



جامعة قاصدي مرباح ، ورقلة - الجزائر
كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قسم علوم التسيير

مذكرة مقدمة لإستكمال متطلبات شهادة الماستر في العلوم التسيير

شعبة علوم التسيير , تخصص إدارة اعمال

بعنوان:

مساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال

" دراسة ميدانية لعينة من البنوك الوطنية الجزائرية في منطقة ورقلة "

من إعداد الطالبتين:

داهش شيماء

بوليف ايمان هبة الرحمان

نوقشت بتاريخ: 24/05/2026

امام اللجنة المكونة من السادة:

(استاذة تعليم العالي - جامعة قاصدي مرباح ورقلة) رئيسا

(استاذة محاضر ب - جامعة قاصدي مرباح ورقلة) مشرفا ومقررا

(استاذ تعليم العالي - جامعة قاصدي مرباح ورقلة) مناقشا

أ/ قداش سميرة

أ.د/ بن زين ايمان

أ/عراية الحاج

السنة الجامعية : 2025-2026



جامعة قاصدي مرباح ، ورقلة - الجزائر
كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قسم علوم التسيير

مذكرة مقدمة لإستكمال متطلبات شهادة الماستر في العلوم التسيير

شعبة علوم التسيير , تخصص إدارة اعمال

بعنوان:

مساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال

" دراسة ميدانية لعينة من البنوك الوطنية الجزائرية في منطقة ورقلة "

من إعداد الطالبتين:

داهش شيماء

بوليف ايمان هبة الرحمان

نوقشت بتاريخ: 24/05/2026

امام اللجنة المكونة من السادة:

رئيسا	(استاذ تعليم العالي - جامعة قاصدي مرباح ورقلة)
مشرفا ومقررا	(استاذ تعليم العالي - جامعة قاصدي مرباح ورقلة)
مناقشا	(الرتبة العلمية - جامعة قاصدي مرباح ورقلة)

أ/قداش سمية
أ.د/ بن زين ايمان
أ/عرابة الحاج

السنة الجامعية : 2025-2026

الاهداء

الحمد لله الذي وفقني لإتمام هذا العمل المتواضع

أهدي ثمرة جهدي هذا إلى أعز الناس على قلبي، إلى من كانا سندي ودعائي الدائم، إلى والديّ العزيزين، أطال الله في عمرهما، اللذين غرسا في حب العلم والعمل، وكانا سببًا فيما وصلت إليه اليوم

وإلى عائلتي الكريمة وإخوتي الأعزاء

زينب , معاذ , سدره , ياسين , آلاء

الذين كانوا دائمًا مصدر دعم وتشجيع لي في مسيرتي الدراسية

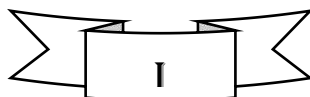
كما أهدي هذا العمل إلى صديقة عمري تيمن بوثليجة التي كانت إلى جانبي بالكلمة الطيبة والتشجيع الدائم

. طيلة حياتي الجامعية

وإلى زميلتي و صديقتي العزيزة في إعداد هذه المذكرة شيماء داهش ، التي شاركتني هذا العمل وساهمت معي في إنجازه

أسأل الله أن يجزيهم جميعًا خير الجزاء

بوليف ايمان هبة الرحمان



بسم الله الرحمن الرحيم

الحمد لله الذي وفقني لإتمام هذا العمل، وجعل ثمرة جهدي خطوة في طريق العلم والنجاح.

أهدي هذا الإنجاز بكل حب وامتنان إلى أغلى ما أملك في هذه الحياة، إلى من كانا سندي ودعائي في كل خطوة، إلى والديّ العزيزين، أطال الله في عمرهما، اللذين لم يدخرا جهدًا في دعمي وتربيّتي على حب العلم والطموح، فلهما مني كل الشكر والعرفان.

كما أهدي هذا العمل إلى أمي الغالية وأبي العزيز، تقديرًا لما قدّماه لي من تضحية وصبر، وأسأل الله أن يجزيهما عني خير الجزاء.

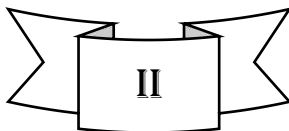
وإلى إخوتي الأعزاء، عبد حكيم، ويحي و مصطفى، الذين كانوا دائمًا إلى جانبي بدعمهم وتشجيعهم، فكانوا خير سند في مسيرتي.

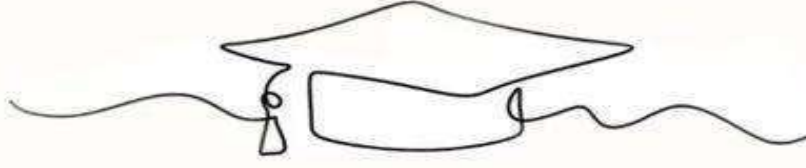
وإلى زوجة أخي الغالية فطومة، التي كانت مثالًا للطيبة والدعم، فجزاها الله عني كل خير.

كما لا يفوتني أن أهدي هذا العمل إلى زميلتي في إعداد هذه المذكرة، إيمان هبة الرحمن بوليف، التي شاركتني هذا الجهد خطوة بخطوة، وكان لتعاونها أثر كبير في إنجاز هذا العمل.

أسأل الله أن يوفق الجميع ويجزيهم عنا خير الجزاء.

داهش شيماء





شكر وتقدير

بكل عبارات الشكر والامتنان، أتقدم بخالص الشكر والتقدير إلى أستاذتنا المشرفة إيمان بن زين، على توجيهاتها القيّمة ونصائحها السديدة، التي كان لها الأثر الكبير في إتمام هذا العمل.

ولا يفوتني أن أتقدم بجزيل الشكر إلى كافة الأساتذة الكرام الذين أشرفوا على تكويننا طوال مسيرتنا الدراسية، من بدايتها إلى نهايتها، وكان لهم الفضل فيما وصلنا إليه اليوم. كما أتوجه بالشكر إلى الجامعة التي احتضنت هذا العمل وساهمت في توفير الظروف المناسبة لإنجازه.

وفي الأخير، أتقدم بالشكر لكل من ساهم من قريب أو بعيد، بشكل مباشر أو غير مباشر، في إنجاز هذا العمل، ولو بكلمة طيبة.

الملخص:

تهدف هذه الدراسة إلى إبراز مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال داخل البنوك الجزائرية، من خلال دراسة ميدانية شملت مجموعة من البنوك الناشطة على مستوى ولاية ورقلة وبلدية حاسي مسعود، . واعتمدت هذه الدراسة على المنهج الوصفي التحليلي، بالإضافة إلى الدراسة الميدانية باستخدام الاستبيان كأداة رئيسية لجمع البيانات، حيث تم توزيع 10 استبيانات على مسؤولي أمن نظام المعلومات بالبنوك محل الدراسة، وتم تحليل البيانات باستخدام برنامج SPSS الإصدار 27. وقد توصلت الدراسة إلى جملة من نتائج من بينها اعتماد البنوك محل الدراسة على تطبيق أبعاد أمن نظام المعلومات بمستوى مرتفع، كما تبين وجود مستوى فعال لإدارة استمرارية الأعمال داخل هذه البنوك. وأظهرت نتائج التحليل الإحصائي وجود علاقة ارتباطية ضعيفة أي بنسبة منخفضة بين أمن نظام المعلومات وإدارة استمرارية الأعمال. كما أكدت الدراسة أهمية الأنظمة المعلوماتية المعتمدة داخل البنوك في تعزيز حماية البيانات وتقليل المخاطر وضمان استمرارية الخدمات البنكية في مختلف الظروف.

الكلمات المفتاحية: أمن نظام المعلومات، إدارة استمرارية الأعمال، سرية المعلومات، سلامة المعلومات، توافر المعلومات، البنوك

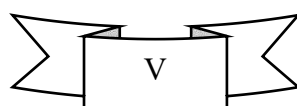
الجزائرية، نظم المعلومات البنكية.

Abstract:

This study aims to highlight the contribution of Information Systems Security to supporting Business Continuity Management within Algerian banks through a field study conducted on a group of active banks located in Ouargla Province and the municipality of Hassi Messaoud. The study adopted the descriptive-analytical approach, in addition to a field study using a questionnaire as the main data collection tool. A total of 10 questionnaires were distributed to Information Systems Security officers in the banks under study, and the collected data were analyzed using SPSS version 27. The study yielded several findings, most notably that the banks under study implement the dimensions of Information Systems Security at a high level. The results also indicated an effective level of Business Continuity Management within these banks. Statistical analysis revealed a weak correlation, with a low percentage, between Information Systems Security and Business Continuity Management. Furthermore, the study confirmed the importance of the information systems adopted by banks in enhancing data protection, reducing risks, and ensuring the continuity of banking services under various circumstances.

Keywords:

Information System Security, Business Continuity Management, Confidentiality, Integrity, Availability, Algerian Banks, Banking Information Systems



قائمة المحتويات

رقم الصفحة	قائمة المحتويات
I-II	اهداء
III	شكر وتقدير
IV -V	ملخص الدراسة
VI- VII	فهرس المحتويات
VIII-IX -X	قائمة الجداول
XI- XII	قائمة الاشكال
XIII	قائمة الملاحق
XIV -XV	قائمة المختصرات
١-ط	مقدمة
	الفصل الاول: الادبيات النظرية و التطبيقية لأمن نظام المعلومات واستمرارية الاعمال
2	تمهيد
3	المبحث الأول: ماهية امن نظام المعلومات
2-11	المطلب الاول: مفهوم امن نظام المعلومات
11-16	المطلب الثاني: اساسيات امن نظام المعلومات
16-20	المطلب الثالث: مخاطر امن نظم المعلومات والتدابير المتخذة
20	المبحث الثاني ماهية ادارة استمرارية الاعمال
21-27	المطلب الاول مفهوم ادارة استمرارية الاعمال
27-33	المطلب الثاني: معايير نظام إدارة الاستمرارية الاعمال وفق ISO22301
33-35	المطلب الثالث: العلاقة بين امن نظام المعلومات وإدارة استمرارية الاعمال
36	المبحث الثالث: الدراسات السابقة المتعلقة بأمن نظام المعلومات وإدارة استمرارية الاعمال
36-50	المطلب الاول: الدراسات السابقة المتعلقة بأمن نظام المعلومات وإدارة استمرارية الاعمال
50-54	المطلب الثاني: ابعاد امن نظام المعلومات وادارة استمرارية الاعمال
54-60	المطلب الثالث: مقارنة بين الدراسات السابقة والدراسة الحالية
61-62	خلاصة الفصل الأول
	الفصل الثاني: الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال للبنوك الجزائرية وكالة بورقلة ورقلة
64	تمهيد
64	المبحث الأول: الطريقة والأدوات المستخدمة في الدراسة الميدانية
64-85	المطلب الأول: الطريقة المعتمدة في الدراسة

قائمة المحتويات

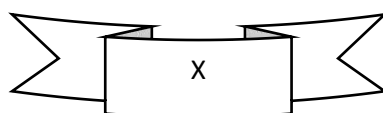
85-90	المطلب الثاني: أداة تقديم الدراسة
90-92	المطلب الثالث : أدوات الإحصائية المستخدمة
92	المبحث الثاني: عرض ومناقشة النتائج
92-153	المطلب الأول: عرض وتحليل نتائج محاور الدراسة
153-160	المطلب الثاني: عرض وتحليل نتائج اختبار فرضيات الدراسة
160-170	المطلب الثالث: مناقشة الدراسة
171-172	خلاصة الفصل الثاني
173-175	خاتمة
177-180	قائمة المراجع
182-202	الملاحق
204-209	الفهرس

قائمة الجداول

الجدول	عنوان الجدول	الصفحة
01-01	اختلاف والعلاقة بين امن نظام المعلومات ونظام المعلومات والامن السيبراني	7
01-02	فرق بين معايير امن نظام المعلومات	15
01-03	ابعاد امن نظام المعلومات من الدراسات السابقة	50
01-04	ابعاد ادارة استمرارية الاعمال من الدراسات السابقة	53
01-05	ملخص الدراسات السابقة	55
02-01	متغيرات الدراسة	66
02-02	احصائيات الاستبيانات الموزعة والمسترجعة على عينة	77
02-03	توزيع العينة حسب اسم البنك	78
02-04	توزيع العينة حسب نوع البنك	80
02-05	توزيع العينة حجم البنك	81
02-06	توزيع العينة حسب توفر النظام المعلوماتي	83
02-07	توزيع العينة حسب وجود خطة استمرارية الاعمال	84
02-08	توزيع درجات التطبيق في سلم التقدير الخماسي	88
02-09	ترميز خصائص نوع البنك	89
02-10	ترميز خصائص حجم البنك	89
02-11	تقدير معامل الثبات	90
02-12	توزيع اجابات افراد العية حول مدى الاعتماد على سياسية امن المعلومات	93
02-13	توزيع اجابات افراد العية حول مدى الاعتماد على التحكم في الوصول	94
02-14	توزيع اجابات افراد العية حول مدى الاعتماد على المصادقة	96
02-15	توزيع اجابات افراد العية حول مدى الاعتماد على سياسة كلمات المرور	97
02-16	توزيع اجابات افراد العية حول مدى الاعتماد على التشفير	99
02-17	توزيع اجابات افراد العية حول مدى الاعتماد على التوعية الامينة	100
02-18	توزيع اجابات افراد العية حول مدى الاعتماد على سجلات التدقيق	102
02-19	توزيع اجابات افراد العية حول مدى الاعتماد على التحقق من صحة البيانات	103
02-20	توزيع اجابات افراد العية حول مدى الاعتماد على كشف التلاعب	105

قائمة الجداول

106	توزيع اجابات افراد العية حول مدى الاعتماد على تقسيم الصلاحيات	02-21
108	توزيع اجابات افراد العية حول مدى الاعتماد على امن قواعد البيانات	02-22
109	توزيع اجابات افراد العية حول مدى الاعتماد على انظمة التنبيه الامني	02-23
110	توزيع اجابات افراد العية حول مدى الاعتماد على استمرارية الخدمة	02-24
112	توزيع اجابات افراد العية حول مدى الاعتماد على النسخ الاحتياطي	02-25
113	توزيع اجابات افراد العية حول مدى الاعتماد على استرجاع البيانات	02-26
115	توزيع اجابات افراد العية حول مدى الاعتماد على مراقبة الانظمة	02-27
116	توزيع اجابات افراد العية حول مدى الاعتماد على البنية التحتية البديلة	02-28
118	توزيع اجابات افراد العية حول مدى الاعتماد على ادارة الصيانة	02-29
119	متوسطات الحسابية والانحرافات المعيارية للاجابات افراد العينة حول سرية المعلومات	02-30
121	متوسطات الحسابية والانحرافات المعيارية للاجابات افراد العينة حول سلامة المعلومات	02-31
122	متوسطات الحسابية والانحرافات المعيارية للاجابات افراد العينة حول توافر المعلومات	02-32
124	احصائيات الوصفية للابعاد امن نظام المعلومات	02-33
124	ترتيب عبارات المتغير امن نظام المعلومات حسب درجة الموافقة لدى افراد العينة	02-34
127	توزيع اجابات افراد العية حول مدى الاعتماد على خطة استمرارية	02-35
128	توزيع اجابات افراد العية حول مدى الاعتماد على مراجعة الخطة	02-36
130	توزيع اجابات افراد العية حول مدى الاعتماد على خطة التعافي	02-37
132	توزيع اجابات افراد العية حول مدى الاعتماد على فريق الازمات	02-38
133	توزيع اجابات افراد العية حول مدى الاعتماد على زمن الاستجابة	02-39
135	توزيع اجابات افراد العية حول مدى الاعتماد على اجراءات الطوارئ	02-40
136	توزيع اجابات افراد العية حول مدى الاعتماد على سجل المخاطر	02-41
138	توزيع اجابات افراد العية حول مدى الاعتماد على تقييم المخاطر	02-42
139	توزيع اجابات افراد العية حول مدى الاعتماد على زمن الاسترجاع	02-43
141	توزيع اجابات افراد العية حول مدى الاعتماد على معيار ادارة استمرارية الاعمال	02-44
142	المتوسطات الحسابية والانحرافات المعيارية للاجابات العينة حول ادارة استمرارية الاعمال	02-45



قائمة الجداول

144	المتوسطات الحسابية والانحرافات المعيارية للمتغيري الدراسة	02-46
146	الاحصائيات الوصفية لمستوى امن نظام المعلومات وادارة استمرارية الاعمال	02-47
149	نتائج اختبار التوزيع الطبيعي حسب نوع البنك	02-48
150	الاحصائيات الوصفية للمتغيرات الدراسة حسب حجم البنك	02-49
153	نتائج اختبار التوزيع الطبيعي حسب حجم المؤسسة	02-50
154	مصفوفة الارتباط للابعد امن نظام المعلومات	02-51
155	مصفوفة الارتباط للمتغيرات الدراسة	02-52
157	الاحصائيات الوصفية لمستوى متغيري الدراسة حسب نوع البنك	02-53
157	نتائج اختبار Test T لقياس الفروق حسب نوع البنك	02-54
157	تحليل الاحادي الخاص بامن نظام المعلومات	02-55
160	اختبار Kruskal-Wallis	02-56

قائمة الاشكال

الصفحة	عنوان الشكل	الشكل
ط	نموذج الدراسة	01
9	اهداف تحقيق امن المعلومات	01-01
25	دورة حياة إدارة استمرارية الاعمال	02-01
51	يوضح ابعاد امن نظام المعلومات	03-01
79	توزيع العينة حسب اسم البنك	01-02
80	توزيع العينة حسب نوع البنك	02-02
82	توزيع العينة حسب حجم البنك	03-02
82	توزيع العينة حسب حجم البنك	04-02
83	توزيع العينة حسب توفر النظام المعلوماتي	05-02
84	توزيع العينة حسب وجود خطة استمرارية الاعمال	06-02
93	توزيع اجابات افراد العية حول مدى الاعتماد على سياسية امن المعلومات	07-02
95	توزيع اجابات افراد العية حول مدى الاعتماد على التحكم في الوصول	08-02
96	توزيع اجابات افراد العية حول مدى الاعتماد على المصادقة	09-02
98	توزيع اجابات افراد العية حول مدى الاعتماد على سياسة كلمات المرور	10-02
99	توزيع اجابات افراد العية حول مدى الاعتماد على التشفير	11-02
101	توزيع اجابات افراد العية حول مدى الاعتماد على التوعية الامنية	12-02
102	توزيع اجابات افراد العية حول مدى الاعتماد على سجلات التدقيق	13-02
104	توزيع اجابات افراد العية حول مدى الاعتماد على التحقق من صحة البيانات	14-02
105	توزيع اجابات افراد العية حول مدى الاعتماد على كشف التلاعب	15-02
107	توزيع اجابات افراد العية حول مدى الاعتماد على تقسيم الصلاحيات	16-02
108	توزيع اجابات افراد العية حول مدى الاعتماد على امن قواعد البيانات	17-02
109	توزيع اجابات افراد العية حول مدى الاعتماد على انظمة الاتبيه الامني	18-02
111	توزيع اجابات افراد العية حول مدى الاعتماد على استمرارية الخدمة	19-02
112	توزيع اجابات افراد العية حول مدى الاعتماد على النسخ الاحتياطي	20-02

قائمة الاشكال

114	توزيع اجابات افراد العية حول مدى الاعتماد على استرجاع البيانات	21-02
115	توزيع اجابات افراد العية حول مدى الاعتماد على مراقبة الانظمة	23-02
117	توزيع اجابات افراد العية حول مدى الاعتماد البنية التحتية البديلة	24-02
118	توزيع اجابات افراد العية حول مدى الاعتماد على ادارة الصيانة	25-02
127	توزيع اجابات افراد العية حول مدى الاعتماد على خطة استمرارية الاعمال	26-02
129	توزيع اجابات افراد العية حول مدى الاعتماد على مراجعة الخططة	27-02
131	توزيع اجابات افراد العية حول مدى الاعتماد على خطة التعافي	28-02
132	توزيع اجابات افراد العية حول مدى الاعتماد على فريق ادارة الازمات	29-02
134	توزيع اجابات افراد العية حول مدى الاعتماد على زمن الاستجابة	30-02
135	توزيع اجابات افراد العية حول مدى الاعتماد على اجراءات الطوارئ	31-02
137	توزيع اجابات افراد العية حول مدى الاعتماد على سجل المخاطر	32-02
138	توزيع اجابات افراد العية حول مدى الاعتماد على تقييم المخاطر	33-02
140	توزيع اجابات افراد العية حول مدى الاعتماد على زمن استرجاع	34-02
141	توزيع اجابات افراد العية حول مدى الاعتماد على معيار ادارة استمرارية الاعمال	35-02

قائمة الملاحق

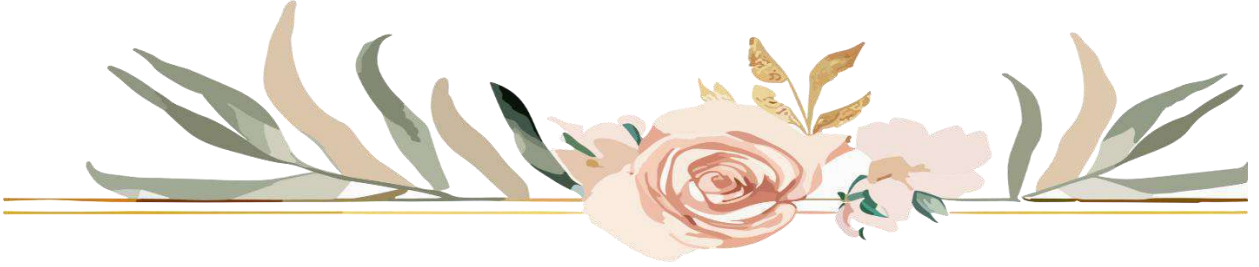
الملاحق	عنوان الملاحق	رقم الصفحة
01	استمارة الاستبيان	182
02	حول معيار ISO المطبق في بنك السلام	185
03	حول معيار ISO المطبق في بنك الخليج	187
04	محاوّر تدريب بنك BNA	193
05	اسئلة المقابلة	194
06	قائمة الاساتذم الاعضاء المحكمين للاستبيان	195
07	مخرجات spss نسخة 27	198

قائمة المختصرات

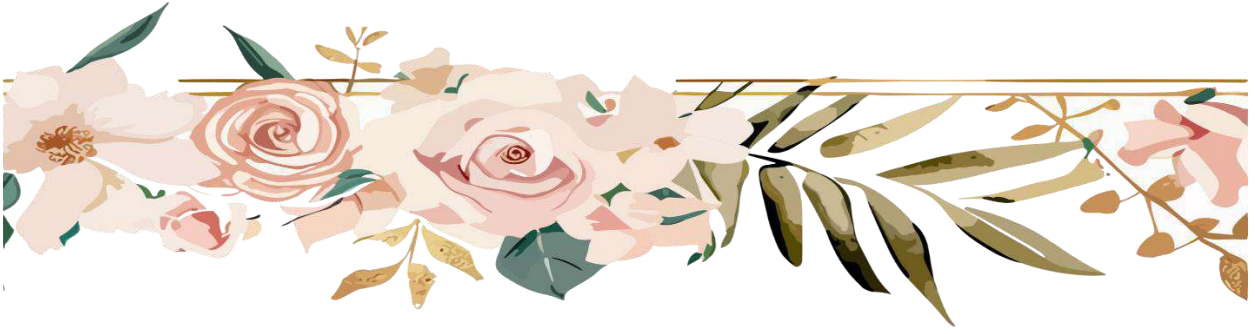
الترجمة	التسمية	الترميز
إدارة استمرارية الأعمال	Business Continuity Management	BCM
نظام إدارة أمن المعلومات	Information Security Management System	ISMS
تحليل أثر الأعمال	Business Impact Analysis	BIA
هدف زمن الاسترجاع	Recovery Time Objective	RTO
هدف نقطة الاستعادة	Recovery Point Objective	RPO
السرية، السلامة، التوافر	Confidentiality, Integrity, Availability	CIA
المنظمة الدولية للتقييس	International Organization for Standardization	ISO
معيار إدارة أمن المعلومات	Information Security Management Standard	ISO 27001
معيار إدارة مخاطر أمن المعلومات	Information Security Risk Management	ISO 27005
إرشادات تحليل أثر الأعمال	Business Impact Analysis Guidelines	ISO 22317
المعهد الوطني للمعايير والتكنولوجيا	National Institute of Standards and Technology	NIST SP 800-34
دليل تخطيط الطوارئ لنظم المعلومات	Contingency Planning Guide for Information Systems	CPGIS
خطة التعافي من الكوارث	Disaster Recovery Plan	DRP
معيار ضوابط أمن المعلومات	Code of Practice for Information Security Controls	ISO 27002
معيار إدارة استمرارية الأعمال	Business Continuity Management Systems	ISO 22301
بنك التنمية المحلية	Banque de Développement Local	BDL
بنك الفلاحة والتنمية الريفية	Banque de l'Agriculture et du Développement Rural	BADR
بنك أفريقيا والخليج	Africa Gulf Bank	AGB
القرض الشعبي الجزائري	Crédit Populaire d'Algérie	CPA

قائمة المختصرات

البنك الخارجي الجزائري	Banque Extérieure d'Algérie	BEA
البنك الوطني الجزائري	Banque Nationale d'Algérie	BNA
بنك الثقة	Trust Bank Algeria	TRUST
نظام المعلومات	Information System	IS
أمن نظام المعلومات	Information System Security	ISS



مقدمة



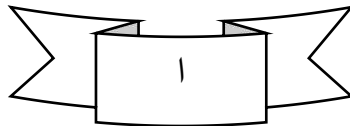
مقدمة

توطئة:

تشهد البنوك في الوقت الراهن تطورات متسارعة بفعل التطور التكنولوجي والتحول الرقمي الذي مسّ مختلف الأنشطة والخدمات المصرفية، حيث أصبحت نظم المعلومات تمثل الركيزة الأساسية في تسيير العمليات البنكية اليومية، لما توفره من تدفق في سرعة معالجة البيانات ودقة وحرص في تنفيذ العمليات وسلاسة في تبادل المعلومات بين مختلف الوكالات والمصالح. إلا أن هذا الاعتماد على التكنولوجيا صاحبه ظهور العديد من المخاطر والتهديدات المعلوماتية، كالهجمات السيبرانية، اختراقات و الأعطال التقنية، وفقدان المعلومات، الأمر الذي جعل أمن نظام المعلومات من بين أهم الأمور التي تسعى البنوك لتحقيقها و تعزيزها من أجل حماية مواردها وضمان استمرارية نشاطها.

