية و الاجتماعية*، 941-952.

22.خضرة صادوق، و خيرة نيل. (96-110). *تطبيقات إنترنت الآشياء في المكتبات: دراسة نظرية*. وهران: جامعة احمد بن بلة وهران.

23.غسان الطالب. (20 03, 2026). *الأمن السيبراني وإدارة مخاطره في مجال الأعمال*. تم الاسترداد من الغد: https://cutt.ly/gBTCv7U

24.فيصل محمد عسيري. (15 03, 2026). *الأمن السيبراني وحماية أمن المعلومات*. تم الاسترداد من كتب: https://www.kutub.info/library/book/21854

25.المادة الثانية من قانون الأمن السيبراني الأردني. (بلا تاريخ).

26.مصطفى ابراهيم سلمان الشمري. (2021). الأمن السيبراني وأثره في الأمن الوطني العراقي. *مجلة العلوم القانونية و السياسية*، 147-190.

27.د.ممدوح عبد العزيز الرفاعي. (2016). *"إدارة سلاسل التوريد" مدخل تحليلي*. كلية التجارة، جامعة عين شمس.

28.فارس حسام مصاروة. (2019). *أثر تكنولوجيا المعلومات على تكامل إدارة سلسلة التوريد*. جامعة الشرق الأوسط.

29.منير عزوز. (2018). *أثر فعالية إدارة سلسلة التوريد على أداء العمليات الإنتاجية في المؤسسات الصناعية*. المسيلة: جامعة محمد بوضياف – المسيلة.

30.فوكي هيكامب، بان روبن دوس لي ، و تروخيو راسوا وسوشميتا روج رولاندو . (14 جانفي, 2024). تحليل أمني منهجي لأنظمة التتبع القائمة على المسار في سلاسل التوريد المدعوة بتقنية FRID.

ثانيا: المراجع باللغة الأجنبية

1. Wallis, T., & Dorey, P. (2024). Collaboration Practices for the Cybersecurity of Supply Chains to Critical Infrastructure. *applied sciences*, 16.

2. Hlynskyy, N., Dovhun, O., & Pochopień, J. (2025). Digitalization and cybersecurity in companies and supply chains: challenges and opportunities. *Scientific Journal of Bielsko-Biala School of Finance and Law*, 53-59.
3. Sadiku, M. N., Chukwu, U. C., & Sadiku, J. O. (2023). Cybersecurity in Supply Chain. *International Journal of Innovative Analyses and Emerging Technology*, 31-40.
4. Said Al-Kindi, M., Alkalbani, H., Al-Hinai, N. S., & Ramadan, R. A. (2025). Supply Chain Security in Information Systems: A Survey. *PLOMS Journal of Artificial Intelligence*, 17.
5. Anurag, D. (2025). Digital Supply Chains and Cybersecurity- Strategies for Protection and Risk Mitigation. *International Research Journal of Engineering & Applied Sciences*, 10-18.
6. Hugh Boyes .(2025) .Cybersecurity and Cyber-Resilient Supply Chains . *Technology Innovation Management Review*.34–28 ،
7. Solfa, F. D. (2022). IMPACTS OF CYBER SECURITY AND SUPPLY CHAIN RISK ON DIGITAL OPERATIONS: EVIDENCE FROM THE UAE PHARMACEUTICAL INDUSTRY. *International Journal of Technology, Innovation and Management (IJTIM)*, 18-31.
8. Sylwi, K., & Zbigniew, B. (2024). Cyberattacks as Threats in Supply Chains. *European Research Studies Journal*, 778-796.
9. Aikaterin, L., & Costas, L. (2026). Cyber Supply Chain Risk Management: From Threats to Treatment. *International Journal of Information Security*, 11.
10. Abhijeet, G., Maximilian, W., Nigel, D., & Richard, W. (2020). Managing cyber risk in supply chains: A review and research agenda. *Heriot-Watt University*, 223-240.
11. Jon. Boyens ،Angela. Smith ،Nadya. Bartol ،Kris. Winkler ،Alex. Holbrook ، وFallon Matthew .(2024) .Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations .*National Institute of Standards and Technology U.S. Department of Commerce*.
12. Ciceri Claudia ،Caniato Federico و ،Moretto Antonella .(2026) .Integrating artificial intelligence capabilities in supply chain cyber risk management . *International Journal of Physical Distribution & Logistics Management*.
13. Valentina Clavijo Mesa, M., Elena Patino-Rodriguez, C., & Jesus Guevara Carazas, F. (2024). Cybersecurity at Sea: A Literature Review of Cyber-AttackImpacts and Defenses in Maritime Supply Chains. *MDPI*, 11-15.
14. Alqudhaibi, A., Albarrak, M., Aloseel, A., Munshi, A., Alsharif, T., Jagtap, S., & Salonitis, K. (2026). Proactive cybersecurity in industry 4.0: a survey of cybersecurity threatprediction approaches in manufacturing systems. *International Journal of Information Security* , 14-25.