وفي ظل البيئة المصرفية الحديثة، لم يعد أمن نظام المعلومات يقتصر فقط على حماية البيانات والأنظمة من التهديدات، بل أصبح عنصراً استراتيجياً يساهم بشكل مباشر في دعم إدارة استمرارية الأعمال، من خلال ضمان استمرارية الخدمات البنكية وتقليل المخاطر والأزمات التي قد تؤثر على السير العادي لنشاط البنكي اليومي. فكلما كانت الأنظمة المعلوماتية أكثر أماناً وفعالية، زادت قدرة البنك على مواجهة المخاطر والحفاظ على استمرارية عمليات وخدمات المقدمة للزبائن.

ومن هذا المنطلق، تناولنا بدراسة العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال داخل البنوك الجزائرية، خاصة في ظل التوسع في استخدام الأنظمة البنكية الرقمية والاعتماد المتزايد على الحلول التكنولوجية الحديثة، الأمر الذي يفرض على البنوك ضرورة تبني إجراءات أمنية فعالة تضمن حماية نظمها المعلوماتية وتدعم قدرتها على الاستمرار في تقديم خدماتها بكفاءة وفعالية.



ب_ طرح الإشكالية:

يُعد موضوع مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال من المواضيع الحديثة التي حظيت باهتمام متزايد في ظل التوسع الكبير في استخدام الأنظمة الرقمية داخل المؤسسات، غير أن الدراسات التي تناولت طبيعة العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال في البيئة الجزائرية لا تزال محدودة وانطلاقاً من أهمية هذا الموضوع نظرياً وتطبيقياً، وسعيًا إلى إبراز الدور الذي يؤديه أمن نظام المعلومات في تعزيز قدرة المؤسسات على مواجهة المخاطر والأزمات وضمان استمرارية أنشطتها، تتمثل إشكالية هذه الدراسة من خلال محاولة تحليل طبيعة العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال، وذلك من خلال تناول الجانب النظري والميداني للإجابة عن السؤال الرئيسي الآتي:

إلى أي مدى يساهم أمن نظام المعلومات في دعم إدارة استمرارية الأعمال بعينة البنوك ولاية ورقلة؟

للإجابة على الإشكالية الرئيسية المتعلقة بمدى مساهمة أمن نظام المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة، تم تقسيمها إلى مجموعة من التساؤلات الفرعية كما يلي:

1. ما مستوى تطبيق أبعاد أمن نظام المعلومات داخل البنوك محل الدراسة؟
2. ما مستوى تطبيق إدارة استمرارية الأعمال داخل البنوك محل الدراسة؟
3. ما العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال داخل البنوك محل الدراسة؟
4. هل يوجد مساهمة ذا دلالة إحصائية عند مستوى دلالة ($\alpha \geq 0.05$) لبعد سرية المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة؟
5. هل يوجد مساهمة ذا دلالة إحصائية عند مستوى دلالة ($\alpha \geq 0.05$) لبعد سلامة المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة؟
6. هل يوجد مساهمة ذا دلالة إحصائية عند مستوى دلالة ($\alpha \geq 0.05$) لبعد توافر المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة؟

مقدمة

7. هل توجد فروق ذات دلالة إحصائية في إجابات أفراد عينة الدراسة حول إدارة استمرارية الأعمال باختلاف (النوع،

الحجم) البنوك؟

8. إلى أي مدى تساهم أبعاد أمن نظام المعلومات مجتمعة في تعزيز فعالية إدارة استمرارية الأعمال داخل البنوك محل

الدراسة؟

ت-الفرضيات:

في ضوء العرض السابق لمشكلة الدراسة المتعلقة بأثر أمن نظام المعلومات على إدارة استمرارية الأعمال داخل البنوك محل

الدراسة، يمكن صياغة الفرضيات التالية بهدف اختبار صحتها:

1. تتمتع البنوك محل الدراسة بمستوى مرتفع من تطبيق إدارة استمرارية الأعمال؛

2. تتمتع البنوك بمستوى مرتفع من أمن نظام المعلومات ;

3. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين أمن نظام المعلومات وإدارة استمرارية

الأعمال داخل البنوك محل الدراسة؛

4. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سرية المعلومات وإدارة استمرارية الأعمال في

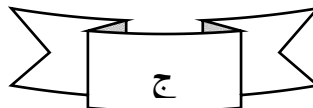
البنوك محل الدراسة؛

5. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سلامة المعلومات وإدارة استمرارية الأعمال

في البنوك محل الدراسة؛

6. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين توافر المعلومات وإدارة استمرارية الأعمال في

البنوك محل الدراسة.



7. لا توجد فروق ذات دلالة إحصائية للإجابات أفراد العينة في الدراسة حول إدارة الاستمرارية الاعمال تعزي متغيرات

التنظيمية لبنوك محل الدراسة

8. توجد علاقة ارتباطية ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين أبعاد أمن نظام المعلومات وإدارة

استمرارية الأعمال داخل البنوك محل الدراسة

ث - أهداف البحث:

أولاً: الأهداف النظرية

- ✓ توضيح المفاهيم الأساسية المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال;
- ✓ إبراز أبعاد أمن نظام المعلومات والمتمثلة في: سرية المعلومات، سلامة المعلومات، وتوافر المعلومات;
- ✓ توضيح أهمية إدارة استمرارية الأعمال ودورها في ضمان استمرارية الأنشطة والخدمات داخل البنوك;
- ✓ إبراز طبيعة العلاقة النظرية بين أمن نظام المعلومات وإدارة استمرارية الأعمال;
- ✓ إثراء الجانب المعرفي والدراسات السابقة المتعلقة بموضوع أمن نظام المعلومات واستمرارية الأعمال في البيئة البنكية.

ثانياً: الأهداف التطبيقية

- ✓ التعرف على مستوى تطبيق أبعاد أمن نظام المعلومات داخل البنوك محل الدراسة;
- ✓ تحديد مستوى تطبيق إدارة استمرارية الأعمال داخل البنوك محل الدراسة;
- ✓ تحليل طبيعة العلاقة الارتباطية بين أبعاد أمن نظام المعلومات وإدارة استمرارية الأعمال داخل البنوك;
- ✓ دراسة أثر كل بُعد من أبعاد أمن نظام المعلومات والمتمثلة في: سرية المعلومات، سلامة المعلومات، وتوافر المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة;
- ✓ التعرف على مدى مساهمة تطبيق معايير وإجراءات أمن المعلومات في تعزيز قدرة البنوك على مواجهة الأزمات وضمان

استمرارية خدماتها;

مقدمة

✓ تقديم مجموعة من النتائج والتوصيات التي يمكن أن تساعد البنوك محل الدراسة على تحسين مستوى أمن نظام المعلومات وتعزيز فعالية إدارة استمرارية الأعمال.

✓ ثالثاً: الأهداف السياقية

✓ ابراز الدور الذي يلعبه أمن نظام المعلومات في دعم استمرارية الأعمال وتقليل المخاطر والاضطرابات داخل البنوك;

✓ تسليط الضوء على واقع تطبيق أمن نظام المعلومات وإدارة استمرارية الأعمال في البيئة البنكية الجزائرية;

✓ المساهمة في توجيه اهتمام البنوك نحو تعزيز الجاهزية الرقمية والأمنية لمواجهة التهديدات والأزمات المختلفة.

ح- أهمية البحث :

تتجلى أهمية هذه الدراسة من خلال عدة جوانب مترابطة، يمكن توضيحها فيما يلي:

1-من الجانب النظري:

تسهم هذه الدراسة في إثراء الأدبيات العلمية المتعلقة بموضوع أمن نظام المعلومات وإدارة استمرارية الأعمال، باعتبارها من المواضيع الحديثة التي أصبحت تحظى باهتمام متزايد في القطاع المصرفي، خاصة في ظل التقدم التكنولوجي المتسارع وكثرت المخاطر السيبرانية. كما تبرز الدراسة أهمية أبعاد أمن نظام المعلومات والمتمثلة في سرية المعلومات، سلامة المعلومات، وتوافر المعلومات، ودورها في دعم استمرارية الأعمال داخل البنوك على مستوى ولاية ورقلة.

2-من الجانب التطبيقي:

توفر هذه الدراسة بيانات ومؤشرات ميدانية حول واقع تطبيق أمن نظام المعلومات داخل البنوك محل الدراسة بولاية ورقلة وبلدية حاسي مسعود، ومدى مساهمته في دعم إدارة استمرارية الأعمال. كما يمكن أن تساعد النتائج المتوصل إليها مسؤولي البنوك وصناع القرار على تعزيز إجراءات الأمن المعلوماتي وتطوير الأنظمة المعلوماتية المعتمدة، بما يساهم في التقليل من المخاطر والتهديدات وضمان استمرارية الخدمات البنكية بكفاءة وفعالية.

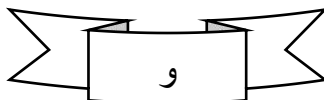
3-من جانب السياق:

تتميز هذه الدراسة بمعالجتها لموضوع مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال ضمن بيئة البنوك ، وبشكل خاص البنوك الناشطة على مستوى ولاية ورقلة وبلدية حاسي مسعود، وهو ما يجعلها تأخذ قيمة تطبيقية وميدانية خاصة. كما تأتي هذه الدراسة في ظل التوجه المتزايد نحو الرقمنة وتبني الأنظمة المعلوماتية الحديثة داخل القطاع المصرفي، الأمر الذي يجعل موضوع الأمن المعلوماتي واستمرارية الأعمال من الأولويات الأساسية لضمان استقرار الخدمات البنكية وتعزيز الثقة في المعاملات المالية.

ج - مبررات اختيار البحث:

- تتمثل دوافع اختيار هذا الموضوع في مجموعة من الاعتبارات العلمية والعملية، من أبرزها:
- انسجام موضوع الدراسة مع طبيعة التخصص، باعتباره من المواضيع الحديثة المرتبطة بمجال إدارة الأعمال ونظم المعلومات;
 - الرغبة في التعمق والبحث في المواضيع الحديثة ذات العلاقة بأمن نظام المعلومات وإدارة استمرارية الأعمال داخل المؤسسات البنكية;
 - قلة الدراسات التي تناولت العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال، على مستوى الجزائر;
 - إبراز أهمية تطبيق أبعاد أمن نظام المعلومات داخل البنوك ودورها في ضمان استمرارية الأنشطة والخدمات البنكية;
 - المساهمة في نشر الوعي بأهمية إدارة استمرارية الأعمال داخل المؤسسات البنكية، خاصة في ظل الأزمات والمخاطر التقنية والتنظيمية;
 - محاولة تقديم إضافة علمية يمكن الاستفادة منها في تطوير السياسات والإجراءات المتعلقة بأمن المعلومات واستمرارية الأعمال داخل البنوك;
 - محاولة تقديم قيمة علمية مضافة تُسهم في دعم وإثراء المكتبة الجامعية بمرجع أكاديمي متخصص، بما يفتح المجال أمام الباحثين للاستفادة من نتائجه في الدراسات المستقبلية

خ - حدود البحث:



مقدمة

حدود البشرية: تمثلت الحدود البشرية للدراسة في مسؤولي أمن نظام المعلومات داخل البنوك محل الدراسة، باعتبارهم الفئة الأكثر ارتباطاً بموضوع الدراسة، حيث تم استهداف مسؤول واحد عن أمن نظام المعلومات في كل بنك، ليبلغ عدد أفراد العينة 10 أفراد يمثلون مختلف البنوك محل الدراسة.

حدود الزمانية: أُنجزت الدراسة خلال الموسم الجامعي 2026/2025، أما الدراسة الميدانية فقد تمت خلال الفترة الممتدة بين شهري مارس وأفريل 2026

حدود المكانية: تمت هذه الدراسة في مجموعة من البنوك الناشطة بولاية ورقلة، بما في ذلك البنوك المتواجدة ببلدية حاسي مسعود، والتي تمثلت في كل من: بنك التنمية المحلية BDL، بنك الفلاحة والتنمية الريفية BADR، بنك السلام، بنك أفريقيا والخليج AGB، بنك القرض الشعبي الجزائري CPA، بنك الثقة TRUST، بنك البركة، البنك الخارجي الجزائري BEA، البنك الوطني الجزائري BNA، وسوسيتيه جنرال الجزائر.

حدود الموضوعية: تم التركيز في هذه الدراسة على أمن نظام المعلومات كمتغير مستقل، من خلال الأبعاد التالية: سرية المعلومات، سلامة المعلومات، وتوافر المعلومات، أما المتغير التابع فتمثل في إدارة استمرارية الأعمال داخل البنوك محل الدراسة

د - منهج البحث والأدوات المستخدمة:

بناءً على طبيعة الدراسة والأهداف المحددة لها، تم اعتماد المنهج الوصفي التحليلي في الجانب النظري، حيث تم التركيز على تعريف المفاهيم والمصطلحات المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال، مع توضيح مختلف الجوانب النظرية المرتبطة بهما. أما في الجانب التطبيقي، فقد تم الاعتماد على الدراسة الميدانية من خلال استخدام مجموعة من أدوات جمع البيانات المتمثلة في الملاحظة، الوثائق الرسمية، المقابلة الشخصية، والاستبيان، وذلك بهدف جمع بيانات دقيقة تساعد على تحليل واقع أمن نظام المعلومات ودوره في دعم إدارة استمرارية الأعمال داخل البنوك محل الدراسة.

وقد اعتمد الاستبيان كأداة رئيسية لجمع البيانات الكمية المتعلقة بمتغيرات الدراسة، في حين استُخدمت المقابلة الشخصية والملاحظة كأدوات مساندة لتفسير النتائج وتعزيز مصداقيتها. أما فيما يخص معالجة البيانات وتحليلها، فقد تم الاعتماد على

مقدمة

البرنامج الإحصائي IBM SPSS Statistiques الإصدار 27، وذلك لدراسة المؤشرات الإحصائية وتحليل العلاقات بين متغيرات الدراسة بما يسمح بفهم مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال داخل البنوك محل الدراسة

ذ - مرجعية البحث:

اعتمدنا من أجل جمع المعلومات المتعلقة بموضوع الدراسة على مجموعة من المراجع باللغة العربية والأجنبية، وذلك بهدف الإحاطة بمختلف الجوانب النظرية المرتبطة بأمن نظام المعلومات وإدارة استمرارية الأعمال. وقد ساهمت هذه المراجع في بناء الإطار النظري للدراسة وتدعيم الجانب التطبيقي، وتمثلت هذه المراجع في: الكتب، المذكرات الجامعية (الماستر)، المقالات العلمية المحكمة، إضافة إلى الدراسات والأبحاث المنشورة ذات الصلة بموضوع الدراسة.

ر - صعوبات البحث:

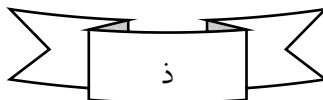
لا يخلو أي بحث علمي من مجموعة من الصعوبات والعراقيل التي قد تواجهنا أثناء إنجاز الدراسة، وقد تمثلت أهم الصعوبات التي واجهتنا فيما يلي:

- صعوبة الحصول على دراسات سابقة حديثة تجمع بين متغيري أمن نظام المعلومات وإدارة استمرارية الأعمال؛
- صعوبة تحديد أبعاد المتغيرات بشكل دقيق بما يتناسب مع طبيعة الدراسة؛
- انعدام المراجع المتخصصة المتوفرة في مكتبة الجامعة؛
- صعوبة الوصول إلى بعض المعلومات المتعلقة بأنظمة أمن المعلومات داخل البنوك، نظراً لطبيعة السرية التي يتميز بها القطاع المصرفي وتكتم على بعض المعلومات من مسؤولي بنوك؛
- ضيق الوقت وصعوبة التنسيق مع بعض أفراد عينة الدراسة بسبب طبيعة العمل داخل البنوك.

ز - هيكل البحث:

لمعالجة إشكالية الدراسة وتحقيق أهدافها، وفي ضوء المنهجية المعتمدة، تم تقسيم البحث إلى فصلين، أحدهما نظري والآخر

تطبيقي.



مقدمة

حيث حُصص الفصل الأول للإطار النظري للدراسة، واشتمل على مبحثين، تناول المبحث الأول الأدبيات النظرية المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال، بهدف توضيح المفاهيم الأساسية وأبعاد متغيرات الدراسة، بينما تضمن المبحث الثاني عرض وتحليل الدراسات السابقة ذات الصلة بموضوع الدراسة، والتي شكلت مرجعية علمية أساسية ساهمت في تدعيم الجانب النظري للدراسة الحالية.

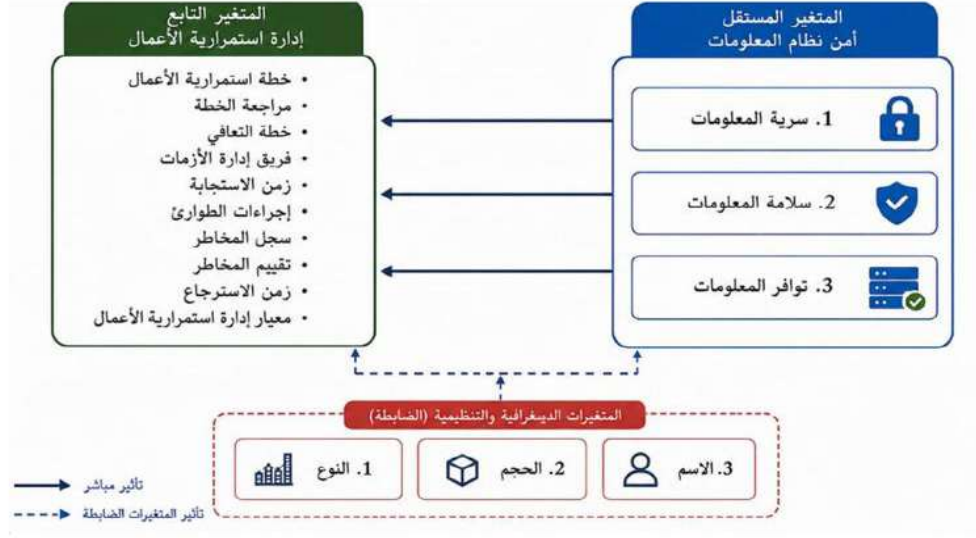
أما الفصل الثاني، فقد حُصص للدراسة الميدانية، حيث تناول المبحث الأول الطريقة والإجراءات المعتمدة في جمع البيانات وتحليلها، في حين حُصص المبحث الثاني لعرض نتائج الدراسة الميدانية وتحليلها ومناقشتها في ضوء الإطار النظري والدراسات السابقة.

س- نموذج الدراسة:

استناداً إلى الأدبيات النظرية المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال، وبناءً على الدراسات السابقة التي تناولت هذا الموضوع، تم اعتماد أمن نظام المعلومات كمتغير مستقل بأبعاده المتمثلة في: سرية المعلومات، سلامة المعلومات، وتوافر المعلومات، في حين تم اعتماد إدارة استمرارية الأعمال كمتغير تابع وبناءً على ذلك، تم تطوير نموذج الدراسة بهدف تحليل طبيعة العلاقة بين أبعاد أمن نظام المعلومات وإدارة استمرارية الأعمال داخل البنوك محل الدراسة، وذلك من خلال اختبار مساهمة كل بعد من أبعاد أمن المعلومات على قدرة البنوك في دعم استمرارية الأعمال وتقليل المخاطر وضمان استمرارية تقديم الخدمات البنكية حيث سيكون هذا الشكل وفق النموذج الموالي:



الشكل 01: يوضح نموذج الدراسة



المصدر: من تصور الطالبين بالاعتماد على الدراسات السابقة

ش -تحديد المفاهيم الإجرائية:

أمن نظام المعلومات: يقصد بأمن نظام المعلومات مجموعة الإجراءات والتدابير التقنية والتنظيمية التي تهدف إلى حماية المعلومات والأنظمة من التهديدات والمخاطر، وضمان سرية المعلومات وسلامتها وتوافرها داخل المؤسسة البنكية.

إدارة استمرارية الأعمال: يقصد بإدارة استمرارية الأعمال قدرة المؤسسة على ضمان استمرارية أنشطتها وخدماتها الأساسية أثناء الأزمات والطوارئ من خلال التخطيط المسبق واتخاذ الإجراءات اللازمة للتقليل من آثار المخاطر والتعافي منها.



الفصل الاول: الادبيات النظرية لأمن نظام المعلومات
وإدارة استمرارية الاعمال



الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

تمهيد:

في ظل التحول الرقمي واعتماد المؤسسات المتزايد على نظم المعلومات في تسيير مختلف أنشطتها، أصبح أمن نظم المعلومات ضرورة حتمية وليس مجرد جانب تقني. فالمعلومات أصبحت أحد النقاط الحساسة التي تمس المؤسسة، وأي تهديد يمس سريتها أو سلامتها أو توفرها قد يؤدي إلى تعطل العمليات وخسائر مادية ومعنوية جسيمة. ومن هنا، يبرز دور أمن نظم المعلومات كآلية أساسية لحماية المؤسسة من مختلف المخاطر والتهديدات الداخلية والخارجية، من خلال وضع سياسات وإجراءات وتقنيات تضمن حماية الأصول المعلوماتية وضمان استمرارية تدفق المعلومات دون انقطاع. كما يساهم أمن نظم المعلومات بشكل مباشر في دعم إدارة استمرارية الأعمال، إذ يساعد على تقليل آثار الأزمات، وضمان استرجاع الأنظمة، والحفاظ على قدرة المؤسسة على مواصلة نشاطها في مختلف الأزمات والظروف الطارئة.

ومن خلال هذا الفصل سيتم معالجة ثلاث مباحث مقسمة على النحو الآتي:

المبحث الاول: ماهية أمن نظام المعلومات .

المبحث الثاني: ماهية ادارة استمرارية الاعمال .

المبحث الثالث: الدراسات السابقة المتعلقة بأمن نظام المعلومات وإدارة استمرارية الاعمال .

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية

المبحث الاول: ماهية أمن نظام المعلومات

يُعدّ أمن نظم المعلومات عنصراً حيويًا تركز عليه المؤسسات في حماية أصولها المعلوماتية من شتى التهديدات والمخاطر، مع ضمان السرية والسلامة والتوافر. ومن خلال تبني مجموعة متكاملة من السياسات والإجراءات الفعالة، تتمكن المؤسسة من تعزيز مستوى حماية نظمها المعلوماتية، بما يدعم استمرارية أعمالها ويحدّ من تداعيات المخاطر والأزمات.

المطلب الاول مفهوم امن نظام المعلومات

يمثّل أمن نظم المعلومات محورًا أساسيًا في حماية المؤسسة وضمان استقرار نشاطها، لما له من دور في الحدّ من المخاطر التي قد تهدّد أصولها المعلوماتية. ويهدف هذا المطلب إلى تسليط الضوء على الإطار العام لمفهوم أمن نظم المعلومات، وأهدافه، وأهميته بالنسبة للمؤسسة.

أولاً: مفهوم أمن نظام المعلومات

تباينت وتعددت التعاريف التي قدمها المفكرون والباحثون حول هذا المفهوم، بحيث وقع اختيارنا على التعاريف التالية:

➤ يعرف "الأمن" يشير إلى السياسات والإجراءات، والتدابير التقنية المستخدمة لمنع الوصول الغير المصرح به، التغيير

والسرقة، أو الأضرار المادية لنظم المعلومات¹

➤ كما يعرف على أنه:

"مجموعة السياسات والإجراءات الإدارية والتقنية التي تهدف إلى حماية الموارد المعلوماتية من الوصول غير المصرح به أو التلاعب أو

التخريب".²

¹ نبان طيب إبراهيم، أهمية امن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة ، مجلة التنمية والاقتصاد التطبيقي، العدد3، مارس 2018، ص36

² قدور مقراني، تقييم مدى مساهمة امن نظم المعلومات الالكترونية في الحد من مخاطر نظم المعلومات : دراسة حالة مؤسسة الاتصالات الجزائرية، مذكرة نيل شهادة الماستر كلية علوم الاقتصادية والتجارية وعلوم التسيير جامعة قاصدي مرباح ورقلة 2016، ص 25

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

➤ عرفه المكتب الوطني الاسترالي للتدقيق Australian National Audit Office " بحماية أنظمة المعلومات بما

تشمله البنى التحتية التي تسهل استخداماتها كالتقنيات والعمليات والخدمات والمعلومات " ¹.

➤ كما يعرف أمن نظام المعلومات بأنه عبارة عن تلك " العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف

حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغض تحقيق سلامتها وتوافرها وسريتها وفق

الصلاحيات والترتيبات المتعارف عليها ²

من خلال ما تم التطرق اليه من مجمل التعاريف السابقة فيما يخص مصطلح امن نظام المعلومات يتضح لنا انه عبارة عن إطار تنظيمي وإداري وتقني تسعى المؤسسة من خلاله الى حماية بياناتها وانظمتها من شتى المخاطر من اجل ضمان الاستخدام السليم للمعلومات بهدف استمرارية النشاط

يمثل أمن نظام المعلومات أحد الركائز الأساسية في حماية الموارد الرقمية للمؤسسة وتعزيز استقرارها التنظيمي. ويمكن إبراز

أهميته من خلال النقاط التالية:

- حماية المعلومات المتعلقة بالمنتجات والعملاء والمعاملات الإلكترونية من السرقة أو التلاعب أو الإلتفاف;³
- يعتبر امن نظم المعلومات من الدعائم الضرورية لحماية المؤسسة من الاضرار الناجمة عن الهجمات التي تتعرض لها نظم المعلومات;⁴
- يساهم في تحسين أداء الأجهزة والبرامج من خلال اعتماد إجراءات وقائية فعالة مثل: الجدران النارية والتشفير;

¹ أيمن محمد فارس الدنف, واقع إدارة امن نظم المعلومات في الكليات التقنية في غزة, مذكرة نيل شهادة الماجستير كلية التجارة جامعة الإسلامية غزة 2013 ص44

² دليلة العوي, محاضرات أنظمة المعلوماتية, كلية الاعلام والاتصال جامعة الجزائر 3 إبراهيم سلطان شسبوط, 2020/ 2021, ص48

³ بن طيب إبراهيم مرجع سبق ذكره ص 34

⁴ نبيل حليمي رشيد حفصي أهمية الامن المعلوماتي بالمؤسسة الاقتصادية دراسة حالة مديرية توزيع الكهرباء والغاز بوقرلة, مجلة الجزائرية للدراسات الاقتصادية والإدارية المجلد

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

- ضمان سرية المعلومات ومنع الوصول غير المصرح به إليها¹;
- الحفاظ على سلامة البيانات ومنع تعديلها أو حذفها بطرق غير قانونية;
- ضمان توافر المعلومات واستمرارية الوصول إليها عند الحاجة دون انقطاع;
- تقليل مخاطر توقف نظم المعلومات والأنظمة التشغيلية داخل المؤسسة;
- حماية المؤسسة من الأخطاء البشرية والكوارث الطبيعية وجرائم الحاسوب;
- دعم استمرارية الأعمال وضمان عدم تعطل العمليات خاصة عبر الإنترنت. ;
- تعزيز الامتثال للقوانين والتشريعات المتعلقة بأمن المعلومات والخصوصية .

يتضح من أهمية امن نظام المعلومات اننا أحد لمركزات التي تعتمد عليها المؤسسات في حماية مواردها الرقمية وضمان استمرارية نشاطها. فأمن نظام المعلومات لا يقتصر فقط على حماية البيانات من السرقة أو التلاعب، بل يعتمد ليشمل تعزيز كفاءة الأنظمة من خلال الاعتماد على آليات وقائية فعالة، وضمان سرية وسلامة وتوافر المعلومات في مختلف الظروف. كما يساهم في الحد من المخاطر التشغيلية الناتجة عن الهجمات الإلكترونية أو الأخطاء البشرية، ويدعم استمرارية الأعمال خاصة في البيئات الرقمية، إضافة إلى دوره في تحقيق الامتثال للتشريعات والقوانين ذات الصلة، مما يعزز من موثوقية المؤسسة ويقوي مكانتها التنظيمي

الا ان هناك بعض المصطلحات التي يجب التمييز بينهم والتي لها علاقة كبيرة بأمن نظام المعلومات وفي نفس الوقت تفترق

عليها وهي:

الامن السيبراني ونظام المعلومات

فيما يلي سنتطرق الى العلاقة بينهم وبعض الفروقات:

1. الامن السيبراني :

¹ بن طيب إبراهيم مرجع سبق ذكره ص 37 - 43

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

يُعرّف الأمن السيبراني بأنه مجموعة من التقنيات والإجراءات والسياسات التنظيمية التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات والبرامج والبيانات من الهجمات الإلكترونية ومحاولات الوصول غير المصرح به، بما يضمن تقليل المخاطر السيبرانية وحماية الأصول الرقمية للأفراد والمؤسسات والدول، كما يهدف إلى تعزيز سرية المعلومات وسلامتها وتوافرها، إضافة إلى ضمان استمرارية الخدمات واسترجاع البيانات عند الحاجة، خاصة في ظل تزايد التهديدات السيبرانية وتنوع أشكالها مثل البرمجيات الخبيثة والهجمات الإلكترونية والتصيد الاحتيالي. ويُعد الأمن السيبراني عنصراً أساسياً في حماية الفضاء السيبراني، حيث يشمل عدة مجالات مثل أمن الشبكات وأمن التطبيقات والأمن السحابي، كما يعتمد على مبدأ المثلث الأمني (السرية، السلامة، التوافر) كركيزة أساسية لضمان فعاليته في حماية المعلومات وتقليل الخسائر الناتجة عن الهجمات الرقمية¹.

2. نظام المعلومات:

يُعرّف نظام المعلومات بأنه منظومة متكاملة تضم مجموعة من العناصر المترابطة مثل الأفراد، والبيانات، والبرمجيات، والأجهزة، والإجراءات، تعمل جميعها على جمع البيانات ومعالجتها وتحويلها إلى معلومات ذات قيمة. وتهدف هذه المنظومة إلى دعم عملية اتخاذ القرار داخل المؤسسة من خلال توفير معلومات دقيقة وموثوقة وفي الوقت المناسب. كما يساهم نظام المعلومات في تنظيم وتسهيل تدفق المعلومات بين مختلف المستويات الإدارية داخل المؤسسة، مما يساعد على تحسين الأداء وزيادة كفاءة العمل وتقليل الأخطاء. ويعتمد هذا النظام على التقنيات الحديثة لتخزين البيانات ومعالجتها واسترجاعها بسرعة وفعالية².

وفي الجدول التالي سنتطرق الى الفرق بين هذه المصطلحات والعلاقة التي تربطهم:

¹ الدام محمد، الامن السيبراني، مذكرة ماستر لنيل شهادة الماستر في الحقوق تخصص جريمة وامن، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، ص 8-6

² عبد الحكيم بن بختي، دور نظم المعلومات في تحسين الأداء الوظيفي للإدارة الجزائرية، الحديقة مجلة العلوم الانسان والمجتمع المجلد 13 العدد 03 السنة 2024 ص 603-602

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

الجدول 01-01 : أوجه الاختلاف والعلاقة بين امن نظام المعلومات ونظام المعلومات والامن السيبراني

البيانات المصطلحات	امن نظام المعلومات	نظام المعلومات	الامن السيبراني
الهدف	ضمان سرية وسلامة وتوافر المعلومات داخل النظام	دعم اتخاذ القرار وتحسين أداء المؤسسة	حماية البيئة الرقمية بالكامل من الهجمات السيبرانية وضمان الأمن الرقمي
النطاق	داخلي مرتبط بنظام المعلومات داخل المؤسسة	داخلي داخل المؤسسة جانب إداري وتقني	(مؤسسات، أفراد، دول، شبكات عالمية)
التركيز	حماية المعلومات النظام المؤسسة من الاختراق أو التلف أو التعديل	جمع البيانات ومعالجتها وتبادل المعلومات	مواجهة التهديدات والهجمات الإلكترونية على نطاق واسع
الأدوات	تشفير، جدران نارية، صلاحيات وصول، نسخ احتياطي كلمة السر	قواعد بيانات، برمجيات، شبكات، أجهزة	أنظمة دفاع متقدمة، تحليل تهديدات، ذكاء اصطناعي، استجابة للحوادث
العلاقة بينهم	تعتبر جزء من نظام المعلومات يهتم بالحماية	يمثل البنية تجمع فيها المعلومات	إطار شامل يضم حماية نظم المعلومات وأمنها

المصدر: من اعداد الطالبتين بناء على المراجع المدروسة

من خلال ال مقارنة بين هذه المصطلحات نرى ان هناك علاقة تكاملية بين نظم المعلومات وأمن نظم المعلومات والأمن السيبراني أي لا يمكن تجزئتهم عن بعض، بحيث يمثل نظام المعلومات البيئة التي تجمع و تُعالج فيها البيانات وتُستخدم لدعم اتخاذ القرار، بينما يهتم أمن نظم المعلومات بحماية هذه البيانات داخل المؤسسة من المخاطر والتهديدات . أما الأمن السيبراني فهو أكثر شمولية في حماية الأنظمة والشبكات والبيانات على مستوى أكثر اتساع من المؤسسة. وبالتالي، يختلف كل مفهوم من حيث النطاق، لكنها جميعاً تهدف إلى حماية المعلومات وضمان استخدامها بشكل آمن وفعال.

ثانياً: اهداف امن نظام المعلومات

يهدف نظام أمن المعلومات إلى تحقيق مجموعة من الأهداف التي تساهم في حماية البيانات وضمان سلامة الأنظمة واستمرارية عملها داخل المؤسسات وتمثلت كالتالي:

1) تقليل مخاطر توقف الأنظمة والمؤسسات حيث يهدف أمن المعلومات إلى الحد من الأعطال والمشكلات التي قد تؤدي إلى توقف عمل الأنظمة أو تعطل نشاط المؤسسات الاقتصادية;¹

2) يهدف أمن نظم المعلومات إلى حماية المعلومات وضمان استخدامها بشكل آمن وفعال، وذلك من خلال تحقيق مبادئ الثلاث الأعمى (CIA) ، والمتمثلة في السرية (Confidentiality) لحماية خصوصية البيانات، والتكاملية (Integrity) لضمان سلامتها ودقتها، والتوافر (Availability) لضمان إتاحتها عند الحاجة للمستخدمين

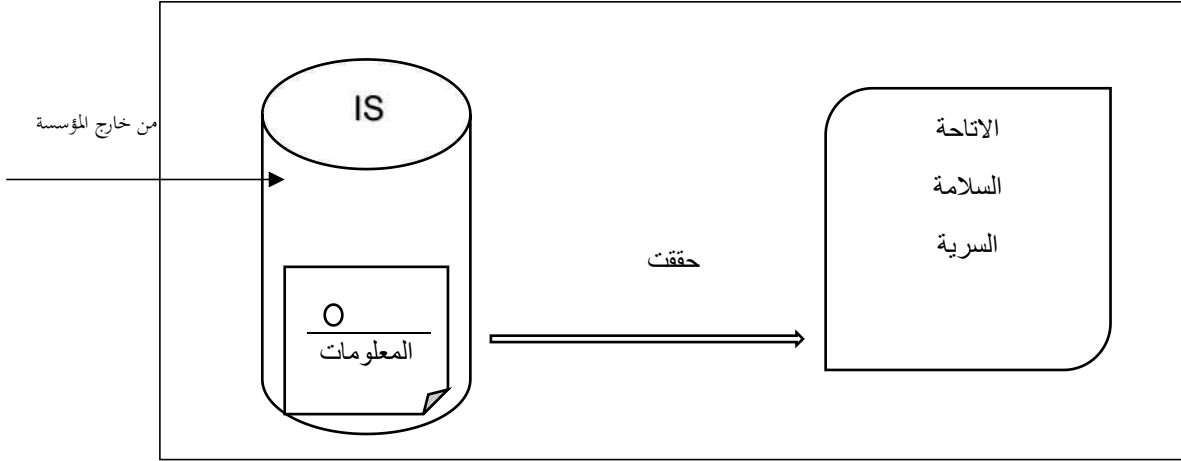
المصرح لهم;²

¹ بن طيب إبراهيم مرجع سبق ذكره ص 36

² ابن محمد فارس الدنف مرجع سبق ذكره ص 45- 46

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

الشكل 01-01 : يوضح اهداف تحقيق امن المعلومات



المصدر: ايمن محمد فارس الدنف، واقع إدارة امن المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها ص 60

(3) ضمان أمن عمليات الإرسال وحماية المعلومات أثناء نقلها عبر الشبكات المختلفة، بحيث تصل إلى الجهة المقصودة

دون اعتراض أو تغيير.¹

ثالثاً: مكونات أمن نظام المعلومات

يُعتبر أمن نظام المعلومات من الركائز الأساسية لضمان حماية الأصول المعلوماتية داخل المؤسسات، حيث يقوم على مجموعة

من المكونات الجوهرية التي تحدد مستوى حماية البيانات وقدرتها على مواجهة التهديدات المختلفة حيث تناولنا هذه المكونات

بشكل التالي:²

(1) السرية (Confidentiality)

¹ بن طيب مرجع سبق ذكره ص 37

² National Institute of Standards and Technology (NIST). An Introduction to Information Security (SP 800-12 Rev.1), 2017, pp. 1–8.

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

تشير السرية إلى حماية المعلومات من الوصول أو الكشف غير المصرح به، بحيث يتم ضمان أن البيانات لا تكون متاحة إلا للأشخاص أو الكيانات التي تمتلك صلاحيات رسمية للوصول إليها. وتعد هذه الخاصية ضرورية للحفاظ على خصوصية المعلومات، خاصة في البيئات التي تحتوي على بيانات حساسة، حيث إن أي خرق لها قد يؤدي إلى أضرار كبيرة على المستوى الفردي أو المؤسسي¹

(2) السلامة (Integrity)

تعني السلامة الحفاظ على دقة البيانات واكتمالها، ومنع أي تعديل غير مصرح به عليها، سواء كان هذا التعديل متعمداً أو ناتجاً عن أخطاء تقنية أو بشرية. وتكمن أهمية هذه الخاصية في ضمان موثوقية المعلومات، حيث إن اتخاذ القرارات يعتمد بشكل كبير على صحة البيانات وسلامتها

(3) التوافر (Availability)

يقصد بالتوافر ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة من قبل المستخدمين المصرح لهم، دون انقطاع أو تعطيل. وتعتبر هذه الخاصية أساسية لضمان استمرارية الأنشطة والخدمات داخل المؤسسة، خاصة في الأنظمة التي تعتمد على التشغيل المستمر

(4) عدم الإنكار (Non-repudiation)

يشير مبدأ عدم الإنكار إلى ضمان عدم قدرة أي طرف مشارك في عملية داخل نظام المعلومات على إنكار قيامه بها لاحقاً، سواء كانت إرسال بيانات أو تنفيذ معاملة أو الوصول إلى مورد معين. ويُعد هذا المبدأ جزءاً من آليات حماية الثقة في الأنظمة المعلوماتية، حيث يعتمد على وسائل التحقق والتوثيق التي تسمح بإثبات حدوث العمليات وربطها بمصدرها.

¹ An Introduction to Information Security (SP 800-12 .National Institute of Standards and Technology (NIST) Rev.1), 2017, pp. 1–8

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

وقد أشار دليل NIST إلى أهمية آليات التحقق والتوثيق داخل أنظمة الأمن المعلوماتي باعتبارها جزءاً من بناء الثقة وضمان إمكانية تتبع العمليات داخل النظام، وهو ما يدعم مبدأ عدم الإنكار ضمناً من خلال آليات التحقق من الهوية والسجلات الأمنية¹

من خلال تطرقنا لمكونات أمن نظام المعلومات، يتضح أنها لا تقتصر فقط على أبعاد تقنية منفصلة، بل تشكل منظومة متكاملة تؤسس لحماية فعالة وشاملة. فالتركيز على السرية والسلامة والتوافر يعكس ما يُعرف بالمثلث الأساسي للأمن المعلوماتي، والذي يمثل حجر الأساس في بناء أي نظام آمن، حيث إن اختلال أحد هذه العناصر يؤدي مباشرة إلى إضعاف باقي المنظومة. كما أن إبراز مبدأ عدم الإنكار يضيف بعداً متقدماً يعزز الثقة في التعاملات الإلكترونية، خاصة من خلال ربط العمليات بمصادرها وإمكانية تتبعها، وهو ما يدعم مصداقية النظام ويحد من الالتزامات المرتبطة بالمعاملات الرقمية.

المطلب الثاني : استراتيجيات أمن نظام المعلومات والمتطلبات الأساسية لضمانه

أولاً: متطلبات امن نظم المعلومات

تقتضي حماية نظم المعلومات داخل المؤسسة توافر مجموعة من المتطلبات الأساسية التي تشكل إطاراً تنظيمياً وتقنياً يهدف إلى ضمان سلامة المعلومات واستمرارية عمل النظام بكفاءة وفعالية. ويمكن عرض هذه المتطلبات فيما يلي:²

✓ ضرورة إعداد سياسة عامة لأمن نظم المعلومات، تتماشى مع طبيعة نشاط المؤسسة وخصوصية تطبيقاتها، وتحدد

الأهداف والضوابط والإجراءات المنظمة لحماية المعلومات؛

✓ التزام الإدارة العليا بتبني ودعم برامج أمن نظم المعلومات، من خلال توفير الموارد اللازمة والإشراف على تنفيذ السياسات

المعتمدة؛

¹ An Introduction to Information Security (SP 800-12 .National Institute of Standards and Technology (NIST) Rev.1), 2017, pp. 1-8

² الطاهر بن عمارة، تقييم مدى مساهمة نظام الامن الالكتروني في الحد من مخاطر نظم المعلومات: دراسة مقارنة لعينة المؤسسات، مذكورة نيل شهادة الماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح، ورقة 2016 / 2017 ص11

الفصل الاول: الادبيات النظرية لأمن نظم المعلومات وإدارة استمرارية الأعمال

- ✓ تحديد مسؤوليات واضحة تتعلق بأمن نظم المعلومات، من خلال تعيين أشخاص أو جهات مختصة تتولى الإشراف والمتابعة والتنسيق في هذا المجال؛¹
- ✓ وضع ضوابط وإجراءات فنية لحماية أنظمة التشغيل والتطبيقات المختلفة، بما يحد من المخاطر المرتبطة بالتشغيل والمعالجة؛
- ✓ اعتماد آليات للرقابة والمراقبة المستمرة على نظم المعلومات والشبكات الحاسوبية، للكشف المبكر عن أي اختراقات أو تهديدات محتملة؛
- ✓ ضمان وجود نظام فعال للنسخ الاحتياطي، بما يسمح باسترجاع البيانات بصورة آمنة وسريعة عند حدوث أعطال أو فقدان للمعلومات؛
- ✓ تأمين المعلومات في مختلف مراحل التعامل معها، سواء أثناء الحفظ أو المعالجة أو النقل عبر الوسائط والشبكات؛
- ✓ العمل على ضمان استمرارية تشغيل نظم المعلومات وجهازيتها، خاصة في حالات الطوارئ والأزمات، من خلال إعداد خطط مناسبة لمواجهة المخاطر المحتملة.

ومن خلال ما تنطرقنا إليه من متطلبات أمن نظم المعلومات، فيظهر بوضوح أن نجاح أي نظام أمني لا يعتمد فقط على الحلول التقنية، بل يركز أساساً على الدعم التنظيمي والإداري، خاصة من خلال التزام الإدارة العليا ووضع سياسات واضحة تحدد الأدوار والمسؤوليات. كما أن الاهتمام بالرقابة المستمرة والنسخ الاحتياطي يعكس أهمية الاستباقية في مواجهة المخاطر بدل الاكتفاء برد الفعل، إضافة إلى أن ضمان استمرارية الأنظمة في حالات الطوارئ يبرز البعد الاستراتيجي للأمن المعلوماتي باعتباره عنصراً داعماً لاستمرارية الأعمال

¹ الطاهر بن عمار، مرجع سبق ذكره ص11

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

ثانيا: استراتيجية امن نظام المعلومات

تعتمد استراتيجية أمن نظم المعلومات على مجموعة من الإجراءات والتدابير التي تهدف إلى حماية المعلومات والأنظمة داخل المؤسسة. ويمكن توضيح أهم هذه الإجراءات فيما يلي:¹

1. تقييم أمن المعلومات:

يقصد به تحليل مستوى الحماية المتوفر لعناصر النظام المعلوماتي، والتأكد من مدى كفاية الإجراءات الأمنية المطبقة، بهدف تحديد نقاط الضعف والعمل على معالجتها.

2. تحديد عناصر النظام المعلوماتي:

يتم في هذه المرحلة التعرف على مكونات النظام مثل الأجهزة، والبرمجيات، وقواعد البيانات، والشبكات، وذلك لمعرفة الأجزاء التي تحتاج إلى حماية أكبر داخل المؤسسة.

3. تصنيف المعلومات حسب أهميتها:

تُصنّف المعلومات إلى فئات مختلفة مثل المعلومات السرية أو العادية، ويهدف هذا التصنيف إلى تنظيم طرق حفظها وتحديد مستوى الحماية المناسب لكل نوع منها.

4. تقييم المخاطر المحتملة:

تتضمن هذه الخطوة تحديد التهديدات التي قد تواجه النظام المعلوماتي، سواء كانت داخلية أو خارجية، وتحليل احتمال حدوثها وتأثيرها على المؤسسة.

5. وضع سياسة أمن المعلومات:

تعمل المؤسسة على إعداد سياسة واضحة لحماية المعلومات، تتضمن مجموعة من القواعد والإجراءات التي تنظم استخدام النظام المعلوماتي وتضمن الحفاظ على سرية البيانات وسلامتها واستمرارية توفرها.

¹ حمودي كاهنة, نظام امن المعلومات في الجزائر دراسة حالة بلدية سوق الاثنين ولاية تيزي وزو ,مذكرة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية, جامعة مولود

معمرى, كلية الحقوق والعلوم السياسية, سنة , 2016 ص 35

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

من خلال استراتيجية أمن نظام المعلومات التي تطرقنا اليها يتبين أنها تقوم على منهجية متكاملة تبدأ ب تقييم الوضع الأمني وتحديد مكونات النظام، وهو ما يسمح بفهم دقيق لنقاط القوة والضعف. وهو ما يساهم في توجيه الموارد بشكل عقلائي وفعال. وتُعد سياسة أمن المعلومات في هذا السياق الإطار المرجعي الذي يضمن توحيد الجهود وتنظيم الممارسات داخل المؤسسة، مما يعزز من فعالية الإجراءات الأمنية ويضمن استمراريته على مدى الطويل

ثالثاً: معايير امن نظام المعلومات

توجد العديد من المعايير والإطارات المستخدمة في إدارة وأمن المعلومات، كل منها يقدم نهجاً مختلفاً لتقييم المخاطر وضمان حماية الأصول المعلوماتية. في هذا القسم، سنستعرض مجموعة مختارة من هذه المعايير، (معيار COBIT، معيار NIST، معيار OCTAVE، معيار ISO 27001) حيث اعتمدنا على تقديم شرح موجز للمعايير الثلاثة الأولى، ثم التركيز بشكل مفصل على المعيار ISO 27001 الأكثر شيوعاً واعتماداً في المؤسسات. ثم نتعرف على أهم الفروقات بين هذه المعايير

• ISO/IEC 27002

هو معيار يقدم مجموعة من الإرشادات وأفضل الممارسات في أمن المعلومات، يهدف إلى مساعدة المؤسسات على اختيار وتطبيق ضوابط أمنية مناسبة بشكل مرن وفقاً للمخاطر، بما يغطي مختلف مجالات الأمن مثل التحكم في الوصول واستمرارية الأعمال وإدارة الأصول.¹

¹ Book, IT Governance and Information Security, Yassine Maleh et al., CRC Press, 2021, pp. 256–257

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

• SO/IEC 27005

هو معيار يوفّر إطاراً منهجياً لإدارة مخاطر أمن المعلومات، من خلال تحديدها وتقييمها ومعالجتها لدعم نظام إدارة أمن المعلومات، مما يساعد المؤسسات على حماية أصولها واتخاذ قرارات أمنية مبنية على تحليل المخاطر.¹

اما بالنسبة لمعيار ISO 27001 الذي اعتبر كأكثر المعايير شيوعاً واستعمالاً على مستوى المؤسسات والذي قمنا بالتطرق اليه بالشكل التالي:²

• مفهوم معيار ISO/IEC 27001:

يُعتبر ISO/IEC 27001 إطاراً دولياً لإدارة أمن المعلومات داخل المؤسسات، يهدف إلى حماية الأصول المعلوماتية عبر اعتماد منهجية قائمة على تحليل المخاطر وتطبيق ضوابط أمنية مناسبة، مع ضمان سرية المعلومات وسلامتها وتوافرها وفق الاحتياجات التشغيلية والاستراتيجية.

خصائصه الأساسية:

✓ نظام إدارة أمن المعلومات (ISMS):

إنشاء نظام متكامل يدمج السياسات والإجراءات ضمن إطار تنظيمي واضح.

✓ منهجية إدارة المخاطر:

تحديد التهديدات، تقييم تأثيرها، واختيار الضوابط الملائمة، مما يجعله قابلاً للتكيف مع مختلف المؤسسات.

✓ دورة التحسين المستمر (PDCA):

التخطيط (Plan)، التنفيذ (Do)، التحقق (Check)، التحسين (Act) لضمان تطوير النظام الأمني باستمرار.

¹ موقع الكتروني : [ISO/IEC 27005:2022 - Guidance on managing information security risks](https://www.iso.org/standard/72431.html) شوهد يوم 2026-4-9 ساعة 14:00

² Scholarly article, The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda, Susanne Schmitt & Stefan Behl, Journal of Information Security, 2021, pages 2,3

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

✓ إمكانية الحصول على شهادة رسمية:¹

تعزيز ثقة العملاء والشركاء من خلال إثبات الالتزام بمعايير أمن المعلومات.

✓ شمولية التطبيق:

يشمل الجوانب التقنية، التنظيمية، البشرية، والقانونية، مما يجعله إطاراً متكاملًا لإدارة أمن المعلومات على مستوى المؤسسة.

جدول 02-01: يوضح فروقات معايير امن نظام المعلومات

البيانات /المعايير	معايير ISO 27001	معايير ISO 27002	معايير ISO 27005
التطبيق	يُطبق كنظام إداري متكامل لإدارة أمن المعلومات داخل المؤسسة (سياسات + إجراءات + تدقيق)	يُطبق كدليل لاختيار وتطبيق الضوابط الأمنية (Controls) داخل المؤسسة	يُطبق عبر منهجية تحليل وتقييم ومعالجة المخاطر الأمنية
المميزات	إطار شامل، قابل للشهادة، يعتمد على التحسين المستمر وإدارة المخاطر	مرن، تفصيلي، يقدم أفضل الممارسات الأمنية	منهجي، يركز على المخاطر، يساعد على اتخاذ قرارات مبنية على تحليل دقيق

¹ Scholarly article, The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda, Susanne Schmitt & Stefan Behl, Journal of Information Security, 2021, pages 2,3

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

الاستخدام	إنشاء نظام إدارة أمن المعلومات داخل المؤسسات والحصول على شهادة رسمية	دعم وتطبيق الضوابط الأمنية ضمن نظام ISO 27001	إدارة وتقييم مخاطر أمن المعلومات لدعم النظام الأمني
مدى الانتشار	الأكثر شيوعاً عالمياً	شائع جداً كمكمل لـ ISO 27001	أقل شيوعاً من ISO 27001 لكنه أساسي في إدارة المخاطر

المصدر: من اعداد الطالبتين

يتضح من خلال تحليل المعايير الثلاثة أن هناك تكاملاً واضحاً بينها، حيث يؤدي كل معيار وظيفة محددة ضمن منظومة أمن المعلومات. فبينما يركز ISO 27001 على بناء نظام إداري شامل، يهتم ISO 27002 بتقديم الضوابط والإرشادات التطبيقية، في حين يختص ISO 27005 بإدارة وتحليل المخاطر. وبالتالي فإن فعالية أمن المعلومات لا تتحقق بالاعتماد على معيار واحد فقط، بل من خلال التكامل بين هذه المعايير لضمان حماية شاملة ومستدامة للأصول المعلوماتية داخل المؤسسات

المطلب الثالث: المخاطر التي تواجه أمن نظام المعلومات والتدابير المتخذة

تعرض أنظمة المعلومات لجملة من المخاطر المتنوعة، سواء كانت تقنية أو بشرية أو مادية، مما قد يؤثر على سلامة البيانات واستمرارية عمل النظام. وللتقليل من هذه التهديدات، تعتمد المؤسسات مجموعة من التدابير الوقائية والتنظيمية والتقنية التي تهدف إلى تعزيز مستوى الحماية وضمان أمن المعلومات

اولاً : المخاطر التي تواجه أمن نظام المعلومات:

تعرض نظم المعلومات لمجموعة من المخاطر التي قد تؤدي إلى تعطيلها أو الإضرار بمحتواها، ويمكن تصنيف هذه المخاطر إلى عدة أنواع رئيسية:¹

¹ بن طيب إبراهيم ,مرجع سبق ذكره ,ص 38- 42

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

1. الأخطاء البشرية¹

تُعد الأخطاء البشرية من أكثر المخاطر شيوعًا، حيث تنتج غالبًا عن نقص الخبرة أو سوء الفهم أو الإهمال أثناء تصميم النظم، أو إدخال البيانات، أو تحديد صلاحيات المستخدمين. وقد تؤدي هذه الأخطاء إلى حذف بيانات مهمة أو استبدالها ببيانات غير صحيحة، مما يؤثر سلبيًا على كفاءة النظام وموثوقية المعلومات.