15. Modarress-Fathi, B., Ansari , A., & Ansa, A. (2026, Januray 6). *Risks on Sustainable Supply Chain and Logistics*. Retrieved from preprints.org: https://www.preprints.org/manuscript/202601.0183
16. Ahi, K., Agrawal, V., & Valizadeh, S. (2026, Feb 22). *LLM Scalability Risk for Agentic-AI and Model Supply Chain Security*. Retrieved from arXiv: https://arxiv.org/abs/2602.19021
17. Ghasemshirazi , S., Shirvani, G., Ranjbar Tavakoli , M., Ghaedi, B., & Amin Langarizadeh, M. (2026, jul 31). *Implementing Zero Trust Architecture to Enhance Security and Resilience in the Pharmaceutical Supply Chain*. Retrieved from arXiv: https://arxiv.org/abs/2508.15776
18. Afifi Mohamed Afifi , Y., Abd Eltawab Hashem, A., & Abulsaoud Ahmed Younis, R. (2026). The Anatomy of a Good Concept: A Systematic Review on Cyber Supply Chain Risk Management. *MDPI*, 18-45.
19. Ciceri, C., Caniato, F., & Moretto, A. (2026). Integrating artificial intelligence capabilities in supply chain cyber risk management. *International Journal of Physical Distribution & Logistics Management*, 38.
20. *MHUV*. (2026, Avril 20). Retrieved from https://www.mhuv.gov.dz/?p=5041&lang=fr
21. Fahed Al-Khatib, S., Yousef Ibrahim, Y., & Alnadi, M. (2024). Cybersecurity Practices and Supply Chain Performance: The Case of Jordanian Banks. *MDPI*, 27.
22. Rakshit Dr. Pushpendu .(2024) .Impact of Cyber Security measurements adopted by supply chain management companies in Navi Mumbai .*JETIR*-9 ، .17
23. Mohd, N., Nurul , A., Nik , S., & Zuraimi , A. (2021). CYBER SECURITY IN SUPPLY CHAIN MANAGEMENT: A SYSTEMATIC REVIEW. *LogForum*, 49-57.
24. Constance, O., Okpala, C., & Nkemakonam , C. (2024). Enhancing SmartManufacturingSupplyChainsThrough CybersecurityMeasures. *International Journal of Engineering Inventions*, 1-6.

ثالثا: المواقع الالكترونية

1. *Algeria Telecom*. (2026, Avril 15). Retrieved from https://www.algerietelecom.dz/
2. *ENAFOR*. (2026, Avril 20). Retrieved from https://www.enafor.dz/
3. *ENAC*. (2026, Avril 20). Retrieved from https://www.enac-dz.com/
4. *SARPI*. (2026, Avril 20). Retrieved from https://sarpi.dz
5. *halliburton*. (2026, Avril 20). Retrieved from https://www.halliburton.com/
6. *Bayat Catering*. (2026, Avril 20). Retrieved from https://www.bayat-catering.com/

الملاحق

ملحق 1: الاستبيان

– جامعة قاصدي مرباح –ورقلة–
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم المناجمنت

إستبيان

السادة و السيدات: يشرفني أن أتقدم إلى سيادتكم الموقرة بهذه الاستمارة التي تدخل ضمن متطلبات نيل شهادة الماستر إدارة أعمال وإمداد، والتي تناقش موضوع " **أثر الأمن السيبراني على تحسين أداء سلاسل التوريد** "، حيث نطمح من خلالها إلى التعرف على أراءكم القيمة، كما أعلمكم أن الإجابات المقدمة من طرفكم تحظى بالأهمية البالغة لدينا، والسرية التامة ولن تستخدم إلا لغرض البحث العلمي. جزيل الشكر على حسن التعاون.

ومن أجل الإجابة يكفي فقط وضع X في الخانة المناسبة

البيانات الأساسية

1. السن: من 20 إلى 30 سنة ☐ من 31 إلى 40 سنة ☐ من 41 إلى 50 سنة ☐ من 51 فما فوق ☐
2. المستوى التعليمي: ثانوي ☐ جامعي ☐ دراسات عليا ☐
3. عدد سنوات الخبرة: أقل من 5 سنوات ☐ من 5 إلى 10 سنوات ☐ من 11 إلى 20 سنة ☐ أكثر من 20 سنة. ☐
4. الوظيفة: الأمن السيبراني ☐ اللوجستيك ☐
5. حجم المؤسسة: مؤسسة كبيرة ☐ مؤسسة متوسطة ☐ مؤسسة صغيرة ☐ مؤسسة مصغرة ☐
6. نوع القطاع: صناعية ☐ تجارية ☐ خدماتية ☐

المحور الأول: قياس أبعاد الأمن السيبراني

II	أبعاد الأمن السيبراني	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
	البعد الأول: البعد التنظيمي					
1	تلتزم الإدارة العليا بتوفير الموارد المالية اللازمة لتطبيق استراتيجية الأمن السيبراني					
2	توجد سياسات أمنية واضحة ومصرح بها تحدد مسؤوليات الموظفين في حماية البيانات					
3	يقتصر التدقيق على الأنظمة الرقمية على الحالات الطارئة فقط مما يسمح بوجود ثغرات أمنية					
4	يتعاون قسم تكنولوجيا المعلومات مع قسم اللوجستيك لتعزيز الأمن السيبراني					
	البعد الثاني: البعد التقني					
5	تتبنى المؤسسة إجراءات مشددة للمصادقة لمنع الوصول غير المصرح به للبيانات					
6	تفتقر أنظمة النسخ الاحتياطي للتلقائية مما يؤخر استعادة البيانات عند وقوع الهجمات السيبرانية					
7	تعتمد المؤسسة على تقنيات متقدمة (الذكاء الاصطناعي) للتنبؤ بالتهديدات السيبرانية المحتملة					
8	تعتمد المؤسسة على استراتيجية التحديث المستمر للأنظمة التشغيلية للحد من الثغرات الأمنية					
	البعد الثالث: البعد البشري					
9	يبدي الموظفون عدم التزام تام بتغيير كلمات المرور الخاصة بهم بشكل دوري					
10	تحرص المؤسسة على التدريب الدوري المستمر لتطوير أداء الموظفين في التعامل مع المخاطر الرقمية					
11	يساهم الموظف الواعي في تقليل مخاطر هجمات الهندسة الاجتماعية وأي بريد مشبوه					