2. المخاطر البيئية والطبيعية

تشمل هذه المخاطر الكوارث الطبيعية مثل الحرائق، الفيضانات، الزلازل، وانقطاع التيار الكهربائي، إضافة إلى الأعطال التقنية المرتبطة بأنظمة التبريد والطاقة. وغالبًا ما تؤدي هذه المخاطر إلى توقف الأنظمة لفترات متفاوتة، مع احتمال فقدان البيانات أو الحاجة إلى وقت وتكلفة كبيرة لاسترجاعها.

3. الجرائم المعلوماتية والهجمات الإلكترونية

تمثل الجرائم المعلوماتية تهديدًا متزايدًا لأمن نظم المعلومات، وتشمل محاولات الاختراق، سرقة البيانات، نشر البرمجيات الخبيثة، وهجمات حجب الخدمة. وقد تصدر هذه الهجمات من أطراف خارج المؤسسة مثل القراصنة، أو من داخلها عبر إساءة استخدام الصلاحيات الممنوحة للموظفين، مما يجعلها من أخطر أنواع التهديدات.

(5) مخاطر الشبكات والاتصال بالإنترنت

يزيد ارتباط نظم المعلومات بالشبكات العامة، خاصة شبكة الإنترنت، من احتمالية التعرض للاختراق أو تسريب البيانات أثناء نقلها. كما يشكل البريد الإلكتروني والتطبيقات غير الآمنة وسيلة شائعة لاختراق الأنظمة، سواء عبر المرفقات الضارة أو الروابط المشبوهة

¹ بن طيب إبراهيم , مرجع سبق ذكره , ص 38- 42

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

ثانيا : التدابير المتخذة لضمان أمن نظام المعلومات والوسائل الحماية

في ظل تزايد التهديدات، تعتمد المؤسسات على تدابير متكاملة لضمان أمن نظام المعلومات. وفيما يلي أهم هذه

الإجراءات:¹

1. الإجراءات الوقائية لحماية النظام

هي مجموعة خطوات يتم اتخاذها مسبقاً لتفادي أي خطر أو هجوم قد يهدد النظام المعلوماتي، سواء كان داخلي أو خارجي، بهدف تقليل احتمال حدوث المشكلات قبل وقوعها.

2. التدابير التقنية

تعني استخدام أدوات وبرامج حماية مثل مضادات الفيروسات، جدران الحماية، وأنظمة كشف الاختراق، وذلك بهدف حماية البيانات ومنع التلاعب بها أو الوصول غير المصرح به إليها.

3. السياسات التنظيمية والإدارية

هي قواعد يتم وضعها داخل المؤسسة لتحديد من يمكنه الوصول إلى المعلومات وكيفية استخدامها، مع تحديد مسؤوليات كل مستخدم لضمان التحكم في الصلاحيات وتقليل سوء الاستعمال.

4. الإجراءات الرقابية الداخلية

هي عمليات متابعة ومراقبة مستمرة لنشاط المستخدمين داخل النظام، بهدف اكتشاف أي تصرف غير عادي أو استخدام غير مشروع للموارد المعلوماتية.

¹ دليلة العوني ,مرجع سبق ذكره,ص82- 78

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

5. التدابير الفيزيائية¹

تعني حماية الأجهزة والمعدات بشكل مادي، مثل تأمين غرف السيرفرات، استخدام الأقفال أو بطاقات الدخول، ومنع أي شخص غير مخول من الوصول إلى البنية التحتية.

6. التكامل بين التدابير

يعني أن كل هذه الإجراءات تعمل معاً بشكل منسق، لأن الحماية لا تكون فعالة إلا إذا اجتمعت التقنية والتنظيم والرقابة والحماية الفيزيائية لضمان السرية والسلامة واستمرارية المعلومات

من خلال ما تم عرضه حول المخاطر والتدابير، نلاحظ أن نظم المعلومات تواجه عدة تهديدات، أهمها الأخطاء البشرية والهجمات الإلكترونية، لأنها تتكرر وصعب التحكم فيها. كما توجد مخاطر بيئية أيضاً لا يمكن السيطرة عليها تقنياً، وهذا ما يفرض على المؤسسات أن تعتمد حلول شاملة للتعامل معها. ومن جهة أخرى، يتضح أن حماية نظم المعلومات لا تعتمد على إجراء واحد فقط، بل على تكامل عدة تدابير تعمل مع بعضها. هذا التكامل يساعد على رفع مستوى الحماية، وضمان استمرارية عمل المؤسسة، وتقليل الخسائر الممكنة.

المبحث الثاني: ماهية إدارة استمرارية الاعمال

تمهيد:

تُعَدُّ إدارة استمرارية الأعمال من المفاهيم الحديثة التي تهدف إلى ضمان استمرارية الأنشطة الأساسية للمؤسسات ومواجهة الأزمات والاضطرابات المحتملة من خلال وضع خطط واستراتيجيات تضمن الحد من المخاطر وسرعة التعافي وفي هذا السياق، يُعَدُّ أمن نظام المعلومات عنصراً أساسياً في دعم إدارة استمرارية الأعمال، من خلال حماية البيانات والأنظمة المعلوماتية من التهديدات المختلفة، مما يعزز قدرة المؤسسة على تحقيق الاستقرار التنظيمي وضمان استمرارية أداؤها بكفاءة.

¹ دليلة العوني، مرجع سبق ذكره، ص 82-78

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

المطلب الاول: مفهوم إدارة استمرارية الاعمال

تمهيد:

تُعد إدارة استمرارية الأعمال من الركائز الأساسية التي تعتمد عليها المؤسسات الحديثة لضمان استقرارها في بيئة تتسم بتزايد المخاطر وعدم اليقين. فهي لا تقتصر على وضع خطط للطوارئ، بل تمثل نظاماً إدارياً متكاملًا يعزز قدرة المنظمة على الاستمرار والتعافي عند حدوث الأزمات. ومن ثمّ، فإن فهم مفهومها وأهميتها، إلى جانب تحديد متطلباتها الأساسية، يشكل أساساً لبناء نظام فعال لاستمرارية الأعمال.

اولاً: مفهوم إدارة استمرارية الاعمال:

نشير في هذا الصدد الى مصطلح ادارة استمرارية الاعمال بالترميز التالي(BCM)، ولقد تنوعت وتعددت التعاريف من الخبراء والباحثين بحيث نذكر منها ما يلي:

- عرفها (Chan) بأنها عملية إدارية تركز على كشف المخاطر المحتملة المؤثرة على استمرارية المنظمة وبقاؤها مبكراً من خلال تنفيذ إجراءات وقائية تحول دون تلك المخاطر لضمان استمرارية التشغيل.¹
- كما عرف على انه إطار عمل يتكون من خطط تساعد في ضمان استمرار عمليات الشركة عند التعرض إلى كارثة.²
- كما يمكننا القول بأن إدارة استمرارية الأعمال تمثل مجموعة الإجراءات التي تجعل المنظمات على أهبة الاستعداد لمواجهة المخاطر والأزمات من خلال خطط معدة سلفاً تمكن الجهة من الاستجابة للتعطل واستئناف الأعمال والتعافي واستعادة الخدمات المقدمة والتي حددت في أهداف استمرارية الاعمال.³

¹ أسماء عبد الرحمن الغامدي , واقع إدارة استمرارية الاعمال ايزو 22031 في القطاع العام لمواجهة الازمات : المملكة العربية السعودية نموذجاً , مجلة إدارة المخاطر والأزمات

المجلد 4, العدد 1, 30 مارس 2022 ص 20

² موقع الكتروني <https://hbrarabic> :

³ أسماء عبد الرحمن الغامدي , مرجع سبق ذكره , ص 20

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

- كما يعرف إدارة استمرارية الأعمال هي تطوير الاستراتيجيات والخطط والإجراءات لحماية أو توفير بديل طريقه العمليات الخاصة بالعمليات التجارية التي إذا توقفت يمكن أن تلحق أضرارًا جسيمة أو تسبب خسائر فادحة، وهي تشمل خطة استمرارية الاعمال وإدارة الازمات.¹

وانطلاق من كل هذه التعريف السابقة يمكن صياغة تعريف الشامل لإدارة استمرارية الاعمال على نحو التالي:

تُعرف إدارة استمرارية الأعمال (BCM) بأنها إطار إداري ومنهجي متكامل يهدف إلى تمكين المؤسسة من التعرف المبكر على المخاطر والتهديدات المحتملة التي قد تؤثر على استمرارية أنشطتها، وتقييم آثارها، ووضع السياسات والاستراتيجيات والخطط الوقائية والعلاجية الكفيلة بمنع وقوعها أو الحد من تداعياتها، بما يضمن استمرار العمليات الحيوية أو استعادتها في الوقت المناسب عند التعرض لأزمات أو كوارث، مع الحفاظ على مصالح أصحاب المصلحة وسمعة المؤسسة واستدامة أدائها

هذا التعريف يجمع بين كونها عملية إدارية، وإطار عمل قائم على التخطيط المسبق، ومنظومة إجراءات تهدف إلى الوقاية والاستجابة والتعافي بما يحقق استمرارية الأعمال بكفاءة وفعالية.

ثانيا: أهمية ادارة استمرارية الأعمال

تمثلت الأهمية في العناصر التالية:²

- ✓ تُعد إدارة استمرارية الأعمال وظيفة تنظيمية حديثة نسبياً، برزت أهميتها بشكل متزايد خلال العقود الأخيرة نتيجة تنامي المخاطر والأزمات التي تواجه منظمات الأعمال;
- ✓ تسهم في ضمان استمرارية العمليات الحيوية داخل المؤسسة، لاسيما الأنشطة الحرجة التي يترتب على تعطيلها آثار مالية وتشغيلية جسيمة ;

¹ خديجة يحيى العرياني هناء علي ضحوي، إدارة المعلومات بفاعلية اثناء الازمات من خلال نظام إدارة استمرارية الاعمال في المؤسسات، المجلة الدولية لنشر والبحوث والدراسات، المجلد الثالث، 20 أكتوبر 2021 ص71

² خديجة يحيى عرياني هناء علي ضحوي، مرجع سبق ذكره، ص 73

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

- ✓ تمثل أداة استراتيجية لتعزيز قدرة المؤسسات، خاصة في القطاعات الصناعية والمالية، على مواجهة الاضطرابات والحفاظ على استقرارها التشغيلي¹;
- ✓ تدعم استدامة الأداء المؤسسي من خلال الاعتماد على التقنيات الحديثة والأنظمة الداعمة للأعمال اليومية والعمليات الأساسية;
- ✓ تعزز دور المؤسسة في دعم الاقتصاد الوطني، باعتبار أن استمرارية القطاعات الحيوية تنعكس إيجاباً على استقرار البيئة الاقتصادية ككل;
- ✓ تسهم في ترسيخ ثقافة تنظيمية قائمة على الاستعداد المسبق للطوارئ، من خلال تبني ترتيبات وإجراءات تضمن التعامل الفعال مع الأزمات وتقليل آثارها السلبية.

لاحظنا من خلال أهمية ان إدارة استمرارية الاعمال لم تعد مجرد وظيفة تنظيمية حديثة، بل أصبحت أداة استراتيجية محورية في مواجهة بيئة غير مستقرة، حيث يبرز دورها بشكل خاص في ضمان استمرارية الأنشطة الحيوية التي يرتبط توقفها بخسائر والكوارث مباشرة، وهو ما يعكس تحولها من بعد تقني إلى بعد استراتيجي يؤثر في استقرار المؤسسة والاقتصاد ككل. كما أن التركيز على ترسيخ ثقافة الاستعداد المسبق يدل على أن الاستمرارية لا تُبنى عند وقوع الأزمة، بل تُؤسس ضمن الممارسات اليومية للمؤسسة.

ثالثاً: متطلبات ادارة استمرارية الاعمال

- ترتكز إدارة استمرارية الأعمال على مجموعة من المتطلبات الأساسية التي تضمن استعداد المؤسسة لمواجهة الظروف الطارئة وتمثلت في النقاط التالي:²

¹ خديجة يحي عرياني، هناء علي ضحوي، مرجع سبق ذكره، ص 73

² فايز جمعة صالح النجار، اروي محمد الحرايزة، الدكاء الاستراتيجي واثره في إدارة الاستمرارية الاعمال دراسة حالة في امانة عمان الكبرى، مجلة العالمية للاقتصاد والاعمال، ص 342

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

✓ التزام ودعم الإدارة العليا ويقصد بها:¹

- تبني الإدارة العليا لمفهوم استمرارية الأعمال أصبح شرطاً جوهرياً لنجاح تطبيقه داخل المنظمة;
- يتجسد هذا الدعم في إنشاء هيكل تنظيمي أو لجنة مختصة تتولى الإشراف على نظام إدارة استمرارية الأعمال;

- ضمان توفير الموارد المالية والبشرية اللازمة لتنفيذ البرامج والخطط ذات الصلة;

✓ تقييم المخاطر وإدارتها ويقصد بها:

- تحديد المخاطر المحتملة التي قد تؤثر على سير العمليات وتحليل طبيعتها ومصادرها وتقييم درجة تأثير كل خطر واحتمالية وقوعه لتحديد مستوى خطورته;
- ترتيب المخاطر وفق أولويتها وتأثيرها على الأنشطة الحيوية.
- وضع تدابير وقائية وإجراءات تصحيحية تهدف إلى تقليل احتمالية حدوث المخاطر أو الحد من آثارها عند وقوعها.

✓ تحليل تأثير الأعمال (BIA):

- تحديد العمليات وجمع البيانات المتعلقة بالوظائف التشغيلية وأنظمة الدعم وتطبيقات تكنولوجيا المعلومات وتحليلها;
- إجراء مقابلات مع المسؤولين عن الوحدات التنظيمية للتحقق من دقة المعلومات وتحديد أولويات الاسترداد;
- تحديد زمن الاسترداد المقبول لكل نشاط (الفترة الزمنية بين التوقف واستعادة التشغيل);
- إعداد تقرير شامل يتضمن نتائج التحليل وأولويات الاستعادة، ورفعها للإدارة التنفيذية لاتخاذ القرارات المناسبة.

ومن خلال هذا الطرح يتضح لنا أن متطلبات إدارة استمرارية الأعمال تركز على دعم قيادي فعال، ومنهجية دقيقة في إدارة المخاطر، وتحليل علمي لتأثير تعطل العمليات، وعلى أي مؤسسة أن تسعى لتطبيق إدارة استمرارية الاعمال وأن تركز على تطبيقها على أكمل وجه للتفادي الأزمات وتعامل معها بكل كفاءة وفاعلية.

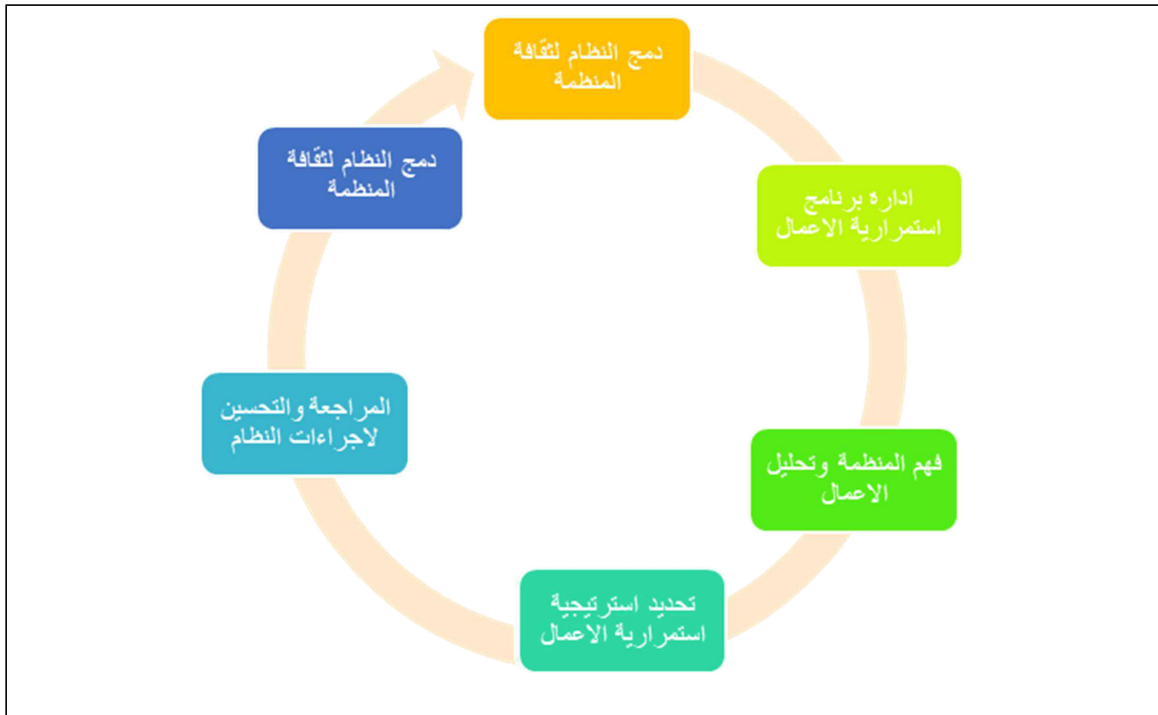
¹ فايز جمعة صالح النجار اروي محمد الحرايزة , مرجع سبق ذكره , ص342

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

رابعاً: دورة حياة إدارة استمرارية الاعمال

تمر إدارة استمرارية الاعمال بسلسلة من الخطوات حسب (Smith, 2003) تتمثل فيما يلي:¹

الشكل 01-02: دورة حياة إدارة استمرارية الاعمال



المصدر: أسماء عبد الرحمن واقع إدارة استمرارية الاعمال ايزو 22301 في القطاع العام لمواجهة الازمات: المملكة العربية

السعودية نموذجاً ص 5

وفيما يلي سنتطرق الى تفصيل لهذه السلسلة من الخطوات:

- برنامج إدارة استمرارية الاعمال: تركز على التزام الإدارة العليا ودعمها المستمر، من خلال إعداد وتطوير خطط استمرارية الأعمال، مع توفير.

¹ أسماء عبد الرحمن الغامدي مرجع سبق ذكره ص 21 = 22

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

- الموارد البشرية والمادية اللازمة لضمان إنشاء البرنامج وتنفيذه بفعالية. كما تتطلب تحديد هيكل تنظيمي واضح، سواء بإنشاء وحدة متخصصة أو تعيين مسؤول يتولى الإشراف على إدارة استمرارية الأعمال داخل المؤسسة.¹
- فهم المنظمة:

يتحقق ذلك من خلال الإلمام الشامل بأهداف المنظمة وتوجهاتها الاستراتيجية، مع تحديد أولوياتها الأساسية والموارد الضرورية لسير نشاطها. كما يشمل إجراء تحليل دقيق للمخاطر المحتملة التي قد تؤثر على العمليات، بما يسمح ببناء تصور واضح لطبيعة التهديدات وتأثيرها على استمرارية الأعمال

• تحديد استراتيجية استمرارية الأعمال:

يتم ذلك من خلال إدماج إدارة استمرارية الأعمال ضمن الاستراتيجية العامة للمنظمة، مع وضع سيناريوهات محتملة للأزمات والكوارث، وتحديد الإجراءات المناسبة للتعامل معها، بما يضمن استمرارية الأنشطة الحيوية وتقليل آثار الاضطرابات.

• تنفيذ وتطوير النظام:

يرتكز هذا الجانب على تفعيل خطط الاستجابة للطوارئ التي تم إعدادها مسبقاً، مع توثيقها وتسهيل الوصول إليها عند الحاجة. كما يشمل تنفيذ خطط الاستمرارية من قبل الفرق المختصة، والعمل على تطويرها بشكل مستمر لضمان القدرة على التعافي من آثار الأزمات بكفاءة.

• المراجعة والتحسين لإجراءات النظام:

يتضمن هذا العنصر إجراء مراجعة دورية لخطط استمرارية الأعمال واختبار فعاليتها، بهدف الكشف عن أوجه القصور أو الفجوات، والعمل على معالجتها. كما يشمل تنظيم تدريبات عملية للموظفين لضمان جاهزيتهم لتنفيذ هذه الخطط عند الضرورة

¹ أسماء عبد الرحمن الغامدي مرجع سبق ذكره ص 21-22

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

• دمج النظام في ثقافة المنظمة:

يتطلب نجاح نظام استمرارية الأعمال أن يصبح جزءًا من الثقافة التنظيمية، وذلك من خلال تعزيز وعي الموظفين بأهميته،

وتوضيح أدوارهم ومسؤولياتهم، إضافة إلى دعم التعلم والتدريب المستمر لضمان التطبيق الفعال للإجراءات¹

يتضح أن دورة حياة إدارة استمرارية الأعمال تقوم على منهجية ديناميكية مستمرة تبدأ بدعم الإدارة العليا ولا تنتهي عند التنفيذ، بل تمتد إلى المراجعة والتحسين المستمر، وهو ما يعكس طبيعتها كعملية متجددة وليست إجراءً مؤقتًا. كما أن إدماج الاستمرارية ضمن الاستراتيجية العامة وفهم المنظمة يؤكد على ضرورة توافيقها مع الأهداف الكبرى، في حين يشكل دمجها في الثقافة التنظيمية على أهمية المرحلة، لأنها تضمن استدامة التطبيق وتحويل من خطط مكتوبة إلى ممارسات فعلية داخل المؤسسة.

المطلب الثاني : معايير إدارة استمرارية الاعمال

أولا : معايير إدارة استمرارية الاعمال

يوجد العديد من المعايير الدولية الخاصة بإدارة استمرارية الأعمال، غير أن هذه الدراسة اقتصرت على ثلاثة معايير

أساسية تم اختيارها لارتباطها المباشر بهذا المجال، والمتمثلة في:

▪ **معييار NIST SP 800-34** : يعرف معيار NIST SP 800-34 بأنه دليل إرشادي يقدم مجموعة من

التوصيات والاعتبارات المنهجية التي تساعد المؤسسات على إعداد خطط الطوارئ الخاصة بأنظمة المعلومات، بما يضمن

الاستجابة الفعالة واستمرارية الأنشطة في حالة وقوع الكوارث. ويركز هذا المعيار بشكل أساسي على الجوانب التقنية

المرتبطة باستمرارية نظم المعلومات، حيث يوضح كيفية إعداد خطط التعافي من الكوارث (DRP)، وتحديد الأدوار في

تعزيز جاهزية المؤسسة لمواجهة المخاطر التقنية وتقليل آثارها على سير العمل.²

¹ أسماء عبد الرحمن الغامدي مرجع سبق ذكره ص 21- 22

² Erma Dearnawati et al., Preparation of IT Disaster Recovery Plan (DRP) using NIST SP 800-34 Framework, Eduvest Journal, Vol.5, No.1, 2025 ص 955.

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

■ **معييار ISO 22317** : يُعد معيار ISO 22317 مواصفة تقنية تهدف إلى تقديم إرشادات منهجية لإنشاء وتنفيذ والحفاظ على عملية رسمية وموثقة لتحليل تأثير الأعمال (BIA) داخل المؤسسة. ويركز هذا المعيار على تحليل تأثير الانقطاعات أو الأزمات المحتملة على مختلف أنشطة المؤسسة، من خلال تحديد الأنشطة الحرجة وتقييم درجة حساسيتها، بالإضافة إلى تحديد أولويات الاستمرارية وتقدير الزمن المقبول للتعافي. كما يساهم هذا المعيار في دعم عملية اتخاذ القرارات من خلال توفير معلومات دقيقة حول تأثير المخاطر على العمليات، مما يساعد المؤسسات على وضع استراتيجيات فعالة لضمان استمرارية الأعمال وتقليل آثار التوقف.¹

وقد تم التركيز بشكل خاص على معيار **ISO 22301** باعتباره الأكثر شيوعاً واعتماداً داخل المؤسسات، نظراً لما يوفره من إطار متكامل يحدد متطلبات إنشاء وتنفيذ وتحسين نظام إدارة استمرارية الأعمال. وفيما يلي عرض موجز لأهم متركزات هذا المعيار.²

1. **تحليل سياق المؤسسة**: يركز النظام في بدايته على فهم شامل للبيئة التي تنشط فيها المؤسسة، سواء كانت عوامل داخلية كالهياكل التنظيمية والثقافة المؤسسية والموارد المتاحة، أو عوامل خارجية مثل المتطلبات القانونية والظروف الاقتصادية والمخاطر البيئية. كما يقتضي تحديد الأطراف ذات العلاقة وتوضيح نطاق تطبيق نظام استمرارية الأعمال بدقة، باعتبار ذلك الأساس الذي تُبنى عليه باقي العمليات.

2. **التزام القيادة العليا** : يُعد دعم الإدارة العليا عنصراً جوهرياً في نجاح النظام، إذ يتعين عليها مواءمة نظام استمرارية الأعمال مع التوجه الاستراتيجي للمؤسسة، وضمان إدماجه ضمن العمليات اليومية. ويشمل ذلك إقرار سياسة رسمية، وتحديد المسؤوليات بوضوح، وتعزيز ثقافة التحسين المستمر داخل المؤسسة.

¹ موقع الكتروني [ISO/TS 22317:2021 - Business Impact Analysis Guidelines for BCMS](https://www.iso.org/standard/72431.html) : شهود يوم 2026 - 10 - 4 على ساعة 3:15

² British Standards Institution (BSI), ISO 22301: Business Continuity Management – Your Implementation Guide, London: BSI, 2016.p5

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

3. التخطيط (Clause 6 – Planning)

يركّز بند التخطيط في معيار ISO 22301 على بناء الأساس الاستراتيجي لنظام إدارة استمرارية الأعمال، من خلال تبني منهج استباقي قائم على تحليل المخاطر وتحديد الأهداف.