12	يمتلك الكادر التقني المهارات اللازمة للتصرف السريع واحتواء الهجمات السيبرانية فور وقوعها					
	البعد الرابع: البعد التعاوني في الأمن السيبراني					
13	تعتمد المؤسسة منصات رقمية موحدة مع الموردين والشركاء لإدارة ومراقبة المخاطر السيبرانية المشتركة					
14	تفرض المؤسسة معايير أمنية محددة على الموردين لتأمين سلامة سلسلة التوريد					
15	تتضمن الاتفاقيات مع الموردين عدم وضوح في إجراءات حماية وسرية البيانات المتبادلة					
16	تبادل المعلومات بشكل فوري بين الشركاء بشأن التهديدات السيبرانية المحددة					

المحور الثاني: أداء سلسلة التوريد

III	أبعاد سلاسل التوريد	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
البعد الأول: الكفاءة التشغيلية						
17	يساهم الأمن السيبراني في تقليص زمن توقف العمليات الناتجة عن الاختراقات					
18	تلعب سلامة البيانات دور مهم في دقة التنبؤ بالطلب المستقبلي في سلسلة التوريد					
19	يؤدي ضعف سلامة البيانات إلى عدم القدرة على تخفيض التكاليف اللوجستية الإضافية					
20	تساعد الأنظمة الآمنة في تحسين سرعة تدفق المعلومات بين جميع حلقات السلسلة					
21	تواجه المؤسسة عدم القدرة على استغلال مواردها المعلوماتية نتيجة ضعف الرقابة الأمنية					
البعد الثاني: جودة الخدمة ورضى العملاء						
22	يعزز ضمان سرية بيانات الزبائن في رفع مستويات الولاء للمؤسسة والثقة في خدماتها					

23	ترفع الحماية السيبرانية موثوقية المؤسسة وتزيد من قدرتها على تسليم الطلبيات في الوقت المناسب					
24	تفتقر بعض الخدمات لعدم خلوها من التلاعب بالبيانات نتيجة ضعف سلامة الأنظمة					
25	يسبب الضعف التقني عدم شفافية تتبع الشحنات عبر حلقات السلسلة					
البعد الثالث: الاستمرارية والمرونة						
26	تمتع سلسلة التوريد بالقدرة على الاستمرارية حتى في ظل الهجمات الرقمية					
27	تساهم خطط الاستجابة السريعة في تقليل الزمن اللازم لعودة العمليات إلى طبيعتها بعد وقوع الأزمة السيبرانية					
28	يدعم دمج الحماية في العمليات في تقليص حجم الخسائر المالية الناجمة عن انقطاع التوريد					
29	يظهر أداء المؤسسة عدم القدرة على التكيف السريع مع المتغيرات الرقمية المفاجئة في السوق					

❖ **شكرا جزيلا على تعاونكم ومساهمتكم في إنجاح هذه الدراسة، يرجى التأكد من عدم ترك أي سؤال دون إجابة.**

ملحق 2: قائمة المحكمين

الرقم	إسم ولقب الأستاذ المحكم	المنصب
01	أميناش ليندة	أستاذة تعليم عالي
02	بن عمارة الطاهر	أستاذ محاضر "ب"

ملحق 3: مخرجات SPSS

Reliability Statistics

Cronbach's Alpha	N of Items
.816	16

Reliability Statistics

Cronbach's Alpha	N of Items
.681	13

Reliability Statistics

Cronbach's Alpha	N of Items
.852	29

Frequencies

Statistics

		السن ((العمر	ماهو مستواك التعليمي؟	كم عدد سنوات الخبرة في المؤسسة؟	ماهي وظيفتك الحالية في المؤسسة؟	ماهو حجم المؤسسة؟
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0

Statistics

		ماهو نوع القطاع الذي تنشط به؟
N	Valid	100
	Missing	0

Frequency Table

السن ((العمر

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	من 20 إلى 30 سنة	27	27.0	27.0	27.0
	من 31 إلى 40 سنة	32	32.0	32.0	59.0
	من 41 إلى 50 سنة	34	34.0	34.0	93.0
	من 51 فما فوق	7	7.0	7.0	100.0
	Total	100	100.0	100.0	

ماهو مستواك التعليمي؟

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	ثانوي	6	6.0	6.0	6.0
	جامعي	75	75.0	75.0	81.0
	دراسات عليا	19	19.0	19.0	100.0
	Total	100	100.0	100.0	

كم عدد سنوات الخبرة في المؤسسة؟

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أقل من 5 سنوات	30	30.0	30.0	30.0
	من 5 إلى 10 سنوات	22	22.0	22.0	52.0
	من 11 إلى 20 سنة	31	31.0	31.0	83.0
	أكثر من 20 سنة	17	17.0	17.0	100.0
	Total	100	100.0	100.0	

ماهي وظيفتك الحالية في المؤسسة؟

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	الأمن السيبراني	22	22.0	22.0	22.0
	اللوجستيك	78	78.0	78.0	100.0
	Total	100	100.0	100.0	

ماهو حجم المؤسسة؟

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	مؤسسة كبيرة	60	60.0	60.0	60.0
	مؤسسة متوسطة	27	27.0	27.0	87.0
	مؤسسة صغيرة	11	11.0	11.0	98.0
	مؤسسة مصغرة	2	2.0	2.0	100.0
	Total	100	100.0	100.0	

ماهو نوع القطاع الذي تنشط به؟

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	صناعية	23	23.0	23.0	23.0
	تجارية	18	18.0	18.0	41.0
	خدماتية	59	59.0	59.0	100.0
	Total	100	100.0	100.0	

Explore

Descriptives

			Statistic	Std. Error
الأمن_السيبراني	Mean		3.5913	.05176
	95% Confidence Interval for Mean	Lower Bound	3.4886	
		Upper Bound	3.6939	
	5% Trimmed Mean		3.6063	
	Median		3.6250	
	Variance		.268	
	Std. Deviation		.51756	
	Minimum		2.13	
	Maximum		4.75	
	Range		2.63	
	Interquartile Range		.63	
	Skewness		-.454	.241
	Kurtosis		.225	.478
سلاسل_التوريد	Mean		3.6515	.03799
	95% Confidence Interval for Mean	Lower Bound	3.5762	
		Upper Bound	3.7269	
	5% Trimmed Mean		3.6436	
	Median		3.6154	
	Variance		.144	
	Std. Deviation		.37992	
	Minimum		2.69	
	Maximum		4.92	
	Range		2.23	
	Interquartile Range		.52	
	Skewness		.406	.241
	Kurtosis		.738	.478