يوجب هذا البند على المنظمة:

- تحديد المخاطر والفرص التي قد تؤثر على تحقيق أهداف استمرارية الأعمال;
- وضع أهداف قابلة للقياس لنظام ; BCMS
- تحديد الإجراءات الكفيلة بمعالجة المخاطر;
- إعداد خطط عمل تضمن تحقيق النتائج المرجوة;

تؤكد أن التخطيط الفعال يشكل حلقة الوصل بين السياسة العامة والمرحلة التنفيذية، مما يضمن الانتقال المنهجي من الإطار النظري إلى التطبيق العملي.¹

4. التشغيل (Clause 8 – Operation)

يمثل بند التشغيل المرحلة التنفيذية المحورية في نظام إدارة استمرارية الأعمال، حيث يتم تحويل الخطط والاستراتيجيات إلى إجراءات عملية قابلة للتطبيق أثناء الأزمات.²

¹ Sánchez Domínguez, Andrea Patricia, Business Continuity Management: A Holistic Framework for Implementation, Master's Starred Paper, Department of Information Systems, St. Cloud State University, Minnesota, United States, 2016 p36 39

² Sánchez Domínguez, Andrea Patricia, Business Continuity Management: A Holistic Framework for Implementation, Master's Starred Paper, Department of Information Systems, St. Cloud State University, Minnesota, United States, 2016 p43 50

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الأعمال

يشمل هذا البند:

✓ تقييم المخاطر المرتبطة بالأنشطة الحرجة

✓ تنفيذ تحليل الأثر على الأعمال لتحديد العمليات الحيوية;

✓ تحديد حدود زمن التعافي ونقاط استعادة البيانات ;

✓ تطوير استراتيجيات الاستمرارية ;

✓ اعداد الاستجابة لطوارئ وتعافي ;

وتشير الدراسة إلى أن بند التشغيل يُعد جوهر المعيار، لأنه يحدد القدرة الحقيقية للمؤسسة على الصمود أمام الانقطاعات. فوجود وثائق دون اختبار أو تطبيق فعلي لا يحقق الاستمرارية الفعلية. كما تؤكد الباحثة أن التكامل بين تحليل الأثر، إدارة المخاطر، ووضع الاستراتيجيات يساهم في تعزيز المرونة التنظيمية ويقلل من الآثار المالية والتشغيلية للأزمات.¹

5. توفير الدعم والموارد

يقتضي نجاح النظام توفير الإمكانيات البشرية والمادية الكافية، وضمان كفاءة العاملين عبر التدريب والتوعية المستمرة. كما يشمل تنظيم قنوات الاتصال أثناء الأزمات، وإحكام إدارة الوثائق والسجلات، بما يضمن وضوح الأدوار والمسؤوليات عند وقوع أي حادث.

6. متابعة وتقييم الأداء

يشمل هذا المعيار قياس مدى فعالية النظام من خلال المراقبة المنتظمة، والتدقيق الداخلي، ومراجعة الإدارة العليا. كما يفرض معالجة حالات عدم المطابقة واتخاذ الإجراءات التصحيحية المناسبة لضمان استمرارية فعالية النظام.

¹ Sánchez Domínguez, Andrea Patricia مرجع سبق ذكره 50 - 43p

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الأعمال

7. التحسين والتطوير المستمر

يرتكز هذا البعد على تطوير النظام بشكل دائم، استناداً إلى نتائج المراجعات والتحليلات والدروس المستفادة من الحوادث

السابقة. ويهدف إلى تعزيز قدرة المؤسسة على الصمود والتكيف مع المتغيرات، بما يرسخ مفهوم المرونة التنظيمية.¹

حيث يتميز معيار ISO 22301 بعدة خصائص تجعله من أكثر المعايير اعتماداً في المؤسسات، ومن أبرز هذه المميزات:²

- تقليل الخسائر الناتجة عن الاضطرابات والأزمات
- ضمان استمرارية العمليات الحيوية وعدم توقف الأنشطة الأساسية
- تعزيز ثقة الأطراف المعنية مثل العملاء والشركاء
- تحسين فهم المؤسسة لنقاط القوة والضعف
- توفير إطار موحد لتطبيق استمرارية الأعمال داخل مختلف أقسام المؤسسة
- إمكانية دمج مع معايير أخرى مثل إدارة الجودة والبيئة
- تعزيز مرونة المؤسسة وقدرتها على التكيف مع التغيرات

وتؤكد هذه المزايا أن تطبيق هذا المعيار لا يقتصر على مواجهة الأزمات فقط، بل يمتد ليشمل تحسين الأداء العام وتعزيز

القدرة التنافسية للمؤسسة.

إن معايير إدارة استمرارية الأعمال تمثل إطاراً منهجياً متكاملًا يوجه المؤسسات نحو تطبيق فعال للاستمرارية، حيث يبرز معيار ISO 22301 كمرجعية ديناميكية قائمة على التحسين المستمر، مع التركيز على مرحلة التشغيل باعتبارها المعيار الحقيقي لفعالية النظام. كما يعكس كل من ISO 22317 و NIST SP 800-34 تكامل البعدين التحليلي والتقني، خاصة من خلال تحليل تأثير الأعمال وخطط التعافي.

¹ مرجع سبق ذكره (British Standards Institution (BSI ص 5-6

² ISO, ISO 22301 – Business Continuity, 2019

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الأعمال

ثانياً: مجالات تطبيق إدارة استمرارية الأعمال

تُطبق إدارة استمرارية الأعمال في مختلف القطاعات الحيوية نظراً لدورها الأساسي في ضمان استمرار تقديم الخدمات والعمليات الأساسية أثناء الأزمات والاضطرابات. ويمكن تلخيص أهم مجالات فيما يلي:¹

■ القطاع المالي والمصرفي

يُعد من أكثر القطاعات حساسية، حيث تُطبق إدارة استمرارية الأعمال لضمان استمرار العمليات البنكية والخدمات المالية مثل التحويلات والمعاملات الإلكترونية، مع تقليل مخاطر التوقف التي قد تؤثر على الاستقرار الاقتصادي.

■ قطاع تكنولوجيا المعلومات والاتصالات

يهدف تطبيقها في هذا المجال إلى حماية البنية التحتية الرقمية مثل الشبكات، مراكز البيانات، والأنظمة المعلوماتية، وضمان استمرارية الخدمات الرقمية والحد من آثار الأعطال والهجمات السيبرانية.

■ القطاع الصحي

تُستخدم لضمان استمرارية الخدمات الطبية والرعاية الصحية، خصوصاً في حالات الطوارئ والكوارث، من خلال الحفاظ على جاهزية المستشفيات والخدمات الحيوية لإنقاذ الأرواح.

■ القطاع الحكومي والإداري

تُطبق لضمان استمرارية الخدمات العمومية والإدارية الأساسية، بما يضمن عدم توقف تقديم الخدمات للمواطنين حتى في حالات الأزمات الكبرى.

¹ National Institute of Standards and Technology (NIST) Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev.1 U.S. Department of Commerce, 2010.p 2 – 4)

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

■ قطاع الطاقة والمرافق الحيوية

يشمل الكهرباء، الغاز، والمياه، حيث تهدف إدارة استمرارية الأعمال إلى ضمان استمرارية تدفق هذه الخدمات الأساسية التي يعتمد عليها المجتمع بشكل مباشر.¹

■ قطاع النقل واللوجستيات

تُستخدم لضمان استمرار حركة النقل البري والجوي والبحري وسلاسل الإمداد، مما يقلل من تأثير الانقطاعات على الاقتصاد والتجارة.

■ القطاع الصناعي والإنتاجي

تركز على تقليل توقف خطوط الإنتاج وحماية العمليات الصناعية من الانقطاع، بما يضمن استمرارية الإنتاج وتقليل الخسائر

من خلال ما تطرقنا إليه فمجالات التطبيق تتركز أساسًا في القطاعات الحيوية كالمجال المالي والصحي والطاقة، حيث يكون للتوقف آثار مباشرة، في حين يعكس امتدادها إلى قطاع تكنولوجيا المعلومات والقطاع الحكومي الطابع الشمولي للاستمرارية، باعتبارها ضرورة لضمان استقرار الخدمات والأنظمة بشكل عام

المطلب الثالث: العلاقة بين أمن نظام المعلومات وإدارة استمرارية الاعمال

في ضوء الإطار النظري الذي تناول مفهومي أمن نظام المعلومات وإدارة استمرارية الأعمال، يتضح أن هناك علاقة تكاملية وثيقة بين هذين المتغيرين، حيث يساهم أمن نظام المعلومات بمختلف أبعاده في دعم فعالية إدارة استمرارية الأعمال داخل المنظمة. وقد أظهرت مراجعة الأدبيات والدراسات السابقة أن كل بعد من أبعاد أمن المعلومات (مثل السرية، السلامة، والتوافر) يؤدي دورًا

¹ National Institute of Standards and Technology (NIST) Contingency Planning Guide for Federal Information Systems (SP 800-34 Rev.1 U.S. Department of Commerce, 2010.p 2 – 4

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

متفاوتاً في تعزيز قدرة المنظمة على الاستجابة للأزمات وضمان استمرارية أنشطتها دون انقطاع. وانطلاقاً من ذلك، سيتم في الفقرات التالية عرض أهم النتائج المستخلصة من تحليل أثر هذه الأبعاد، مع إبراز طبيعة العلاقة التفاعلية بينها وبين إدارة استمرارية الأعمال، خاصة في سياق بيئات العمل المعاصرة.

أولاً: العلاقة بين سرية المعلومات وإدارة واستمرارية الاعمال

تُعد السرية من الركائز الأساسية التي تضمن حماية المعلومات الحساسة من الوصول غير المصرح به، سواء تعلق الأمر ببيانات العملاء أو المعلومات المالية أو الخطط الاستراتيجية. وفي سياق إدارة استمرارية الأعمال، فإن أي خرق للسرية قد يؤدي إلى مشاكل خطيرة مثل فقدان الثقة، الأضرار بالسمعة، أو حتى التعرض لمخاطر قانونية، وهو ما قد يعرقل استمرارية النشاط. علاوة على ذلك، فإن الحفاظ على سرية المعلومات أثناء الأزمات (مثل الهجمات السيبرانية أو الكوارث التقنية) يضمن عدم استغلال هذه الظروف للوصول إلى بيانات حرجية. كما أن تطبيق سياسات التحكم في الوصول والتشفير يساهم في تأمين تدفق المعلومات داخل المنظمة بشكل يضمن استمرارية العمليات دون تهديدات إضافية.

ثانياً : العلاقة بين سلامة المعلومات وإدارة استمرارية الاعمال

تشير السلامة إلى ضمان بقاء المعلومات دقيقة وخالية من التلاعب أو التحريف. وتبرز أهميتها بشكل خاص خلال فترات الأزمات، حيث تعتمد إدارة استمرارية الأعمال على معلومات موثوقة لاتخاذ قرارات سريعة وفعالة. ففي حال تعرضت البيانات للتغيير أو الفساد (سواء بسبب أخطاء تقنية أو هجمات متعمدة)، فإن ذلك قد يؤدي إلى قرارات غير دقيقة مثل عدم إدراك مدى خطورة الأزمة أو اختيار استراتيجيات غير مناسبة للتعافي. لذلك، فإن اعتماد آليات مثل التحقق من صحة البيانات، أنظمة المراجعة، وسجلات التتبع، يعزز من موثوقية المعلومات، ويساهم في تنفيذ خطط الاستمرارية بكفاءة عالية.

ثالثاً: العلاقة بين توافر المعلومات وإدارة استمرارية الاعمال

الفصل الاول: الادبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الاعمال

يُعتبر التوافر البعد الأكثر ارتباطًا بشكل مباشر بإدارة استمرارية الأعمال، إذ يضمن بقاء الأنظمة والمعلومات متاحة للاستخدام في الوقت المناسب، خاصة خلال حالات الطوارئ. فأي انقطاع في الخدمات المعلوماتية (مثل تعطل الخوادم أو الشبكات)

قد يؤدي إلى توقف العمليات الحيوية، مما ينعكس سلبيًا على أداء المنظمة. ومن هنا، تعتمد إدارة استمرارية الأعمال على مجموعة من الإجراءات مثل أنظمة النسخ الاحتياطي، مراكز البيانات البديلة، وخطط التعافي من الكوارث لضمان استمرارية الوصول إلى المعلومات. كما أن تعزيز التوافر لا يقتصر فقط على الجانب التقني، بل يشمل أيضًا التخطيط المسبق وتحديد الأولويات، بحيث يتم ضمان استمرارية الأنظمة الأكثر أهمية أولًا.

تمهيد

يهدف هذا المبحث إلى استعراض أهم الدراسات السابقة المرتبطة بموضوع الدراسة، وذلك للتعرف على أبرز ما توصلت إليه من نتائج والاستفادة منها في دعم الدراسة الحالية وتحديد موقعها ضمن الأدبيات ذات الصلة.

المطلب الأول : الدراسات السابقة المتعلقة بامن نظام المعلومات وإدارة استمرارية الاعمال

أولا : الدراسات السابقة باللغة العربية

1. دراسة بن الطيب ابراهيم بعنوان أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة مجلة التنمية

والاقتصاد التطبيقي جامعة مسيلة العدد 03 مارس (2018) ¹

تتمحور إشكالية هذه الدراسة حول ما مدى يساهم أمن نظم المعلومات في حماية أصول المؤسسة الفكرية وضمان استمرارية نشاطها في ظل تزايد التهديدات الإلكترونية والتحول نحو الاقتصاد الرقمي حيث تهدف الى إبراز الدور المحوري لأمن نظم المعلومات في حماية رأس المال الفكري وضمان استمرارية نشاط المؤسسات الاقتصادية في ظل التحول نحو الاقتصاد القائم على المعلومات . وقد اعتمد الباحث على المنهج الوصفي التحليلي من خلال تحليل الأدبيات النظرية والدراسات السابقة والمعايير الدولية ذات الصلة بأمن نظم المعلومات، دون اللجوء إلى دراسة ميدانية، مما يعني غياب العينة الإحصائية وعدم استخدام أدوات جمع بيانات ميدانية مثل الاستبيان أو المقابلة، والاكتفاء بالمصادر الثانوية.

كما توصلت الدراسة الى:

- تزايد الاعتماد على نظم المعلومات أدى إلى ارتفاع المخاطر والتهديدات الإلكترونية;
- أمن نظم المعلومات يساهم في حماية الأصول الفكرية للمؤسسة من الضياع أو الاختراق;
- تبني سياسات أمن معلومات متكاملة يقلل من المخاطر ويعزز استقرار الأنظمة;
- تطبيق معيار ISO 27001 يساعد في تحسين حماية المعلومات وتعزيز موثوقية النظم;
- أمن نظم المعلومات يدعم استمرارية الأعمال من خلال تقليل التوقف وضمان استمرار العمليات;

¹ بن الطيب ابراهيم، أهمية أمن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة، مجلة التنمية والاقتصاد التطبيقي، العدد 03، جامعة المسيلة، الجزائر، مارس 2018.

الفصل الاول: الادبيات النظرية لأمن نظم المعلومات وإدارة استمرارية الاعمال

2. دراسة كمال مسوس بعنوان ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات

الإلكترونية مجلة الجزائرية للعملة والسياسات الاقتصادية المجلد 13 سنة 2022¹

تهدف هذه الدراسة إلى معالجة إشكالية تتمحور حول مدى مساهمة ممارسات حكومة أمن نظم المعلومات في الحد من الاعتداءات الإلكترونية داخل المؤسسات، اعتمدت الدراسة على المنهج الاستنباطي، واستهدفت عينة من إطارات وموظفي المؤسسات محل الدراسة، تم اختيارهم وفق الأسلوب الملائم لطبيعة البحث، كما استُخدم تحليل الادبيات والدراسات السابقة واستعانة بالتقرير والاحصائيات الحديثة.

وقد توصلت الدراسة إلى:

- تطبيق ممارسات حوكمة أمن نظم المعلومات يساهم بشكل فعال في الحد من الاعتداءات الإلكترونية داخل المؤسسة .
- يساهم في تقليص المخاطر المرتبطة بالهجمات والتهديدات السيبرانية؛
- يعزز مستوى الوعي الأمني لدى العاملين داخل المؤسسة؛
- يرفع من كفاءة وفعالية حماية نظم المعلومات؛
- يساعد على تحسين الرقابة والإشراف على الأنظمة المعلوماتية؛
- يدعم اتخاذ قرارات أمنية أكثر فعالية داخل المؤسسة؛
- يعزز قدرة المؤسسة على مواجهة التهديدات الإلكترونية والتكيف معها .

¹ كمال مسوس، ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الإلكترونية، المجلة الجزائرية للعملة والسياسات الاقتصادية، المجلد 13، الجزائر، 2022.

3. دراسة حليمي نبيل، حفصي رشيد، وبن عباد محمد سمير بعنوان “أهمية الأمن المعلوماتي بالمؤسسة الاقتصادية –

دراسة حالة مديرية توزيع الكهرباء والغاز بورقلة (الجزائر) المجلة الجزائرية للدراسات الاقتصادية والإدارية، المجلد

2، العدد 1، سنة 2022¹

هدفت الدراسة إلى إبراز أهمية الأمن المعلوماتي في حماية معلومات المؤسسة الاقتصادية وتقليل المخاطر التي تهدد نظم المعلومات. وتمثلت إشكالية الدراسة في التساؤل حول: ما دور أمن المعلومات في حماية معلومات المؤسسة الاقتصادية؟ اعتمد الباحثون في هذه الدراسة على منهج دراسة الحالة من خلال تطبيقها على مديرية توزيع الكهرباء والغاز بولاية ورقلة، كما استخدموا المقابلة وتحليل الوثائق كأدوات لجمع البيانات. وتمثلت عينة الدراسة في رئيس قسم الإعلام الآلي وأحد مهندسي الإعلام الآلي بالمؤسسة. كما توصلت الى اهم النتائج :

- يؤكد أمن المعلومات دوره الأساسي في حماية بيانات ومعلومات المؤسسة الاقتصادية من مختلف التهديدات;
- يساهم في تقليل المخاطر المرتبطة بنظم المعلومات مثل الاختراقات والتلاعب بالبيانات;
- يساعد في ضمان سرية المعلومات وسلامتها وتوفرها داخل المؤسسة;
- يعزز من موثوقية النظام المعلوماتي ويزيد من كفاءته التشغيلية;
- يساهم في تحسين أداء المؤسسة من خلال حماية مواردها المعلوماتية;
- أظهرت الدراسة أن وعي العاملين بأهمية أمن المعلومات يلعب دورًا مهمًا في فعالية الحماية.

¹ حليمي نبيل، حفصي رشيد، بن عباد محمد سمير، أهمية الأمن المعلوماتي بالمؤسسة الاقتصادية – دراسة حالة مديرية توزيع الكهرباء والغاز بورقلة (الجزائر)، المجلة الجزائرية للدراسات الاقتصادية والإدارية، المجلد 2، العدد 1، الجزائر، 2022

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

4. دراسة خديجة يحي العرياني وهناء علي الضحوي بعنوان ادارة المعلومات بفاعلية اثناء الازمات من خلال نظام

ادارة استمرارية الاعمال في المؤسسات مجلة الدولية لنشر البحوث والدراسات المجلد 3¹

هدفت دراسة تحليلية استندت على النسخة الحديثة لعام 2019 من المعيار الدولي ISO 22301 إلى تعزيز مفهوم نظام إدارة استمرارية الأعمال في المؤسسات وتوضيح أهميته في إدارة الأزمات والمخاطر لتقليل الخسائر الناتجة عن توقف العمليات أثناء الكوارث. حيث تتمحور إشكالية الدراسة حول ضعف قدرة المؤسسات على إدارة المعلومات وضمان استمرارية أعمالها أثناء الأزمات، في ظل غياب تطبيق نظام فعال لإدارة استمرارية الأعمال وفق المعيار الدولي ISO 22301، اعتمدت

الدراسة على منهج تحليل المحتوى وتحليل وثائق المعيار الدولي ISO 22301 لاستخلاص المتطلبات والإجراءات اللازمة لتطبيق النظام، مع تصميم قائمة مراجعة معيارية وإطار عمل يساعد المؤسسات على تقييم جودة عمليات استمرارية الأعمال وتنفيذها وفق المعيار. كما توصلت الدراسة :

○ وجود نظام إدارة استمرارية الأعمال وفق المعيار الدولي ISO 22301 ضروري لضمان استمرار العمليات أثناء الأزمات والتعطل؛

- يساهم هذا النظام في تقليل الخسائر الناتجة عن توقف الأنشطة أثناء الكوارث والمخاطر؛
- يساعد على تحديد المعلومات والموارد الأساسية التي تحتاجها المؤسسة لتحقيق أهدافها أثناء الأزمات؛
- إمكانية إضافة وثائق وإجراءات داعمة يعزز من مرونة المؤسسة وقدرتها على التكيف؛
- أظهرت الدراسة أهمية رفع مستوى الوعي المؤسسي بمفهوم استمرارية الأعمال داخل المؤسسات؛
- تؤكد على ضرورة وجود إدارة مستقلة لاستمرارية الأعمال تعمل بالتوازي مع إدارة المخاطر والأزمات؛
- تدعو إلى اعتماد أدوات تقييم معيارية لقياس نضج وكفاءة أنظمة استمرارية الأعمال وتحسينها باستمرار.

¹ خديجة يحي العرياني، هناء علي الضحوي، دارة المعلومات بفاعلية أثناء الأزمات من خلال نظام إدارة استمرارية الأعمال في المؤسسات، المجلة الدولية لنشر البحوث

والدراسات، المجلد 3

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

5. دراسة اسماء عبد الرحمن الغامدي بعنوان واقع ادراة استمرارية الاعمال وفق معيار ISO22301 في القطاع

العام لمواجهة الازمات : المملكة العربية السعودية نموذجاً مجلة ادارة المخاطر والازمات (Journal of Risk

& Crisis Management) سنة المجلد 3 العدد 1 سنة 2022¹

تهدف الدراسة الى ايجاد حل للاشكالية التي تتمحور حول ما واقع تطبيق إدارة استمرارية الأعمال وفق معيار ISO 22301 في منظمات القطاع العام بالمملكة العربية السعودية لمواجهة الأزمات؟ حيث تمت الدراسة على عينة تمثلت في منظمات القطاع العام بالمملكة العربية السعودية، وذلك بالاعتماد على الوثائق والتقارير الرسمية، دون إجراء دراسة ميدانية على الأفراد. أما أدوات الدراسة، فقد استخدمت الباحثة المنهج الوصفي التحليلي، مع تحليل الوثائق الرسمية ومعيار ISO 22301 كنموذج مرجعي للتقييم. وأظهرت نتائج الدراسة

○ أن تطبيق إدارة استمرارية الأعمال وفق معيار ISO 22301 في القطاع العام لا يزال جزئياً، مع وجود تفاوت بين الجهات الحكومية؛

○ تبني هذا النظام يسهم في تحسين كفاءة الأداء المؤسسي وتعزيز قدرة المنظمات على مواجهة الأزمات والحد من آثارها.

6. دراسة فايز جمعة صالح النجار واروى محمد الحرايزة بعنوان الذكاء الاستراتيجي واثره في ادارة الاستمرارية

الاعمال : دراسة حالة في امانة عمان الكبرى مجلة العالمية للاقتصاد والاعمال المجلد 12 العدد 3 سنة 2022²

انطلقت الدراسة من الإشكالية التالية: ما أثر الذكاء الاستراتيجي في إدارة استمرارية الأعمال داخل أمانة عمان الكبرى؟ حيث ان عينة الدراسة تمثلت في العاملين في أمانة عمان الكبرى، حيث تم اختيار عينة قصدية من الموظفين. وبخصوص أدوات الدراسة، فقد استخدم الباحثان المنهج الوصفي التحليلي، بالاعتماد على الاستبيان كأداة لجمع البيانات. حيث أظهرت النتائج على ان :

¹ اسماء عبد الرحمن الغامدي، واقع إدارة استمرارية الأعمال وفق معيار ISO 22301 في القطاع العام لمواجهة الأزمات: المملكة العربية السعودية نموذجاً، Journal of Risk & Crisis Management، المجلد 3، العدد 1، المملكة العربية السعودية، 2022

² فايز جمعة صالح النجار، أروى محمد الحرايزة، الذكاء الاستراتيجي وأثره في إدارة استمرارية الأعمال: دراسة حالة في أمانة عمان الكبرى، المجلة العالمية للاقتصاد والأعمال، المجلد 12، العدد 3، الأردن، 2022.

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

- وجود أثر إيجابي ذو دلالة إحصائية للذكاء الاستراتيجي في تحسين إدارة استمرارية الأعمال;¹
- يساهم الذكاء الاستراتيجي في تعزيز فعالية التخطيط لمواجهة الأزمات;
- يدعم مستوى الجاهزية والاستعداد المسبق داخل المؤسسة;
- يساعد في تحسين القدرة على الاستجابة واستمرارية العمليات أثناء الأزمات;
- يعزز تطبيق ممارسات استمرارية الأعمال بشكل أكثر كفاءة داخل المؤسسة.

ثانيا : الدراسات السابقة باللغة الأجنبية

• دراسة Adam A. Semlambo. Catherine G. Mkude. Edison Wazoel Lubua

Wazoel Lubua بعنوان العوامل المؤثرة على امن نظم المعلومات المجلة الدولية للهندسة والعلوم

المجلد: 10، العدد: 1، السنة: 2021²

تهدف الدراسة الى تحديد العوامل المؤثرة في امن نظم المعلومات من خلال المراجعة الشاملة للادبيات العلمية في سياق الافراد والمؤسسات مع التركيز على البيئة الافريقية انطلقت الدراسة من اشكالية مفادها ان امن نظم المعلومات لا يزال يشكل مشكلة حقيقة رغم تعدد الاجراءات التقنية والتنظيمية المتخذة وهو ما يرجع حسب الباحثين الى ضعف الفهم الشامل للعوامل الاساسية المؤثرة في امن المعلومات اعتمدت الدراسة على المنهج التحليلي الوصفي من خلال دراسة مرجعة الادبية حيث تم تحليل عدد كبير من دراسات السابقة المنشورة بعد سنة 2010 دون الاعتماد على عينة ميدانية مباشرة وقد استخدم الباحثون تحليل الوثائق كمصدر رئيسي لجمع البيانات بالاعتماد على محركات الباحث و قواعد بيانات علمية وتوصلت نتائج الدراسة الى ان العوامل المؤثرة في امن نظم المعلومات يمكن تصنيفها الى اربعة محاور رئيسة وهي : العامل البشري وسياسات امن المعلومات وبيئة العمل والعوامل الديمغرافية واكدت الدراسة ان العامل البشري يمثل

¹ فايز جمعة صالح النجار، أروى محمد الحرايزة، الذكاء الاستراتيجي وأثره في إدارة استمرارية الأعمال: دراسة حالة في أمانة عمان الكبرى، المجلة العالمية للاقتصاد والأعمال، المجلد 12، العدد 3، الأردن، 2022.

² Adam A. Semlambo, Catherine G. Mkude, Edison Wazoel Lubua, "Factors Influencing Information Systems Security", International Journal of Engineering and Science, Vol. 10, No. 1, 2021.