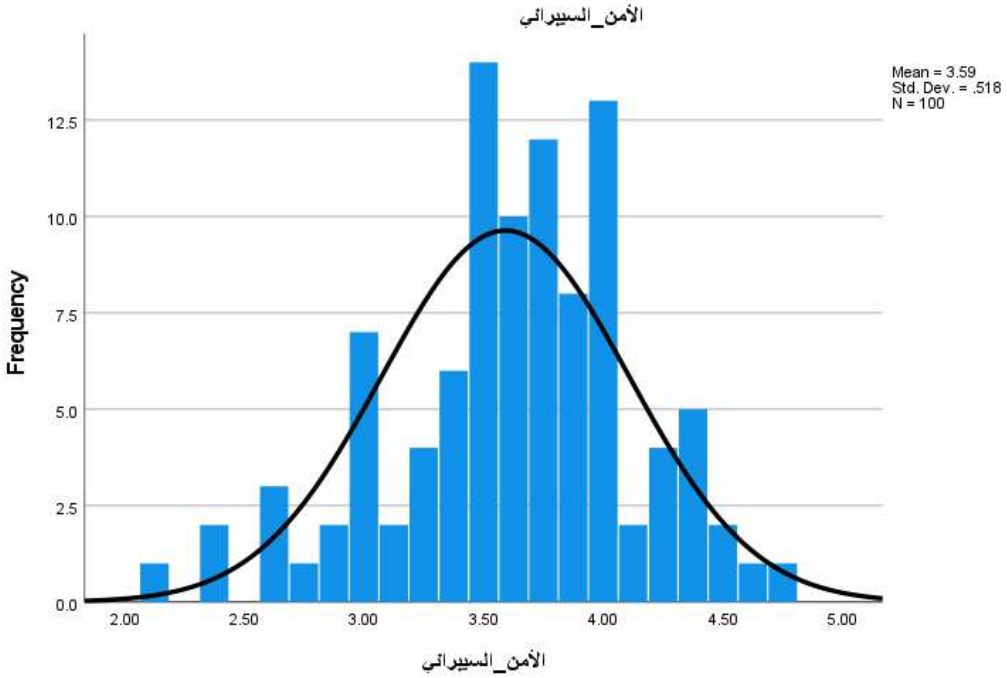
Tests of Normality

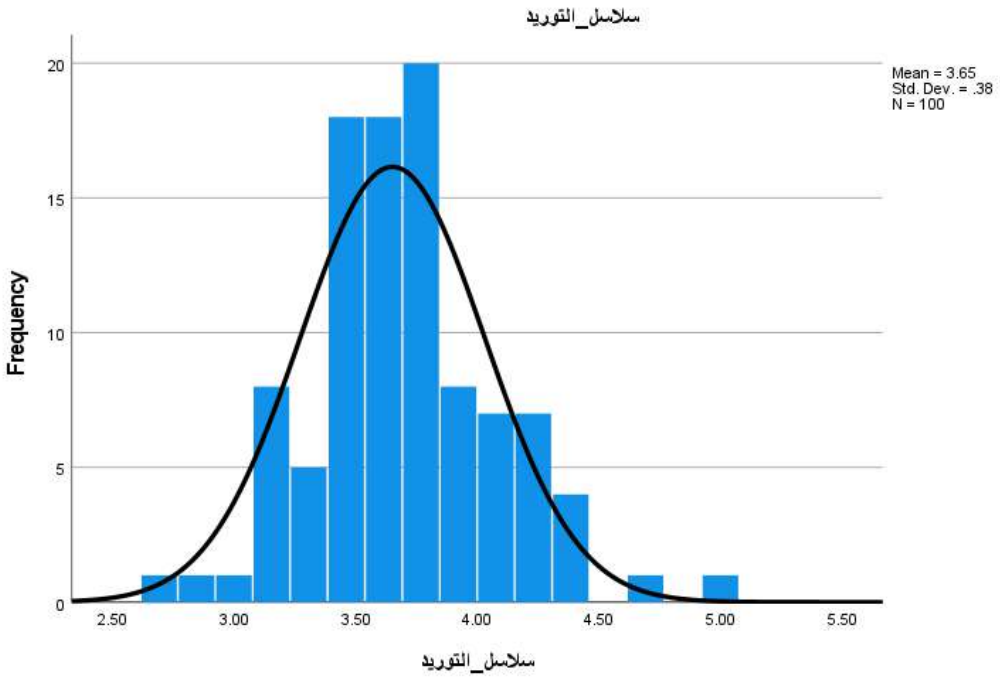
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
الأمن_السيبراني	.103	100	.011	.980	100	.126
سلاسل_التوريد	.107	100	.006	.980	100	.137

a. Lilliefors Significance Correction

Frequencies

Histogram





Frequencies

Statistics

		ماهو نوع القطاع الذي تنشط به؟	تلتزم الإدارة العليا بتوفير الموارد المالية اللازمة لتطبيق استراتيجية الأمن السيبراني	توجد سياسات أمنية واضحة ومصرح بها تحدد مسؤوليات الموظفين في حماية البيانات	يقتصر التدقيق على الأنظمة الرقمية على الحالات الطارئة فقط مما يسمح بوجود ثغرات أمنية	يتعاون قسم تكنولوجيا المعلومات مع قسم اللوجستيك لتعزيز الأمن السيبراني
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		2.36	4.23	4.15	2.75	4.00
Std. Deviation		.835	.908	.903	1.132	.910

Statistics

		تتبنى المؤسسة إجراءات مشددة للمصادقة لمنع الوصول غير المصرح به للبيانات	تفتقر أنظمة النسخ الاحتياطي للتلقائية مما يؤخر استعادة البيانات عند وقوع الهجمات السيبرانية	تعتمد المؤسسة على تقنيات متقدمة (الذكاء الاصطناعي) للتنبؤ بالتهديدات السيبرانية المحتملة	تعتمد المؤسسة على استراتيجية التحديث المستمر للأنظمة التشغيلية للحد من الثغرات الأمنية	يبدي الموظفون عدم التزام تام بتغيير كلمات المرور الخاصة بهم بشكل دوري
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		4.18	2.73	3.28	3.91	2.73
Std. Deviation		.809	1.024	1.181	.986	1.162

Statistics

		تحرص المؤسسة على التدريب الدوري المستمر لتطوير أداء الموظفين في التعامل مع المخاطر الرقمية	يساهم الموظف الواعي في تقليل مخاطر هجمات الهندسة الاجتماعية وأي بريد مشبوه	يمتلك الكادر التقني المهارات اللازمة للتصرف السريع واحتواء الهجمات السيبرانية فور وقوعها	تعتمد المؤسسة منصات رقمية موحدة مع الموردين والشركاء لإدارة ومراقبة المخاطر السيبرانية المشتركة	تفرض المؤسسة معايير أمنية محددة على الموردين لتأمين سلامة سلسلة التوريد
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		3.71	4.30	3.85	3.65	3.73
Std. Deviation		1.217	.704	.957	1.038	1.004

Statistics

		تتضمن الاتفاقيات مع الموردين عدم وضوح في إجراءات حماية وسرية البيانات المتبادلة	تبادل المعلومات بشكل فوري بين الشركاء بشأن التهديدات السيبرانية المحددة	يساهم الأمن السيبراني في تقليص زمن توقف العمليات الناتجة عن الاختراقات	تلعب سلامة البيانات دور مهم في دقة التنبؤ بالطلب المستقبلي في سلسلة التوريد	يؤدي ضعف سلامة البيانات إلى عدم القدرة على تخفيض التكاليف اللوجستية الإضافية
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		2.70	3.56	4.20	4.17	3.88
Std. Deviation		1.049	.946	.636	.711	.891

Statistics

		تساعد الأنظمة الآمنة في تحسين سرعة تدفق المعلومات بين جميع حلقات السلسلة	تواجه المؤسسة عدم القدرة على استغلال مواردها المعلوماتية نتيجة ضعف الرقابة الأمنية	يعزز ضمان سرية بيانات الزبائن في رفع مستويات الولاء للمؤسسة والثقة في خدماتها	ترفع الحماية السيبرانية موثوقية المؤسسة وتزيد من قدرتها على تسليم الطلبيات في الوقت المناسب	تفتقر بعض الخدمات لعدم خلوها من التلاعب بالبيانات نتيجة ضعف سلامة الأنظمة
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		4.18	3.56	4.31	4.17	2.46
Std. Deviation		.770	1.008	.775	.779	.958

Statistics

		يسبب الضعف التقني عدم شفافية تتبع الشحنات عبر حلقات السلسلة	تمتع سلسلة التوريد بالقدرة على الاستمرارية حتى في ظل الهجمات الرقمية	تساهم خطط الاستجابة السريعة في تقليل الزمن اللازم لعودة العمليات إلى طبيعتها بعد وقوع الأزمة السيبرانية	يدعم دمج الحماية في العمليات في تقليص حجم الخسائر المالية الناجمة عن انقطاع التوريد	يظهر أداء المؤسسة عدم القدرة على التكيف السريع مع المتغيرات الرقمية المفاجئة في السوق
N	Valid	100	100	100	100	100
	Missing	0	0	0	0	0
Mean		2.17	3.64	4.13	4.10	2.50
Std. Deviation		.842	.894	.720	.785	.990