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

الحلقة الاضعف في منظومة امن المعلومات وان ضعف الوعي والتكوين يشكل السبب الجوهرى لاستمرار المخاطر الامنية مما يستدعي التركيز على التكوين المستمر ونشر ثقافة امن المعلومات الى جانب الحلول التقنية¹

• دراسة Yona Sangula وDidas Malekia Mfoi وAdam Aloyce Semlambo

بغنوان: Security Threats and Vulnerabilities of Information Systems: A

Case Study of the Institute of Accountancy Arusha (IAA

العنوان باللغة العربية :التحديات ونقاط الضعف الأمنية لأنظمة المعلومات: دراسة حالة معهد المحاسبة في أروشا (IAA) المنشورة في مجلة الحاسوب والاتصالات²

تطرقت هذه الدراسة الى اشكالية تزايد تهديدات وثغرات امن نظم المعلومات داخل المؤسسات التعليمية العالي بتنانيا اعتمدت الادراسة على المنهج الوصفي التحليلي باستخدام الاسلوب الكمي حيث تم جمع البيانات بواسطة استبيان وتم تحليلها باستخدام برمانج spss حيث تكون مجتمع الدراسة من جميع موظفي معهد المحاسبة باروشا من اساتذة وموظفين اداريين والبالغ عددهم 302 موظف وتم اختيار عينة عشوائية قدرها 170 مفردة وقد توصلت الدراسة الى نتائج المتمثلة في ان التهديدات وثغرات امن نظم المعلومات تعود اساسا الى اربعة محاور رئيسة تتمثل في العوامل البشرية وسياسات امن نظم المعلومات وبيئة العمل ومتغيرات ديمغرافية كما ابرزت النتائج ضعف مستوى التوعية والتدريب الامني لدى الموظفين

¹ Adam A. Semlambo, Catherine G. Mkude, Edison Wazoel Lubua, “Factors Influencing Information Systems Security”, International Journal of Engineering and Science, Vol. 10, No. 1, 202

² Adam Aloyce Semlambo, Didas Malekia Mfoi, Yona Sangula, “Security Threats and Vulnerabilities of Information Systems: A Case Study of the Institute of Accountancy Arusha (IAA)”, Journal of Computer and .Communications, Vol. 10, 2022

• دراسة Pedro Oliveira و Isabel Maria Lopes بعنوان “ Information Systems Security Policies in Small and Medium Enterprises ”

العنوان باللغة العربية :سياسة أمن نظم المعلومات في المؤسسات الصغيرة والمتوسطة منشور في مجلة هندسة وإدارة نظم المعلومات¹

هدفت الدراسة إلى تحليل تبني سياسات أمن نظم المعلومات داخل المؤسسات الصغيرة والمتوسطة. تمثلت إشكالية الدراسة في التساؤل حول مدى ملائمة منهج البحث الإجمالي في تقييم تطبيق سياسات أمن نظم المعلومات داخل المؤسسات. اعتمدت الدراسة المنهج التطبيقي باستخدام منهج البحث الإجمالي (Action Research). وتمثلت أدوات الدراسة في الملاحظة، تحليل الوثائق، وتطبيق سياسة أمن نظم المعلومات داخل ست مؤسسات صغيرة ومتوسطة. أما محل الدراسة فكان ست مؤسسات صغيرة ومتوسطة. وتوصلت النتائج إلى أن تطبيق سياسات أمن نظم المعلومات يساهم في تحسين حماية الأنظمة المعلوماتية، وأن منهج البحث الإجمالي يعد وسيلة فعالة لتحديد العوائق وتحسين تطبيق السياسات الأمنية داخل المؤسسات.

❖ دراسة Zahari Abu Bakar و Noorulsadiqin Azbiya Yaacob و Zulkifli Mohamed Udin بعنوان , “ The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework ”

العنوان باللغة العربية :أثر عوامل إدارة استمرارية الأعمال على الأداء التنظيمي: إطار مفاهيمي ، منشور في مجلة المجلة الدولية للاقتصاد والقضايا المالية²

¹ Isabel Maria Lopes, Pedro Oliveira, Information Systems Security Policies in Small and Medium Enterprises, Information Systems Engineering and Management, Vol. 1, No. 2, 2016

² Zahari Abu Bakar, Noorulsadiqin Azbiya Yaacob, Zulkifli Mohamed Udin, “The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework”, International Journal of Economics and Financial Issues, Vol. 5, No. 4, 2015

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

هدفت الدراسة إلى بناء إطار مفاهيمي يوضح العلاقة بين عوامل إدارة استمرارية الأعمال والأداء التنظيمي. تمثلت إشكالية الدراسة في معرفة مدى تأثير ممارسات إدارة استمرارية الأعمال على تحسين أداء المؤسسات. اعتمدت الدراسة المنهج التحليلي المفاهيمي من خلال تحليل الأدبيات السابقة المتعلقة بإدارة استمرارية الأعمال والأداء المؤسسي. وتمثلت أداة الدراسة في تحليل الدراسات والنماذج النظرية السابقة. أما محل الدراسة فكان الأدبيات العلمية المتعلقة بإدارة استمرارية الأعمال والأداء التنظيمي. وشملت أبعاد الدراسة التخطيط لاستمرارية الأعمال، إدارة المخاطر، الاستجابة للأزمات، واستعادة العمليات. وتوصلت الدراسة إلى أن تطبيق ممارسات إدارة استمرارية الأعمال يساهم في تعزيز قدرة المؤسسة على مواجهة الأزمات وتحسين الأداء التنظيمي والمالي.¹

❖ دراسة Piotr Jedynak بعنوان , “ Business Continuity Management – A Management Science Perspective”

العنوان باللغة العربية :إدارة استمرارية الأعمال – منظور علم الإدارة ، منشور في مجلة المجلة الدولية للإدارة المعاصرة ، العدد 4 سنة 2013²

هدفت الدراسة إلى تحليل مفهوم إدارة استمرارية الأعمال من منظور علوم الإدارة وتحديد مكانته ضمن النظريات الإدارية الحديثة. وتمثلت إشكالية الدراسة في تحديد طبيعة إدارة استمرارية الأعمال وموقعها ضمن مجال علوم الإدارة. اعتمدت الدراسة المنهج الوصفي التحليلي القائم على تحليل الأدبيات والنماذج النظرية. وتمثلت أداة الدراسة في المراجعة النظرية للدراسات والكتابات العلمية حول إدارة استمرارية الأعمال. أما محل الدراسة فكان الأدبيات العلمية في مجال الإدارة وإدارة المخاطر. وتناولت الدراسة أبعاداً رئيسية مثل مفهوم إدارة استمرارية الأعمال، تطور المفهوم، مكانته في علم الإدارة، واتجاهات

¹ Zahari Abu Bakar, Noorulsadiqin Azbiya Yaacob, Zulkifli Mohamed Udin, “The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework”, International Journal of Economics and Financial Issues, Vol. 5, No. 4, 2015
² Piotr Jedynak, “Business Continuity Management – A Management Science Perspective”, International Journal of Contemporary Management, No. 4, 2013

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

البحث في هذا المجال. وخلصت الدراسة إلى أن إدارة استمرارية الأعمال تمثل أحد المفاهيم الحديثة في الإدارة الاستراتيجية، وتلعب دوراً مهماً في تعزيز قدرة المؤسسات على مواجهة المخاطر والأزمات.

❖ دراسة كازيميرز كوسموفسكي (Kazimierz T. Kosmowski) بعنوان “ Business continuity management framework for Industry 4.0 companies ”regarding dependability and security of ICT and ICS/SCADA system

العنوان باللغة العربية : “إطار إدارة استمرارية الأعمال لشركات الصناعة 4.0 فيما يتعلق باعتمادية وأمن أنظمة تكنولوجيا المعلومات والاتصالات وأنظمة التحكم الصناعي (ICS/SCADA)”¹

ركزت هذه الدراسة على تطوير إطار لإدارة استمرارية الأعمال في سياق الصناعة 4.0 . وتمثل إشكالية الدراسة في كيفية ضمان استمرارية الأعمال في المؤسسات الصناعية الحديثة في ظل التعقيد التكنولوجي وتزايد الاعتماد على أنظمة المعلومات والتحكم الصناعي، خاصة مع ارتفاع مخاطر الهجمات السيبرانية والأعطال التقنية. وتبرز أهمية هذه الدراسة في تقديم نموذج متكامل يجمع بين الجوانب التقنية والتنظيمية لتعزيز مرونة المؤسسات الصناعية وقدرتها على مواجهة الاضطرابات . اعتمدت الدراسة على منهج مفاهيمي تحليلي من خلال بناء إطار نظري قائم على المعايير الدولية مثل ISO 22301 و ISO 31000، دون الاعتماد على عينة ميدانية، حيث تم التركيز على تحليل الأنظمة الصناعية والتكنولوجية . وتمثلت أدوات الدراسة في تحليل المخاطر، وتحليل أثر الأعمال، وبناء نموذج لإدارة الاستمرارية توصلت الدراسة إلى مجموعة من النتائج، أهمها:

✓ تطبيق نظام إدارة استمرارية الأعمال بشكل متكامل يساهم في تقليل تأثير الاضطرابات وتحسين سرعة الاستجابة;

✓ التركيز على ثقافة المؤسسة وتوعية العاملين يعد عاملاً أساسياً في نجاح تطبيق الاستمرارية;

✓ دمج الأمن السيبراني مع السلامة الوظيفية يعزز من حماية الأنظمة الصناعية ويقلل من احتمالية الانقطاع;

¹ Kazimierz T. Kosmowski, “Business Continuity Management Framework for Industry 4.0 Companies Regarding Dependability and Security of ICT and ICS/SCADA System”, Summer Safety and Reliability Seminar, Vol. 34, 2021

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

✓ أكدت أن وجود خطة استمرارية واضحة ومحدثة يساعد المؤسسات على الحفاظ على سمعتها

وضمان استمرارية خدماتها حتى في الظروف الطارئة.

❖ دراسة للباحثين katarina makka, katarina kampova بعنوان “ Integration of Cybersecurity and Business Continuity Management to Ensure Organizational Resilience in the Digital Environment

العنوان باللغة العربية التكامل بين الأمن السيبراني وإدارة استمرارية الأعمال لضمان مرونة المؤسسات في البيئة الرقمية¹

تمثلت إشكالية الدراسة في كيفية تمكين المؤسسات من مواجهة التهديدات السيبرانية والانقطاعات التكنولوجية من خلال دمج الأمن السيبراني مع إدارة استمرارية الأعمال، وتبرز أهمية الدراسة في كونها تعالج موضوعًا حديثًا يرتبط بتزايد الهجمات السيبرانية وتأثيرها المباشر على استمرارية الأعمال، كما تؤكد على ضرورة الامتثال للمعايير الدولية والتشريعات القانونية مثل ISO 22301 وتوجيهات الاتحاد الأوروبي في مجال الأمن السيبراني. اعتمدت الدراسة على منهج دراسة حالة باستخدام منهج تحليلي تطبيقي داخل مؤسسة نشط في قطاع الطاقة، حيث تم اختيار عينة تمثلت في العمليات الرئيسية والنظم المعلوماتية داخل هذه المؤسسة دون الإفصاح عن هويتها. أما أدوات الدراسة فشملت المقابلات مع الفاعلين داخل المؤسسة، وورشات العمل الموجهة مع مسؤولي العمليات، وتحليل الوثائق الداخلية، بالإضافة إلى تحليل المخاطر وتحليل أثر الانقطاع (BIA).

توصلت الدراسة إلى مجموعة من النتائج المهمة، أبرزها:

✓ إجراء تحليل الأثر يساعد بشكل دقيق في تحديد العمليات الحرجة والموارد الضرورية لاستمرارية النشاط ;

✓ تحديد مؤشرات مثل زمن الاسترجاع (RTO) ونقطة استرجاع البيانات (RPO) يساهم في تحسين سرعة التعافي

وتقليل الخسائر;

¹ Katarina Makka, Katarina Kampova, “Integration of Cybersecurity and Business Continuity Management to Ensure Organizational Resilience in the Digital Environment”, Challenges to National Defence in Contemporary Geopolitical Situation, 2024

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

✓ غياب التكامل بين الأمن السيبراني وإدارة الاستمرارية يزيد من هشاشة المؤسسة أمام التهديدات الرقمية، في حين أن وجود خطط استمرارية مدروسة ومحدثة باستمرار يعزز من قدرة المؤسسة على التكيف مع الأزمات ويضمن استقرارها التنافسي.

❖ دراسة لـ الباحثين ناتاليا كوخارسكا وأوريست بولوتاي، بعنوان “ Relationship Between Information Security and Business Continuity Management in Organizations

العنوان باللغة العربية: علاقة أمن المعلومات بإدارة استمرارية الأعمال داخل المنظمات¹

تمثلت إشكالية الدراسة في البحث عن كيفية ضمان استمرارية نشاط المنظمات في ظل تزايد التهديدات والمخاطر، خاصة مع الاعتماد الكبير على تكنولوجيا المعلومات، وتكمن أهمية الدراسة في إبراز الدور الحيوي لأمن المعلومات في حماية العمليات الحيوية وضمان استمراريته، إضافة إلى توضيح أهمية تبني معايير دولية مثل ISO في تحسين جاهزية المؤسسات لمواجهة الأزمات. اعتمدت الدراسة على المنهج التحليلي الوصفي من خلال تحليل الأدبيات والمعايير الدولية ذات الصلة، حيث لم تعتمد على عينة ميدانية محددة وإنما ركزت على تحليل مفاهيمي وتطبيقي في بيئة المنظمات بشكل عام. أما أدوات الدراسة فتمثلت في تحليل الوثائق والمعايير الدولية مثل ISO 22301 و ISO/IEC 27001، إضافة إلى مراجعة الدراسات السابقة والنماذج التطبيقية في هذا المجال.

توصلت الدراسة إلى عدة نتائج من أهمها :

✓ أن دمج أمن المعلومات ضمن نظام إدارة استمرارية الأعمال يساهم بشكل كبير في تقليل المخاطر وضمان سرعة التعافي بعد الأزمات;

¹ Nataliia Kukharska, Orest Polotai, “Relationship Between Information Security and Business Continuity Management in Organizations”, Information Technology and Security, Vol. 7, No. 2, 2019.

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

✓ أن تطبيق منهجية التخطيط والتنفيذ والمراقبة والتحسين المستمر (PDCA) يعزز من فعالية هذا النظام ويضمن استمراريته، إضافة إلى أن المؤسسات التي تعتمد استراتيجيات واضحة لإدارة المخاطر واستعادة الأنظمة تكون أكثر قدرة على الحفاظ على سمعتها وثقة العملاء;

✓ كما أظهرت النتائج أن غياب التخطيط المسبق والتدابير الوقائية قد يؤدي إلى خسائر مالية كبيرة وحتى توقف نشاط المؤسسة بشكل نهائي.

• دراسة (Georg Sven Lampe, Mihaela Maftai, Ioana Surugiu, Răzvan Cristian Ionescu) بعنوان “ Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis ”

العنوان باللغة العربية :دراسة حول نظام إدارة أمن المعلومات وإدارة استمرارية الأعمال في سياق الأزمة العالمية ضمن أعمال مؤتمر BASIQ الدولي من الدراسات الحديثة¹

تناولت هذه الدراسة العلاقة بين نظام إدارة أمن المعلومات وإدارة استمرارية الأعمال في ظل الأزمات العالمية . حيث تتمحور إشكالية الدراسة حول مدى ضرورة تكامل نظام إدارة أمن المعلومات (ISMS) مع إدارة استمرارية الأعمال (BCM) لمواجهة المخاطر العالمية مثل الأوبئة، خاصة وأن النماذج الحالية لا تغطي بشكل كافٍ هذه التهديدات. وتبرز أهمية هذه الدراسة في كونها تسلط الضوء على الحاجة إلى تطوير استراتيجيات شاملة لإدارة المخاطر والأزمات، بما يضمن حماية العمليات الحيوية والمحافظة على قيمة المؤسسة واستمراريتها في ظل التهديدات المتزايدة . اعتمدت الدراسة على منهج مزدوج يجمع بين المنهج النظري من خلال مراجعة الأدبيات والمعايير الدولية، والمنهج التطبيقي عبر تحليل أثر الأعمال (BIA) وتطبيق منهجية إدارة المخاطر داخل مؤسسات البنية التحتية الحيوية، دون تحديد عينة رقمية دقيقة بل بالتركيز على مؤسسات الطاقة والاتصالات . كما استخدمت أدوات تحليلية مثل تحليل المخاطر، تحليل أثر الأعمال، والمقارنة بالمعايير الدولية مثل ISO 27001 و ISO 22301.

¹. Georg Sven Lampe, Mihaela Maftai, Ioana Surugiu, Răzvan Cristian Ionescu, “Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis”, International .Conference on New Trends in Sustainable Business and Consumption, Vol. 6, 2020

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

توصلت الدراسة إلى عدة نتائج، أهمها :

✓ التكامل بين نظام إدارة أمن المعلومات وإدارة استمرارية الأعمال يساهم بشكل كبير في تعزيز قدرة المؤسسات على

مواجهة الأزمات وتقليل آثارها؛

✓ إدراج مخاطر الأوبئة ضمن خطط الاستمرارية يحسن من نضج أنظمة الأمن المعلوماتي ويزيد من فعالية الاستجابة للأزمات؛

✓ اعتماد تحليل أثر الأعمال يساعد المؤسسات على ترتيب أولوياتها واستعادة نشاطها بشكل تدريجي ومنظم بعد حدوث أي اضطراب، وهو ما يعزز من مرونتها واستدامتها في بيئة مليئة بالمخاطر¹.

• دراسة الباحث (Marko Niemimaa) بعنوان “Interdisciplinary Review of

Business Continuity from an Information Systems Perspective:

”Toward an Integrative Framework

العنوان باللغة العربية :مراجعة متعددة التخصصات لاستمرارية الأعمال من منظور نظم المعلومات: نحو إطار تكاملي²

تناولت الدراسة استمرارية الأعمال من منظور نظم المعلومات، حيث تمحورت إشكالياتها حول ضعف التكامل بين الدراسات

المتعلقة باستمرارية الأعمال وتشنتها بين تخصصات متعددة، مما يحد من قدرة المؤسسات على الاستعداد للحوادث والاستجابة لها

بفعالية. وهدفت الدراسة إلى توحيد الأدبيات السابقة ضمن إطار تكاملي لتحسين فهم استمرارية نظم المعلومات.اعتمدت

الدراسة على المنهج الوصفي التحليلي من خلال مراجعة أدبية شاملة شملت 83 دراسة منشورة بين سنتي 2000 و2012، مع

استخدام تحليل المحتوى وتصنيف الدراسات كأدوات للتحليل.

¹ . Georg Sven Lampe, Mihaela Maftai, Ioana Surugiu, Răzvan Cristian Ionescu, “Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis”, International Conference on New Trends in Sustainable Business and Consumption, Vol. 6, 2020

² Marko Niemimaa, “Interdisciplinary Review of Business Continuity from an Information Systems Perspective: Toward an Integrative Framework”, Communications of the Association for Information Systems, Vol. 37, No. 1, 2015

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

توصلت الدراسة إلى أن استمرارية نظم المعلومات تعتمد على أربعة محاور أساسية تتمثل في العوامل الاجتماعية والتكنولوجية والنماذج التنظيمية وأهمية الاستمرارية، كما أكدت أن غياب إطار موحد أدى إلى تشتت الجهود البحثية، وأن تطوير إطار تكاملي يساهم في تعزيز جاهزية المؤسسات وتقليل الخسائر الناتجة عن تعطل الأنظمة.

المطلب الثاني : ابعاد المتعلقة بامن نظام المعلومات وإدارة استمرارية الاعمال

أولا : ابعاد امن نظام المعلومات

الجدول 01-03 : ابعاد امن نظام المعلومات من الدراسات السابقة

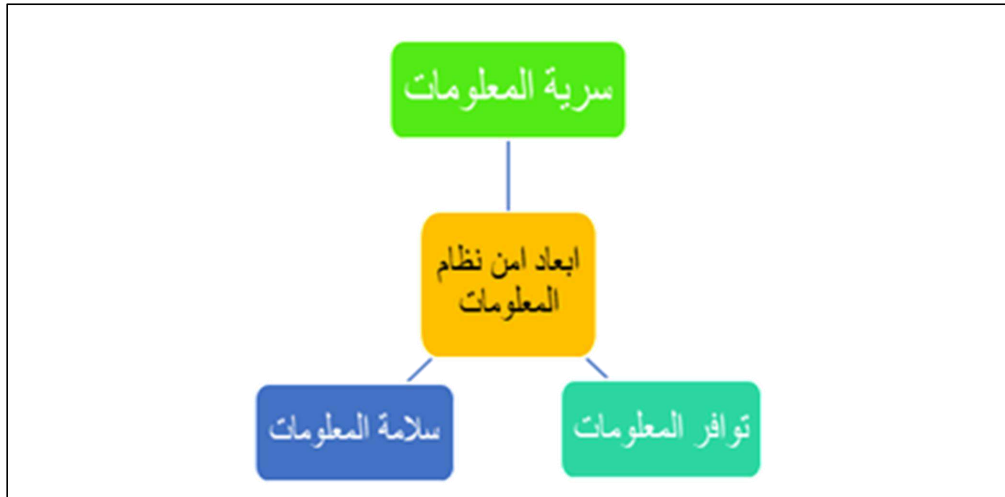
الرقم	الدراسة	الابعاد
1	(بن الطيب إبراهيم 2018)	سرية المعلومات، سلامة المعلومات، توافر المعلومات
2	(حليمي نبيل، حفصي رشيد، بن عياد محمد سمير 2022)	سرية المعلومات، سلامة المعلومات، توافر المعلومات
3	(كمال مسوس 2022)	البعد التنظيمي , البعد التقني , إدارة المخاطر, الالتزام بالمعايير الدولية , الوعي والتدريب الأمني
4	(Adam Smlambo et al) 2021	العامل البشري، سياسات أمن المعلومات، بيئة العمل، العوامل الديمغرافية
5	Hermano Perrelli de ،Gliner Dias Alencar) ,Ivaldir Honório de Farias Júnior ,Moura ,José Gilson de Almeida Teixeira Filho (2018	مستويات نضج أمن المعلومات ,ضوابط الأمن ,تحليل المخاطر, حوكمة أمن المعلومات
6	Pedro Oliveira و Isabel Maria Lopes (2016)	سياسات أمن نظم المعلومات، عوامل النجاح في تطبيق الأمن، وإدارة المخاطر الأمنية

المصدر : من اعداد الطالبتين بناء على الدراسات السابقة

الفصل الاول :الادبيات النظرية لأمن نظام المعلومات و إدارة استمرارية الاعمال

في ضوء ما استعرضته الدراسات السابقة من أطر نظرية وأبعاد مختلفة لأمن نظام المعلومات، ستعتمد هذه الدراسة على الأبعاد التالية: سرية المعلومات، سلامة المعلومات، وتوافر المعلومات. ويعود اختيار هذه الأبعاد إلى كونها من أكثر الأبعاد استخداماً واعتماداً في الدراسات العلمية السابقة، كما تتميز هذه الأبعاد بالشمولية والوضوح في قياس مستوى أمن نظام المعلومات داخل المؤسسات. وتعرف هذه الأبعاد في الأدبيات العلمية باسم مثلث أمن المعلومات (CIA)، الأمر الذي يبرر اعتمادها كأساس في هذه الدراسة وفي ادناه توضيح لكل بعد من هذه الابعاد كما يوضحها الشكل التالي :

الشكل 01-03 : يوضح ابعاد امن نظام المعلومات



المصدر : من اعداد الطالبتين

➤ سرية المعلومات:

هي خاصية تهدف إلى حماية البيانات من الاطلاع أو الوصول من قبل أشخاص أو أنظمة غير مخولة، بحيث يقتصر الوصول إليها فقط على الأفراد الذين يملكون صلاحيات محددة. وتتحقق هذه السرية من خلال تطبيق إجراءات وضوابط أمنية تمنع كشف المعلومات أو تسريبها لجهات غير مصرح لها.¹

➤ سلامة المعلومات

تشير سلامة المعلومات إلى حماية البيانات داخل النظام من التغيير أو الإلتلاف غير المشروع، بما يضمن بقاء المعلومات صحيحة ودقيقة وموثوقة دون تحريف أو تعديل غير مصرح به.²

➤ توافر المعلومات

يقصد بالتوافر ضمان إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة من قبل المستخدمين المصرح لهم، دون انقطاع أو تعطيل. وتعتبر هذه الخاصية أساسية لضمان استمرارية الأنشطة والخدمات داخل المؤسسة، خاصة في الأنظمة التي تعتمد على التشغيل المستمر.³

¹ Whitman, Michael E., & Mattord, Herbert J., Principles of Information Security, Fourth Edition, Cengage Learning, United States of America, 2011, p 12–13

² Bagies, T. Classifying software security requirements into confidentiality, integrity, and availability using machine learning approaches. مجلة PeerJ Computer Science، المجلد 10، 2024، ص 2.

³ National Institute of Standards and Technology (2017), *An Introduction to Information Security (Special Publication 800-12 Revision 1)*, pp. 1–8.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

ثانيا : ابعاد إدارة استمرارية الاعمال

الجدول 01-04 : ابعاد إدارة استمرارية الاعمال من الدراسات السابقة

الرقم	الدراسة	ابعاد
1	اسماء عبد الرحمن الغامدي 2022	التخطيط لاستمرارية الأعمال، إدارة المخاطر، التعافي من الأزمات
2	فايز جمعة صالح النجار واروى محمد الحرايزة 2022	التخطيط الاستراتيجي للاستمرارية، الاستعداد للأزمات، استعادة العمليات
3	خديجة يحيى العرياني وهناء علي الضحوي 2019	تحليل تأثير الأعمال، خطط الاستجابة للأزمات، استعادة العمليات
4	Noorulsadiqin Azbiya و Zahari Abu Bakar (2015) Zulkifli Mohamed Udin, Yaacob	التخطيط لاستمرارية الأعمال، إدارة المخاطر، الاستجابة للأزمات، واستعادة العمليات
5	2013Piotr Jedynak	إدارة المخاطر، المرونة التنظيمية، التعافي بعد الكوارث
6	كوسموفسكي (Kazimierz T. Kosmowski) 2021	إدارة استمرارية الأعمال الأمن السيبراني إدارة المخاطر الأنظمة التقنية

المصدر : من اعداد الطالبتين

اعتمدت الدراسات السابقة في تناول متغير إدارة استمرارية الأعمال على تقسيمه إلى مجموعة من الأبعاد الفرعية التي تبرز مختلف جوانبه. وعلى الرغم من أهمية هذا الطرح التحليلي التفصيلي، إلا أن الدراسة الحالية تتبنى توجهاً منهجياً مختلفاً، يتمثل في التعامل مع متغير إدارة استمرارية الأعمال كبعد مركب وشامل.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

ويستند هذا الاختيار إلى طبيعة المتغير ذاته، كونه يعبر عن منظومة متكاملة من الإجراءات والاستراتيجيات التي تهدف إلى ضمان استمرارية الأنشطة في ظل الأزمات والاضطرابات، مما يجعل تجزئته إلى أبعاد مستقلة قد لا يعكس بدقة ترابط مكوناته وتكامله الوظيفي. وعليه، تم اعتماد هذا المتغير في التحليل التطبيقي كبعد مركب

المطلب الثالث : مقارنة بين الدراسة الحالية والدراسات السابقة

في المطلب السابق، تم التطرق إلى مجموعة من الدراسات السابقة المرتبطة بموضوع البحث، سواء بشكل مباشر أو غير مباشر، وذلك باللغتين العربية والأجنبية، بهدف الإلمام بمختلف الجهود العلمية التي عاجلت هذا المجال. وقد تم التركيز على تحليل المناهج المعتمدة في هذه الدراسات، واستعراض أهم النتائج التي توصلت إليها، إلى جانب دراسة سياقات تطبيقها المختلفة، بما يسمح بإبراز نقاط الالتقاء والاختلاف بينها وبين الدراسة الحالية. ويُرتقب من هذا العرض أن يسهم في توجيه مسار البحث الراهن، من خلال الاستفادة من المعارف المتراكمة، والكشف عن الفجوات البحثية التي يسعى هذا العمل إلى معالجتها وتقديم إضافة علمية بشأنها.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

الجدول 01-05 : ملخص الدراسات السابقة

الباحث الدراسة	المؤسسة محل الدراسة والعينة	أداة المستخدمة	اهم النتائج	اهم التوصيات
الدراسة الحالية (الباحثة)	10 بنوك - 10 وكالات - ورقلة (ورقلة + حاسي مسعود)	الاستبيان مقابلة وبعض الوثائق	تطبيق مرتفع لأبعاد أمن نظام المعلومات وفعالية جيدة لإدارة استمرارية الأعمال، مع وجود ارتباط إيجابي ضعيف بينهما ودور واضح للأنظمة المعلوماتية في حماية البيانات وتقليل المخاطر.	تعزيز التكوين والوعي الأمني، وتحديث الأنظمة والبنية الرقمية، مع توفير فرق متخصصة في أمن المعلومات داخل البنوك.
بن الطيب إبراهيم (2018)	دراسة تحليلية (بدون عينة ميدانية) - المؤسسات الاقتصادية	تحليل الأدبيات	من نظم المعلومات أساس لحماية الأصول المعلوماتية وضمان استمرارية النشاط وتقليل المخاطر الإلكترونية.	اعتماد معيار ISO 27001 وتطوير سياسات أمن معلومات فعالة.
كمال مسوس (2022)	مؤسسات جزائرية - موظفون وإطارات	استبيان + وثائق	حوكمة أمن المعلومات تقلل الاعتداءات الإلكترونية وتعزز الوعي الأمني داخل المؤسسات.	تعزيز الحوكمة الأمنية وتكثيف التكوين المستمر
حليمي وآخرون (2022)	مديرية توزيع الكهرباء والغاز - ورقلة - إطارات وتقنيين	مقابلة + وثائق	أمن المعلومات يساهم في تحسين الأداء التنظيمي وتعزيز سرية وسلامة المعلومات.	دعم التكوين الأمني وتعزيز الوعي التنظيمي
العرياني والضحوي (2019)	تحليل معياري ISO 22301	تحليل محتوى	إدارة استمرارية الأعمال ضرورية لضمان استمرارية العمليات وتقليل الخسائر أثناء الأزمات.	اعتماد نظام استمرارية الأعمال وتحديثه دورياً.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

أسماء الغامدي (2022)	القطاع العام – السعودية	وثائق وتقارير	تطبيق ISO 22301 ما يزال جزئيًا رغم أهميته في تحسين الاستجابة للآزمات.	تعميم تطبيق ISO 22301 وتعزيز الجاهزية المؤسسية.
النجار والحرايزة (2022)	أمانة عمان الكبرى – موظفون	استبيان	الذكاء الاستراتيجي يعزز التخطيط والجاهزية في إدارة استمرارية الأعمال.	دعم التخطيط الاستراتيجي وتحسين اتخاذ القرار.
Semlambo (2021) وآخرون	مراجعة أدبيات (بدون عينة)	تحليل وثائق	العامل البشري يمثل الحلقة الأضعف في أمن المعلومات بسبب ضعف الوعي والتكوين.	نشر ثقافة أمن المعلومات وتكثيف التدريب.
تنزانيا IAA (2022)	معهد المحاسبة – 302 موظف	استبيان + SPSS	ضعف الوعي والتدريب الأمني يزيد من قابلية الأنظمة للاختراق.	تعزيز التدريب ورفع الوعي الأمني.
Makka & Kampova (2024)	مؤسسة طاقة (دراسة حالة)	مقابلات + وثائق	دمج الأمن السيبراني مع استمرارية الأعمال يعزز مرونة المؤسسة أثناء الأزمات.	دمج أنظمة الأمن مع إدارة استمرارية الأعمال.
Niemimaa (2015)	مراجعة 83 دراسة	مراجعة أدبيات	وجود تشتت في دراسات استمرارية الأعمال وغياب إطار موحد للتكامل.	تطوير إطار تكاملي شامل لإدارة الاستمرارية.
Jedynak (2013)	أدبيات الإدارة	تحليل نظري	إدارة استمرارية الأعمال مفهوم استراتيجي لتعزيز مواجهة المخاطر والأزمات.	تشجيع الدراسات التطبيقية في إدارة الاستمرارية.
Kosmowski (2021)	الصناعة 4.0	تحليل مخاطر	دمج الأمن السيبراني مع الاستمرارية يحسن الاستجابة ويقلل الاضطرابات.	تطوير خطط استمرارية مرنة ومحدثة.
Kucharska & Bolotay (2019)	منظمات عامة	تحليل وثائق	دمج أمن المعلومات مع استمرارية الأعمال يقلل المخاطر ويعزز التعافي.	تطبيق ISO 27001 و ISO 22301.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

Lampe et al. (2020)	بنية تحتية (طاقة/اتصالات)	+ BIA تحليل مخاطر	تكامـل ISMS و BCM ضروري لضمان استمرارية الخدمات أثناء الأزمات.	تحسين خطط التعافي وتحديد الأولويات.
Zahari Abu Bakar et al. (2015)	مؤسسات مختلفة	تحليل مفاهيمي	دائرة استمرارية الأعمال تعزز الأداء المؤسسي والقدرة على مواجهة الأزمات.	تبني استراتيجيات فعالة لاستمرارية الأعمال.

المصدر : من اعداد الطالبتين بناء على الدراسات السابقة

اولا : اوجه التشبه بين الدراسة الحالية والدراسات السابقة

تشترك الدراسة الحالية مع الدراسات السابقة في مجموعة من الجوانب، من أبرزها:

- **المنهج المعتمد:** تم الاعتماد على المنهج الوصفي التحليلي في كل من الدراسة الحالية والدراسات السابقة، باعتباره المنهج الأنسب لوصف الظاهرة محل الدراسة وتحليل العلاقات بين المتغيرات، سواء في الدراسات النظرية التي اعتمدت على تحليل الأدبيات، أو في الدراسات الميدانية التي وظفت أدوات جمع البيانات مثل الاستبيان وتحليل النتائج إحصائياً.
- **أدوات جمع البيانات:** تم الاعتماد على الاستبيان كأداة رئيسة لجمع البيانات في كلٍّ من الدراسات السابقة والدراسة الحالية، نظراً لملاءمته لطبيعة الموضوع وقدرته على قياس آراء أفراد العينة بدقة.
- **أداة تحليل البيانات:** تم استخدام الأساليب الإحصائية المناسبة لتحليل البيانات، من خلال الاعتماد على برنامج SPSS، بما يتيح معالجة البيانات واستخراج النتائج وتفسيرها بشكل علمي دقيق.

ثانيا : أوجه الاختلاف بين الدراسات السابقة والدراسة الحالية

هناك العديد من أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة، سواء من حيث الزمان والمكان والعينة، أو من حيث المتغيرات، وكذلك من حيث مجال التطبيق، والنتائج، والتوصيات.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

- من حيث الإطارين المكاني والزمني: أنجزت الدراسة الحالية خلال السنة الجامعية 2025/2026، وتم تطبيقها ميدانيًا في ولاية ورقلة (ورقلة وحاسي مسعود). في حين تنوعت الدراسات السابقة من حيث الإطار الزمني لتشمل الفترة الممتدة تقريبًا بين 2013 و2025، أما من حيث الإطار المكاني فقد طُبقت في بيئات متعددة على المستوى الدولي، شملت الجزائر، والأردن، والسعودية، إضافة إلى دراسات أوروبية وآسيوية مثل ألمانيا والصين وتنازانيا، إلى جانب دراسات تحليلية اعتمدت على معايير دولية دون تحديد دولة بعينها.
- من حيث العينة: اعتمدت الدراسة الحالية على عينة ميدانية مكونة من عشر (10) وكالات بنكية تابعة لعشر (10) بنوك مختلفة، موزعة على مستوى ولاية ورقلة (ورقلة وحاسي مسعود)، حيث تم اختيار وكالة واحدة من كل بنك باعتبارها وحدة تحليل للدراسة. وقد بلغ حجم الاستجابة في الاستبيان نسبة معتبرة مقارنة بمجموع الوكالات المستهدفة. في حين اعتمدت الدراسات السابقة على عينات مختلفة من حيث الحجم والطبيعة، شملت موظفين وإطارات وأفرادًا داخل مؤسسات متنوعة، مع تفاوت في عدد أفراد العينة ونسب التمثيل من دراسة إلى أخرى.
- من حيث القطاع : استهدفت الدراسة الحالية القطاع البنكي بمختلف أنواعه، حيث شملت بنوكًا عمومية وخاصة على مستوى ولاية ورقلة (ورقلة وحاسي مسعود)، مما يعكس طابعًا مختلفًا لمجال التطبيق. في حين تنوعت الدراسات السابقة من حيث القطاعات محل الدراسة، إذ شملت قطاعات متعددة ، إضافة إلى مؤسسات اقتصادية مختلفة، كما أن بعضها ركز على القطاع العام فقط أو القطاع الخاص فقط، وهو ما يعكس اختلافًا في بيئة التطبيق وطبيعة الأنشطة بين الدراسة الحالية والدراسات السابقة.
- من حيث المتغيرات: اعتمدت الدراسة الحالية على متغيرين رئيسيين، يتمثل المتغير المستقل في أمن نظم المعلومات، بينما يتمثل المتغير التابع في إدارة استمرارية الأعمال، بهدف دراسة العلاقة بينهما في البيئة البنكية.. في حين تناولت الدراسات السابقة متغيرات متنوعة، حيث ركز بعضها على أمن نظم المعلومات كمتغير مستقل، بينما اهتمت دراسات أخرى بإدارة استمرارية الأعمال كمتغير تابع أو ضمن إطار مفاهيمي أوسع، كما جمعت بعض الدراسات بين متغيرات

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

مختلفة مثل الحوكمة، الذكاء الاستراتيجي، وإدارة المخاطر، وهو ما يعكس اختلافًا في طبيعة المتغيرات مقارنة بالدراسة الحالية

- **من حيث النتائج :** أظهرت الدراسة الحالية مستوى مرتفعًا نسبيًا في تطبيق أبعاد أمن نظم المعلومات واستمرارية الأعمال داخل البنوك محل الدراسة، مع وجود تفاوت محدود في بعض الجوانب كأنظمة التنبيه الأمني وإدارة الصيانة. وقد اتفقت نتائجها مع الدراسات السابقة التي أكدت وجود علاقة تكاملية بين أمن المعلومات واستمرارية الأعمال، حيث يسهم تعزيز أمن المعلومات في تقليل المخاطر وتحسين قدرة المؤسسات على مواجهة الأزمات. كما اختلفت بعض الدراسات السابقة التي أشارت إلى وجود تحديات تتعلق بضعف التوعية الأمنية أو محدودية التكامل، بينما بينت الدراسة الحالية أن البنوك تطبق إجراءات الأمن والاستمرارية بمستوى جيد وفعال.

- **من حيث الابعاد :** في الدراسات السابقة، تم تناول متغير إدارة استمرارية الأعمال في أبعاد مستقلة ومجزأة، بحيث تم تحليل كل بعد على حدة. أما في هذه الدراسات، فقد اعتمدنا على بعد مركب لإدارة استمرارية الأعمال، باعتبار أن هذا البعد يجمع عناصر متعددة مترابطة، وبالتالي يعكس شمولية الظاهرة

• من حيث التوصيات :

اختلفت الدراسة الحالية عن الدراسات السابقة من حيث طبيعة التوصيات ومجال تركيزها، حيث ركزت أغلب الدراسات السابقة على ضرورة تبني المعايير الدولية مثل ISO 27001 و ISO 22301، وتعزيز خطط التعافي من الكوارث وتحليل أثر الأعمال، إضافة إلى دمج أمن المعلومات مع إدارة استمرارية الأعمال لتحسين مواجهة الأزمات وتقليل المخاطر.

أما الدراسة الحالية فقد ركزت توصياتها على تعزيز فعالية أمن نظام المعلومات داخل البنوك الجزائرية، من خلال تطوير الأنظمة المعلوماتية، وتحسين إجراءات الحماية والرقابة، ورفع مستوى الجاهزية الرقمية والأمنية بما يضمن استمرارية الخدمات البنكية وتقليل الاضطرابات والمخاطر التشغيلية. كما أولت اهتمامًا بخصوصية البيئة البنكية الجزائرية وطبيعة التحديات التي تواجهها.

الفصل الاول :الادبيات النظرية لامن نظام المعلومات و إدارة استمرارية الاعمال

ثالثا : إسهامات الدراسات السابقة في الدراسة الحالية

تتجلى إسهامات الدراسات السابقة في دعم الدراسة الحالية من خلال:

- أسهمت في إثراء الجانب النظري للدراسة من خلال دعم الأدبيات النظرية المتعلقة بأمن نظم المعلومات وإدارة استمرارية الأعمال، والمساعدة في صياغة فرضيات الدراسة؛
- ساهمت في ضبط متغيرات الدراسة، حيث تم تحديد المتغير المستقل في أمن نظم المعلومات، والمتغير التابع في إدارة استمرارية الأعمال؛
- مكّنت من تحديد وضبط المفاهيم والمصطلحات الأساسية المرتبطة بموضوع الدراسة، بما يعزز الدقة العلمية
- وفّرت تصوّرًا واضحًا حول الأساليب الإحصائية المناسبة، وكيفية استخدام أدوات جمع البيانات، لا سيما الاستبيان، وتحليلها وتفسير نتائجها؛
- ساعدت في التعمق في موضوع الدراسة بشكل منهجي ومنظم؛
- ساعدت في بناء أداة الدراسة (الاستبيان) من خلال الاستفادة من الأبعاد والمؤشرات المعتمدة في الدراسات السابقة وتكييفها مع موضوع البحث؛
- أتاحت الاطلاع على أهم النتائج التي توصلت إليها الدراسات السابقة، مما ساعد في توجيه الدراسة الحالية والانطلاق منها؛
- ساعدت في رسم الإطار العام للبحث وتنظيم مساره، بما يسهل عملية الرجوع إلى المصادر والمراجع المختلفة؛
- مكّنت من التعرف على جوانب إضافية ذات صلة بموضوع أمن نظم المعلومات واستمرارية الأعمال، والاستفادة منها في تعزيز الدراسة الحالية.

الفصل الاول: الادبيات النظرية لأمن نظم المعلومات وإدارة استمرارية الأعمال

خلاصة الفصل الأول

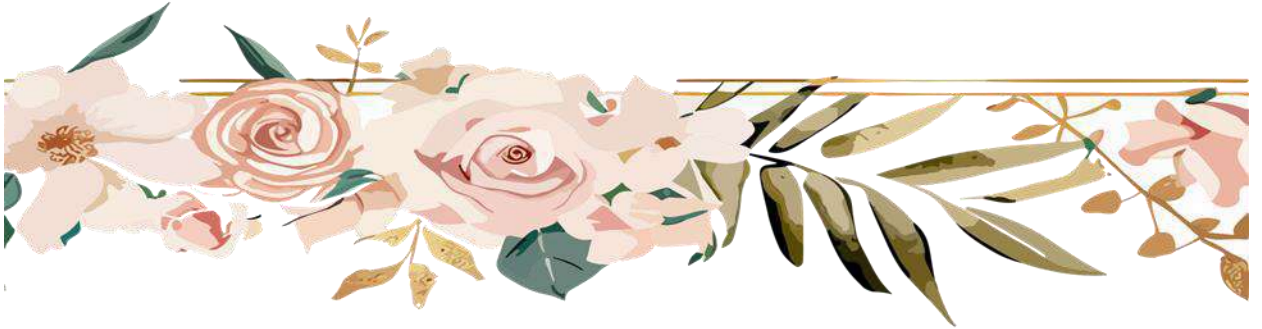
تناول هذا الفصل الإطار النظري لكل من أمن نظم المعلومات وإدارة استمرارية الأعمال، باعتبارهما من المواضيع الحديثة التي تزايدت أهميتها في ظل التحول الرقمي والاعتماد المتزايد على الأنظمة المعلوماتية داخل المؤسسات . وقد تم التطرق في البداية إلى مفهوم أمن نظم المعلومات، من خلال عرض مجموعة من التعاريف التي تناولته من جوانب تقنية وتنظيمية، مع إبراز أهدافه الأساسية المتمثلة في حماية المعلومات وضمان سريتها وسلامتها وتوافرها، إضافة إلى توضيح مكوناته ومتطلباته والاستراتيجيات المعتمدة لتحقيقه، إلى جانب عرض أهم المخاطر التي تهدده والتدابير الوقائية المعتمدة للحد منها. كما تم التطرق إلى أبرز المعايير الدولية المرتبطة بأمن المعلومات، وعلى رأسها معيار ISO 27001 باعتباره من أكثر المعايير اعتمادًا وانتشارًا داخل المؤسسات. كما تناول الفصل مفهوم إدارة استمرارية الأعمال باعتبارها إطارًا إداريًا واستراتيجيًا يهدف إلى تمكين المؤسسة من مواجهة الأزمات وضمان استمرارية أنشطتها الحيوية وتقليل آثار الانقطاعات المحتملة. وتم عرض أهميتها ومتطلباتها الأساسية، بالإضافة إلى دورة حياتها ومراحل تطبيقها داخل المؤسسة، مع التركيز على معيار ISO 22301 الذي يمثل المرجع الأساسي في إدارة استمرارية الأعمال، وتوضيح أهم خصائصه ومجالات تطبيقه في مختلف القطاعات.

ومن جهة أخرى، تم إبراز العلاقة التكاملية بين أمن نظم المعلومات وإدارة استمرارية الأعمال، حيث تبين أن حماية المعلومات وضمان سريتها وسلامتها وتوافرها تُعد من العوامل الأساسية التي تدعم قدرة المؤسسة على الاستمرار ومواجهة الأزمات بفعالية. كما أظهرت الدراسات السابقة، العربية والأجنبية، وجود اهتمام متزايد بدراسة هذه العلاقة، مع التأكيد على أن تعزيز أمن نظم المعلومات يساهم بشكل مباشر في تحسين فعالية استمرارية الأعمال وتقليل المخاطر التشغيلية والتقنية.

وفي ختام الفصل، تم استعراض أهم الدراسات السابقة ذات الصلة بموضوع البحث، وتحليل أوجه التشابه والاختلاف بينها وبين الدراسة الحالية، مع توضيح الإسهامات التي قدمتها هذه الدراسات في بناء الإطار النظري وصياغة متغيرات وأبعاد الدراسة الحالية



الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم
إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة



الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تمهيد

استكمالاً لما تم التطرق إليه في الفصل الأول من الجانب النظري، يأتي هذا الفصل ليعالج الجانب التطبيقي من خلال إجراء دراسة ميدانية على مستوى مجموعة من البنوك العمومية والخاصة والمختلطة، وذلك على مستوى ولاية ورقلة ، بهدف إبراز مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال. وقد تم الاعتماد على مجموعة من أدوات جمع البيانات، تمثلت في الاستبيان والمقابلة والملاحظة ووثائق الرسمية، حيث تم توزيع الاستبيان على عينة الدراسة، إلى جانب إجراء مقابلات مع مدير IT + مسؤول الامن المعلوماتي ، بالإضافة إلى الاعتماد على الملاحظة الميدانية، بما يساهم في الحصول على بيانات دقيقة وشاملة تعكس واقع البنوك محل الدراسة.

كما تم تقسيم هذا الفصل إلى مبحثين رئيسيين حيث يتناول المبحث الأول منهجية الدراسة، في حين يُخصص المبحث الثاني لعرض وتحليل ومناقشة النتائج.

المبحث الأول : الطريقة والأدوات المستخدمة في الدراسة الميدانية

يهدف هذا المبحث إلى توضيح المنهجية العلمية المعتمدة في الدراسات الميدانية التي تم تنفيذها بغرض تحقيق أهداف الدراسة والإجابة عن الإشكالية المطروحة، وذلك من خلال تحديد المنهج المتبع، وتوضيح أدوات جمع البيانات ، بالإضافة إلى عرض الأساليب الإحصائية التي تم اعتمادها لتحليل النتائج المتحصل عليها.

المطلب الأول : الطريقة المعتمدة في الدراسة

اعتمدت هذه الدراسة على مجموعة من المناهج والإجراءات العلمية التي تهدف إلى تحليل المعطيات المستخلصة وربطها بالفرضيات المطروحة، وذلك من خلال ما يلي:

أولاً : منهج الدراسة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تم الاعتماد على المنهج الوصفي التحليلي، لكونها الأنسب لطبيعة موضوع الدراسة وأهدافها. حيث يسمح المنهج الوصفي التحليلي بوصف واقع أمن نظام المعلومات في دعم إدارة استمرارية الاعمال داخل البنوك الجزائرية وتحليل مختلف أبعاده، بما يساهم في تفسير النتائج المتوصل إليها

ثانيا : أدوات جمع البيانات

اعتمدت الدراسة على مجموعة من الأدوات العلمية التي تم اختيارها بعناية، لما توفره من بيانات ومعلومات دقيقة تساعد في فهم موضوع الدراسة وتمثل فيما يلي:

I. الملاحظة

تم استخدام الملاحظة لرصد مختلف الممارسات المرتبطة بأمن نظام المعلومات داخل البنوك، وذلك بهدف تكوين صورة واقعية حول كيفية تطبيق إجراءات الأمن المعلوماتي ودورها في دعم استمرارية الاعمال.

II. الوثائق الرسمية

تم الاعتماد على مجموعة من الوثائق والتقارير الرسمية المتوفرة على مستوى البنوك ، لما تتضمنه من بيانات دقيقة تساهم في دعم التحليل وتفسير النتائج المتعلقة بأمن نظام المعلومات و إدارة استمرارية الأعمال.

III. المقابلة الشخصية

تم إجراء مقابلة شبه مهيكلة مع أحد مسؤول ذوي الخبرة في بنوك المدروسة ، بهدف توضيح بعض الجوانب المرتبطة بموضوع الدراسة، وتفسير النتائج المتحصل عليها، مما ساهم في إثراء التحليل ودعم مناقشة النتائج بشكل علمي دقيق.

IV. الاستبيان

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُعدّ الاستبيان الأداة الأساسية التي اعتمدنا عليها في جمع البيانات الميدانية استنادا على الدراسات السابقة ، حيث تم إعداده وفق منهجية علمية دقيقة شملت مجموعة من الأسئلة المغلقة والمفتوحة. وقد وُزِعَ على عينة مسؤولي الامن المعلومات لكل بنك بهدف التعرف على آرائهم وتقييماتهم حول مدى إدراكهم لأبعاد امن نظام المعلومات السائدة ودعمها في إدارة استمرارية الاعمال داخل البنوك محل الدراسة

V. متغيرات الدراسة

الجدول 02-01 : نموذج يوضح متغيرات الدراسة

المتغيرات	متغيرات الدراسة
المتغير المستقل	امن نظام المعلومات
المتغير التابع	إدارة استمرارية الاعمال

المصدر : من اعداد الطالبتين

ثالثا : لمحة عامة عن البنوك

1. التعريف بالبنوك المدروسة

❖ بنك التنمية المحلية BDL

يُعدّ بنك التنمية المحلية (BDL) من البنوك العمومية الجزائرية، حيث تأسس سنة 1985 في شكل شركة مساهمة، ويهدف إلى دعم وتمويل مختلف الأنشطة الاقتصادية، خاصة تلك المرتبطة بالمؤسسات الصغيرة والمتوسطة والجماعات المحلية. ويساهم البنك بدور مهم في تمويل مشاريع التنمية المحلية، من خلال تقديم مجموعة متنوعة من الخدمات البنكية التي تشمل القروض الاستثمارية، تمويل الاستغلال، وخدمات الدفع وإدارة الحسابات. ويعتمد بنك التنمية المحلية على استراتيجية تهدف

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة

من البنوك الجزائرية بورقلة

إلى مرافقة المتعاملين الاقتصاديين وتسهيل توجيههم إلى التمويل، بما يساهم في تحفيز الاستثمار ودعم التنمية الاقتصادية على المستوى الوطني، إضافة إلى سعيه لتحديث خدماته عبر إدماج التكنولوجيات الحديثة وتحسين جودة الأداء المصرفي و في إطار توسيع نشاطه وتعزيز تواجده الميداني، يمتلك البنك شبكة واسعة من الفروع عبر مختلف ولايات الوطن، من بينها فرع ولاية ورقلة محل الدراسة، والذي يُمثل امتداداً تنظيمياً للبنك على المستوى المحلي حيث يضطلع هذا الفرع بدور محوري في تقديم الخدمات البنكية لمختلف الاعوان الاقتصاديين في المنطقة، ومرافقة المشاريع الاستثمارية، خاصة في بيئة اقتصادية تتميز بتنوع الأنشطة التجارية والخدماتية. كما يسعى فرع ولاية ورقلة إلى تجسيد أهداف البنك من خلال تحسين جودة الخدمات، تسهيل الوصول إليها، وتبني أساليب تسيير حديثة، بما يساهم في دعم التنمية الاقتصادية المحلية وتعزيز دور البنك في تمويل الاقتصاد الوطني.

❖ بنك الفلاحة والتنمية الريفية BADR

يُعدّ بنك الفلاحة والتنمية الريفية مؤسسة مالية وطنية تأسست بتاريخ 13 مارس 1982 في شكل شركة مساهمة، ويُصنف ضمن أبرز البنوك العمومية في الجزائر، حيث يساهم بدور محوري في تمويل ومرافقة مختلف قطاعات النشاط الاقتصادي، لاسيما تلك المرتبطة بالمجال الفلاحي. ويُسهّم البنك في دعم الفلاحة وتربية المواشي، الصناعات الغذائية، إضافة إلى الصيد البحري وتربية المائيات، من خلال توفير صيغ تمويلية وخدمات بنكية تتماشى مع خصوصيات هذه القطاعات واحتياجاتها التنموية. كما يعمل البنك على تسهيل التوجه إلى الخدمات المالية عبر باقة متنوعة من المنتجات البنكية التي تهدف إلى مرافقة الزبائن في مختلف مراحل نشاطهم، بما يعزز من مساهمته في دعم التنمية الريفية والاقتصاد الوطني. وفي إطار توسيع نشاطه وتعزيز حضوره الميداني، يمتلك البنك شبكة واسعة من الفروع عبر مختلف ولايات الوطن، من بينها فرع الجهوي ولاية ورقلة ، والذي يُمثل امتداداً تنظيمياً للبنك على المستوى المحلي. حيث يساهم هذا الفرع الجهوي بدور هام في تجسيد مهام البنك، من خلال تقديم الخدمات البنكية للفلاحين، المستثمرين، ومختلف المتعاملين الاقتصاديين في المنطقة، مع التركيز على دعم الأنشطة الفلاحية والقطاعات المرتبطة بها.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

ويسعى فرع ولاية ورقلة إلى تحسين جودة خدماته وتقريبها من الزبائن، عبر اعتماد أساليب تسيير حديثة وتوفير حلول تمويلية ملائمة لخصوصيات المنطقة، بما يساهم في تحقيق التنمية الاقتصادية المحلية وتعزيز دور البنك في دعم الاقتصاد الوطني.