Correlations

Correlations

		سلاسل_التوريد	البعد_التنظيمي	البعد_التقني	البعد_البشري	البعد_التعاوني
سلاسل_التوريد	Pearson Correlation	1	.498**	.494**	.548**	.405**
	Sig. (2-tailed)		.000	.000	.000	.000
	N	100	100	100	100	100
البعد_التنظيمي	Pearson Correlation	.498**	1	.636**	.572**	.412**
	Sig. (2-tailed)	.000		.000	.000	.000
	N	100	100	100	100	100
البعد_التقني	Pearson Correlation	.494**	.636**	1	.687**	.557**
	Sig. (2-tailed)	.000	.000		.000	.000
	N	100	100	100	100	100
البعد_البشري	Pearson Correlation	.548**	.572**	.687**	1	.407**
	Sig. (2-tailed)	.000	.000	.000		.000
	N	100	100	100	100	100
البعد_التعاوني	Pearson Correlation	.405**	.412**	.557**	.407**	1
	Sig. (2-tailed)	.000	.000	.000	.000	
	N	100	100	100	100	100
الأمن_السيبراني	Pearson Correlation	.602**	.812**	.879**	.832**	.723**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	100	100	100	100	100

Correlations

		الأمن_السيبراني
سلاسل_التوريد	Pearson Correlation	.602**
	Sig. (2-tailed)	.000
	N	100
البعد_التنظيمي	Pearson Correlation	.812**
	Sig. (2-tailed)	.000
	N	100
البعد_التقني	Pearson Correlation	.879**
	Sig. (2-tailed)	.000
	N	100

البعد_البشري	Pearson Correlation	.832**
	Sig. (2-tailed)	.000
	N	100
البعد_التعاوني	Pearson Correlation	.723**
	Sig. (2-tailed)	.000
	N	100
الأمن_السيبراني	Pearson Correlation	1
	Sig. (2-tailed)	
	N	100

**. Correlation is significant at the 0.01 level (2-tailed).

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	الأمن_السيبراني[b]	.	Enter

a. Dependent Variable: سلاسل_التوريد
b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.602[a]	.362	.356	.30492

a. Predictors: (Constant), الأمن_السيبراني

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.178	1	5.178	55.694	.000[b]
	Residual	9.111	98	.093		

	Total	14.289	99			

a. Dependent Variable: سلاسل_التوريد
b. Predictors: (Constant), الأمن_السيبراني

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.065	.215		9.611	.000
	الأمن_السيبراني	.442	.059	.602	7.463	.000

a. Dependent Variable: سلاسل_التوريد

Regression

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	البعد_التعاوني, البعد_البشري, البعد_التنظيمي, البعد_التقني[b]	.	Enter

a. Dependent Variable: سلاسل_التوريد
b. All requested variables entered.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.612[a]	.374	.348	.30686

a. Predictors: (Constant), البعد_التعاوني, البعد_البشري, البعد_التنظيمي, البعد_التقني

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	5.344	4	1.336	14.188	.000[b]
	Residual	8.946	95	.094		
	Total	14.289	99			

a. Dependent Variable: سلاسل_التوريد

b. Predictors: (Constant), البعد_التعاوني, البعد_البشري, البعد_التنظيمي, البعد_التقني

Coefficients[a]

Model		Unstandardized Coefficients B	Standardized Coefficients Std. Error	Beta	t	Sig.
1	(Constant)	2.093	.218		9.589	.000
	البعد_التنظيمي	.126	.063	.218	2.007	.048
	البعد_التقني	.026	.086	.039	.298	.767
	البعد_البشري	.181	.063	.332	2.882	.005
	البعد_التعاوني	.097	.060	.158	1.615	.110

a. Dependent Variable: سلاسل_التوريد