❖ بنك السلام

يُعدّ بنك السلام الجزائر مؤسسة مصرفية متعددة الخدمات، تنشط وفق الأطر التشريعية الجزائرية ، مع التزامها الكامل بتطبيق أحكام الشريعة الإسلامية في مختلف معاملاتها. وقد نال البنك اعتماد بنك الجزائر في سبتمبر 2008، لياشر نشاطه بتقديم خدمات مصرفية حديثة ومبتكرة تستجيب لمتطلبات مختلف الفاعلين الاقتصاديين. ويعتمد البنك على استراتيجية تنمية منسجمة مع توجهات الاقتصاد الوطني، من خلال طرح منتجات وخدمات بنكية عصرية تقوم على مبادئ الشفافية والمصادقية، مع خضوع معاملاته لرقابة هيئة شرعية متخصصة تضمن توافقها مع الضوابط الإسلامية. وفي إطار تعزيز انتشاره، عمل البنك على توسيع شبكته عبر مختلف ولايات الوطن، من بينها فرع ولاية ورقلة محل الدراسة، الذي يُمثل امتدادًا تنظيميًا للبنك على المستوى المحلي. حيث يؤدي هذا الفرع دورًا مهمًا في تقديم الخدمات المصرفية الإسلامية ومرافقة الأفراد والمؤسسات، خاصة في منطقة تتميز بأهمية اقتصادية مرتبطة بالأنشطة الطاقوية والتجارية. كما يسعى فرع ورقلة إلى تجسيد توجهات البنك من خلال تحسين جودة الخدمات، وتسهيل الوصول إليها، وتعزيز الثقة مع الزبائن، وذلك عبر اعتماد أنظمة عمل حديثة وتوفير منتجات مالية تتلاءم مع خصوصيات السوق المحلي، بما يساهم في دعم التنمية الاقتصادية على المستويين الجهوي والوطني.

❖ بنك الخليج AGB

يُعدّ بنك أفريقيا والخليج مؤسسة مصرفية تقدم خدمات مالية وبنكية متنوعة، تعتمد على حلول مبتكرة ومتطورة تكنولوجياً بهدف تلبية احتياجات مختلف الزبائن. ويرتكز نشاط البنك على مقاربة تتمحور حول الزبون، من خلال توفير خدمات مصرفية مصممة بما يتماشى مع احتياجاته الحالية والمستقبلية، سواء للأفراد أو المؤسسات، مع الحرص على تحسين جودة التجربة المصرفية وتعزيز العلاقة مع العملاء. كما يعتمد البنك على توظيف التقنيات الحديثة في تقديم خدماته، بما يساهم في تطوير الأداء المصرفي وتسهيل العمليات المالية، إضافة إلى دعمه لمختلف الأنشطة الاقتصادية والمساهمة في تعزيز النمو الاقتصادي وفتح آفاق أوسع للفرص

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استثمارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الاستثمارية والتنموية. وفي إطار انتشاره عبر مختلف مناطق الوطن، يتواجد البنك على مستوى ولاية ورقلة، حيث تم اعتماد فرع ورقلة كمحل للدراسة الميدانية. ويُعد هذا الفرع امتداداً تنظيمياً للبنك على المستوى المحلي، إذ يساهم بدور مهم في تقديم الخدمات البنكية لمختلف المتعاملين الاقتصاديين، ومرافقة الأنشطة التجارية والاستثمارية في المنطقة. ويسعى فرع ورقلة إلى تجسيد استراتيجية البنك من خلال تحسين جودة الخدمات المصرفية، تسهيل الوصول إليها، وتبني أنظمة عمل حديثة، بما يساهم في تلبية احتياجات الزبائن وتعزيز التنمية الاقتصادية على المستوى المحلي.

❖ بنك القرض الشعبي الجزائري CPA

يُعدّ بنك القرض الشعبي الجزائري من أبرز البنوك التجارية في الجزائر، حيث تأسس سنة 1966، ويتميّز بطابعه العمومي باعتبار أن رأسماله الاجتماعي مملوك في غالبيته للدولة، والذي يُقدّر حالياً بحوالي 200 مليار دينار جزائري. وقد استطاع البنك أن يرسّخ مكانته كفاعل اقتصادي محوري من خلال مرافقة العديد من المشاريع الكبرى، مما أكسبه سمعة متميزة على الصعيدين الوطني والدولي. ويعتمد البنك على تنوّع خدماته البنكية الموجهة لمختلف فئات الزبائن، بما في ذلك المؤسسات، والمهنيين، والأفراد، معتمداً في ذلك على خبرته الطويلة وموارده البشرية المؤهلة. كما يتميّز بانتشاره الجغرافي الواسع، من خلال شبكة تضم عدداً كبيراً من الوكالات عبر التراب الوطني، إضافة إلى شبائيك للصيرفة الإسلامية، مما يعكس سعيه لتقريب خدماته من مختلف المناطق. وفي إطار مواكبة التطورات التكنولوجية، يقدّم البنك مجموعة من الخدمات المصرفية الرقمية، مثل الخدمات البنكية عبر الهاتف النقال والإنترنت، إلى جانب مراكز اتصال تضمن استثمارية الخدمة وتحسين جودة الأداء. وفي هذا السياق، تُعد وكالة ورقلة إحدى الوكالات التابعة للبنك، حيث تمثل امتداداً محلياً لنشاطه، وتعمل على تقديم مختلف الخدمات البنكية لفائدة المتعاملين الاقتصاديين والأفراد في المنطقة. كما تساهم الوكالة في دعم النشاط الاقتصادي المحلي من خلال مرافقة المشاريع وتلبية احتياجات الزبائن، وفق السياسات والإجراءات المعتمدة من طرف البنك الأم، وبما يتماشى مع خصوصيات المنطقة الاقتصادية.

❖ بنك TRUST

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُعدّ بنك (TBA) بنكاً خاصاً خاضعاً للقانون الجزائري، تأسس بتاريخ 14 أبريل 2002 في شكل شركة مساهمة، وبدأ نشاطه الفعلي سنة 2003، برأس مال أولي قدره 750 مليون دينار جزائري. وقد عرف البنك تطوراً ملحوظاً في رأسماله عبر السنوات، ليواكب متطلبات التنظيم المصرفي في الجزائر، حيث بلغ مستويات معتبرة انسجاماً مع القوانين التي تحدد الحد

الأدنى لرأس مال البنوك والمؤسسات المالية. وينتمي البنك إلى مجموعة نيست للاستثمارات القابضة، وهي مجموعة دولية مقرها قبرص، تنشط في عدة قطاعات اقتصادية تشمل الخدمات المصرفية والمالية، التأمين وإعادة التأمين، العقار، الصناعة والسياحة، كما تمتد استثماراتها عبر عدد كبير من الدول. وقد عززت هذه المجموعة حضورها في الجزائر من خلال عدة شركات تابعة، ما يعكس توجهها نحو توسيع نشاطها في السوق الجزائرية. ويهدف بنك الثقة الجزائري إلى تقديم خدمات مصرفية متنوعة تلبي احتياجات الأفراد والمؤسسات، من خلال توفير منتجات مالية حديثة والمساهمة في تمويل مختلف الأنشطة الاقتصادية، بما يعزز دوره في دعم التنمية الاقتصادية. وفي إطار توسيع شبكته وتعزيز تواجده الميداني، يمتلك البنك مجموعة من الفروع عبر مختلف ولايات الوطن، من بينها فرع ولاية ورقلة الواقع في بلدية حاسي مسعود الذي هو محل الدراسة، والذي يُمثل امتداداً تنظيمياً للبنك على المستوى المحلي. حيث يضطلع هذا الفرع بدور مهم في تقديم الخدمات البنكية للمتعاملين الاقتصاديين، ومرافقة الأنشطة التجارية والاستثمارية في المنطقة. كما يسعى فرع حاسي مسعود ولاية ورقلة إلى تجسيد استراتيجية البنك من خلال تحسين جودة الخدمات البنكية، تسهيل الوصول إليها، وتبني أساليب تسيير حديثة، بما يساهم في دعم التنمية الاقتصادية المحلية وتعزيز مكانة البنك ضمن القطاع المصرفي الجزائري.

❖ بنك البركة

يُعدّ بنك البركة الجزائري أول بنك إسلامي في الجزائر، حيث تم إنشاؤه سنة 1991 برأسمال مختلط (عمومي وخاص)، وبدأ نشاطه الفعلي في شهر سبتمبر من نفس السنة. وقد أصبح مع مرور الوقت أحد أبرز الفاعلين في مجال الصيرفة الإسلامية داخل النظام المصرفي الجزائري، مستفيداً من انتمائه إلى مجموعة البركة المصرفية ذات الامتداد الدولي والخبرة الواسعة في مجال التمويل الإسلامي.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استثمارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

شهد البنك تطوراً ملحوظاً من حيث هيكله ورأسماله، إذ انطلق برأسمال أولي قُدِّر بـ 500 مليون دينار جزائري، ليصل حالياً إلى ما يقارب 20 مليار دينار جزائري، مع حصوله على الاعتماد الكامل لممارسة مختلف العمليات البنكية والتمويلية والاستثمارية وفق مبادئ الشريعة الإسلامية، وتحت إشراف هيئة رقابة شرعية متخصصة. ويقدم البنك مجموعة متنوعة من الخدمات المالية الموجهة للأفراد والمؤسسات والمهنيين، من خلال صيغ تمويل إسلامية معتمدة مثل المراجعة، الإجارة، السلم، الاستصناع، المشاركة والمضاربة، بما يساهم في دعم الاقتصاد الحقيقي وفق مقاربة تشاركية وأخلاقية. كما يساهم في دعم التجارة الخارجية عبر توفير أدوات بنكية كالإعتمادات المستندية، التحصيلات المستندية والضمانات البنكية. وفي إطار تقريب خدماته من الزبائن، يعتمد البنك على شبكة من الوكالات عبر مختلف ولايات الوطن، من بينها وكالة ورقلة، التي تُعد امتداداً محلياً لنشاط البنك. حيث تسهر هذه الوكالة على تقديم مختلف الخدمات البنكية والمالية لفائدة المتعاملين الاقتصاديين والأفراد في المنطقة، مع الالتزام بنفس المبادئ المعتمدة من طرف البنك الأم، خاصة ما يتعلق بتطبيق الصيرفة الإسلامية وتبني الحلول المالية المبتكرة التي تستجيب لمتطلبات البيئة الاقتصادية المحلية.

❖ بنك الخارجي الجزائري BEA

يُعدّ بنك الخارجية الجزائري (BEA) من أبرز البنوك العمومية في الجزائر، حيث تأسس سنة 1967، ويُصنف كأحد الركائز الأساسية للقطاع المصرفي الوطني، خاصة في مجال تمويل التجارة الخارجية. ويضطلع البنك بدور محوري في مرافقة المؤسسات الاقتصادية، لاسيما تلك الناشطة في مجالات الاستيراد والتصدير، من خلال تقديم مجموعة متكاملة من الخدمات البنكية التي تشمل تمويل العمليات التجارية الدولية، القروض، خدمات الصرف، وإدارة الحسابات. كما يسعى بنك الخارجية الجزائري إلى تطوير خدماته بما يتماشى مع متطلبات الاقتصاد الحديث، من خلال إدماج التكنولوجيات المصرفية المتطورة وتحسين جودة الأداء، بما يعزز مكانته في السوق البنكي ويساهم في دعم التنمية الاقتصادية الوطنية. وفي إطار توسيع شبكته وتعزيز حضوره الميداني، يمتلك البنك عدة فروع عبر مختلف ولايات الوطن، من بينها فرع حاسي مسعود ولاية ورقلة محل دراستنا، والذي يُمثل امتداداً

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تنظيماً للبنك على المستوى المحلي. حيث يضطلع هذا الفرع بدور مهم في تقديم الخدمات البنكية للمتعاملين الاقتصاديين، خاصة المؤسسات الناشطة في المجالات التجارية والصناعية، مع التركيز على مرافقة العمليات المرتبطة بالتجارة الخارجية. ويسعى فرع حاسي مسعود إلى تجسيد استراتيجية البنك من خلال تحسين جودة الخدمات البنكية، تسهيل الوصول إليها، واعتماد أساليب تسيير حديثة، بما يساهم في دعم النشاط الاقتصادي المحلي وتعزيز دور البنك في تمويل الاقتصاد الوطني.

❖ بنك الوطني الجزائري BNA

تأسس البنك الوطني الجزائري بموجب المرسوم رقم 821/66 بتاريخ 13 جوان 1966، ليخلف مجموعة من البنوك الأجنبية التي كانت تنشط في الجزائر، من بينها القرض الصناعي والتجاري (CIC)، وبنك باريس والدول الهولندية (BPPB)، إضافة إلى البنك الوطني من أجل الصناعة والتجارة في الجزائر (BNCIA) والقرض الجزائري التونسي (CFAT)، وهو ما جعله يشكل دعامة أساسية في بناء النظام المصرفي الوطني. ويتميز البنك بدوره الحيوي في تمويل مختلف القطاعات الاقتصادية، خاصة قطاعي الصناعة والتجارة، إلى جانب مساهمته في تمويل التجارة الخارجية ودعم الاستثمار، وذلك من خلال شبكة واسعة من الوكالات والمديريات الجهوية المنتشرة عبر مختلف ولايات الوطن. وفي هذا الإطار، تُعد وكالة حاسي مسعود إحدى الوكالات التابعة للبنك، حيث تمثل امتداداً محلياً لنشاطه، وتعمل على تجسيد أهدافه من خلال تقديم مختلف الخدمات البنكية لفائدة المتعاملين الاقتصاديين والأفراد في المنطقة. كما تساهم الوكالة في دعم النشاط الاقتصادي المحلي، خاصة في منطقة تُعد من أهم الأقطاب الاقتصادية، من خلال مرافقة المشاريع وتلبية احتياجات الزبائن وفق السياسات والإجراءات المعتمدة من طرف البنك الأم.

❖ بنك الجمعية العامة للجزائر Société générale

تُعدّ سوسيتيه جنرال الجزائر إحدى أبرز البنوك الخاصة الناشطة في الجزائر، وقد تأسست سنة 2000، وهي مملوكة بالكامل لمجموعة سوسيتيه جنرال العالمية. ومنذ إنشائها، عملت على تعزيز مكانتها ضمن القطاع المصرفي الجزائري من خلال

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تقديم خدمات مالية حديثة ومبتكرة تستجيب لمتطلبات مختلف فئات الزبائن. وتتميز سوسيتيه جنرال الجزائر بشبكة واسعة في توسع مستمر، تضم أكثر من 100 وكالة موزعة عبر العديد من ولايات الوطن، بالإضافة إلى مراكز أعمال مخصصة لخدمة المؤسسات والشركات. كما تقدم خدماتها لأكثر من 290,000 عميل من الأفراد والمهنيين والمؤسسات، بالاعتماد على موارد بشرية مؤهلة تتجاوز 1,700 موظف، مما يعكس حجم نشاطها ودورها في تمويل الاقتصاد الوطني. وفي إطار انتشارها الجغرافي، تتواجد سوسيتيه جنرال الجزائر على مستوى بلدية حاسي مسعود بولاية ورقلة، حيث تم اختيار هذا الفرع كمحلل للدراسة الميدانية. ويُعد هذا الفرع امتداداً تنظيمياً للبنك على المستوى المحلي، إذ يضطلع بدور مهم في تقديم مختلف الخدمات البنكية ومرافقة المتعاملين الاقتصاديين، خاصة في منطقة تتميز بنشاطها البترولي والحركية الاقتصادية المرتبطة به. ويسعى فرع حاسي مسعود إلى تجسيد استراتيجية البنك من خلال تحسين جودة الخدمات، تسهيل الوصول إليها، وتبني تقنيات مصرفية حديثة، بما يساهم في تلبية احتياجات الزبائن وتعزيز التنمية الاقتصادية على المستوى المحلي.

2. أنظمة الامن المعلوماتي

○ تقديم نظام المعلومات SAB المستخدم من طرف البنك التنمية المحلية BDL

يعتمد بنك التنمية المحلية على نظام SAB كمنصة معلوماتية متكاملة لتسيير العمليات البنكية والمالية داخل الفروع. لا يقتصر هذا النظام فقط على تسجيل العمليات، بل يقوم بمعالجتها وربطها مباشرة بالحسابات المركزية للبنك، مما يضمن دقة عالية في البيانات المالية. كما يُستخدم بشكل يومي في متابعة حركة الأموال داخل البنك، إعداد التقارير المالية، ومراقبة السيولة. إضافة إلى ذلك، يساعد النظام في تقليل التدخل اليدوي، حيث يتم أتمتة العديد من العمليات، مما يقلل من نسبة الأخطاء ويزيد من سرعة الإنجاز داخل الوكالات.

○ تقديم نظام المعلومات Oracle المستخدم من طرف البنك الفلاحة والتنمية الريفية BADR

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُعد نظام Oracle داخل بنك الفلاحة والتنمية الريفية قاعدة البيانات المركزية الأساسية التي تُخزن فيها جميع المعلومات البنكية. يقوم على حفظ بيانات الزبائن، القروض، الحسابات، والمعاملات المالية بطريقة منظمة وآمنة. كما يتميز هذا النظام بقدرته على معالجة عدد كبير من العمليات في نفس الوقت دون التأثير على الأداء، وهو ما يجعله مناسباً لبنك BADR الذي يتعامل مع عدد كبير من الزبائن والمشاريع الفلاحية. بالإضافة إلى ذلك، يُستخدم في استخراج التحليلات والتقارير التي تساعد البنك في اتخاذ قرارات استراتيجية دقيقة.

○ تقديم نظام المعلومات Temenos T24 المستخدم من طرف البنك السلام

يعد نظام Temenos T24 النظام البنكي المركزي المعتمد داخل بنك السلام الجزائر، ويُستخدم كمنصة موحدة لتسيير جميع العمليات البنكية اليومية بشكل لحظي ومترابط. يُعتبر هذا النظام أساسى البنك لأنه يربط بين مختلف الوظائف مثل فتح الحسابات، إدارة القروض، معالجة التحويلات، وتسجيل العمليات المالية بشكل فوري دون تأخير. داخل البنك، عندما يقوم الزبون بأي عملية (إيداع، سحب، طلب تمويل)، يتم إدخالها مباشرة في النظام ويتم تحديث الرصيد آلياً في نفس اللحظة. كما يسمح هذا النظام بربط جميع الفروع بقاعدة بيانات مركزية واحدة، مما يعني أن أي عملية تتم في فرع معين يمكن متابعتها أو استرجاعها من أي فرع آخر. بالإضافة إلى ذلك، يُستعمل في تسيير المنتجات الإسلامية مثل المراجعة والإجارة بطريقة مدمجة داخل النظام، مما يسهل احترام الضوابط الشرعية أثناء المعالجة.

○ تقديم نظام المعلومات Microsoft Dynamics CRM (TBM) المستخدم من طرف الخليج

AGB

يُستعمل نظام Microsoft Dynamics CRM داخل بنك أفريقيا والخليج كأداة متخصصة في إدارة علاقة البنك مع الزبائن. يسمح هذا النظام بجمع كل المعلومات المتعلقة بالزبون في ملف واحد، مثل نوع الحساب، تاريخ العمليات، الخدمات المستخدمة، وسلوك التعامل البنكي. هذا يساعد الموظفين على فهم احتياجات كل زبون بشكل دقيق، وبالتالي تقديم

عروض

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استثمارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

وخدمات مناسبة له مثل القروض أو البطاقات أو المنتجات الاستثمارية. كما يُستخدم النظام أيضًا في متابعة الشكاوى والتواصل مع الزبائن، مما يحسن جودة الخدمة ويعزز العلاقة بين البنك والعملاء.

○ تقديم نظام المعلومات Delta المستخدم من طرف بنك القرض الشعبي الجزائري CPA

يُعتبر نظام Delta داخل البنك القرض الشعبي الجزائري النظام الأساسي لتسيير العمليات البنكية اليومية في جميع الفروع. يتم من خلاله تنفيذ و معالجة مختلف العمليات مثل فتح الحسابات، التحويلات البنكية، عمليات الدفع، وتسديد القروض. كما يعمل النظام على توحيد البيانات بين مختلف الوكالات، مما يسمح بمتابعة حساب الزبون من أي فرع في الوطن. هذا يساهم في تحسين سرعة الخدمة وضمان دقة المعلومات، إضافة إلى تسهيل عمليات الرقابة المالية داخل البنك.

○ تقديم نظام المعلومات Banks المستخدم من طرف بنك TRUST

يُستخدم نظام Banks داخل بنك الثقة الجزائري كنظام معلوماتي لتسيير العمليات البنكية الداخلية بشكل شامل. عمليًا، يقوم هذا النظام بتسجيل كل العمليات المالية، متابعة الحسابات، وتوفير بيانات دقيقة حول الوضع المالي اليومي للبنك. كما يُستخدم في إعداد التقارير التحليلية التي تعتمد عليها الإدارة في تقييم الأداء واتخاذ القرارات. ويساعد النظام أيضًا في تحسين مراقبة السيولة وتنظيم العمليات داخل الفروع بطريقة أكثر دقة وفعالية.

○ تقديم نظام المعلومات Citrix المستخدم من طرف بنك البركة

يُستخدم نظام Citrix داخل بنك البركة الجزائري كمنصة للوصول الآمن إلى الأنظمة البنكية عن بعد. عمليًا، هذا النظام لا يعالج العمليات البنكية مباشرة، بل يسمح للموظفين بالدخول إلى الأنظمة الداخلية للبنك من أي جهاز بطريقة مؤمنة. هذا مهم جدًا في البنوك التي تعتمد على الصيرفة الإسلامية، لأن حماية البيانات والعمليات المالية تعتبر أولوية. كما يساعد النظام في تسهيل العمل بين الفروع وتمكين الموظفين من العمل عن بعد دون التأثير على أمن المعلومات أو جودة الخدمة.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

○ تقديم نظام المعلومات OGA المستخدم من طرف البنك الخارجي الجزائري BEA

يُستخدم نظام OGA داخل بنك الخارجية الجزائري كأداة لدعم التسيير الإداري والمالي وربط مختلف المصالح البنكية. عملياً، هذا النظام يعمل كحلقة وصل بين الأقسام المختلفة داخل البنك، مثل المحاسبة، العمليات البنكية، والمراقبة. فعند تنفيذ أي عملية مالية، يتم تمرير بياناتها عبر النظام بشكل منظم إلى مختلف المصالح المعنية، مما يسمح بمتابعة دقيقة لكل حركة مالية داخل البنك. كما يساعد هذا النظام الإدارة في الحصول على رؤية شاملة حول الوضع المالي، مما يسهل عملية اتخاذ القرار في الوقت المناسب.

○ تقديم نظام المعلومات Delta Version 8 المستخدم من طرف بنك الوطني الجزائري BNA

يُستخدم نظام Delta Version 8 داخل البنك الوطني الجزائري كنظام تشغيل أساسي للفروع، حيث يركز على معالجة العمليات اليومية التي تتم على مستوى الشباك. عملياً، هذا النظام هو الأداة التي يعتمد عليها الموظف في تسجيل العمليات المباشرة مثل فتح الحسابات، عمليات الإيداع والسحب، التحويلات الداخلية، وتسديد القروض. كما يقوم النظام بتحديث الحسابات بشكل آلي بعد كل عملية، مما يضمن دقة البيانات المالية وتفاذي الأخطاء اليدوية. ورغم أنه نظام تقليدي مقارنة بالأنظمة الحديثة، إلا أنه يتميز بالاستقرار العالي ويُعتبر مناسباً لتسيير العمليات الروتينية داخل البنك. غير أنه محدود من ناحية التكامل مع الخدمات الرقمية والتحليل المتقدم للبيانات.

○ تقديم نظام المعلومات Delta Version 11 المستخدم من طرف بنك سوستي جنرال

تستخدم سوسيتيه جنرال الجزائر نظام Delta Version 11 وهو إصدار متطور من نظام دلتا، تم تصميمه ليتماشى مع التحول الرقمي داخل البنوك. عملياً، هذا النظام يتيح معالجة أسرع للعمليات البنكية مقارنة بالإصدارات السابقة، مع دعم أكبر للخدمات الرقمية. كما يسمح بدمج العمليات البنكية التقليدية مع التطبيقات الإلكترونية والهاتف المحمول، بحيث يمكن للزبون متابعة حسابه وإجراء بعض العمليات عن بعد. داخل البنك، يُستخدم هذا النظام لتسريع معالجة المعاملات وتحسين جودة الخدمة داخل الفروع.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

رابعا : المجتمع وعينة الدراسة

1. المجتمع الدارسة

يتكون مجتمع الدراسة من البنوك الناشطة على مستوى ولاية ورقلة، نظراً لأهمية هذا القطاع في تبني نظم المعلومات وتطبيق ممارسات أمنها لضمان استمرارية الأعمال. وقد تم التركيز في هذه الدراسة على مسؤولي أمن نظام المعلومات داخل هذه البنوك، باعتبارهم الفاعل الرئيسي في وضع وتنفيذ سياسات الأمن المعلوماتي وضمان استمرارية الأنظمة.

2. العينة الدارسة

نظراً لطبيعة الدراسة، تم الاعتماد على أسلوب الحصر الشامل الجزئي الموجه ، حيث تم استهداف مسؤول واحد عن أمن نظام المعلومات في كل بنك. وقد شملت العينة:

6 بنوك على مستوى ولاية ورقلة 4 بنوك على مستوى حاسي مسعود

أي بمجموع 10 بنوك تمثل وحدات الدراسة.

تم توزيع 10 استبياناً ، وهو ما يعكس تمثيلاً مباشراً لكل بنك مشارك.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-02 :الاحصائيات الاستبيانات الموزعة والمسترجعة على العينة

	N	%
Observations Valide	10	100,0
Exclue ^a	0	,0
Total	10	100,0

المصدر : من اعداد الطالبتين بناء من مخرجات SPSS

تُظهر نتائج الجدول أن نسبة استرجاع الاستبيانات بلغت 100%، وهي نسبة مرتفعة جدًا تعكس تعاون أفراد العينة واهتمامهم بموضوع الدراسة. كما أن جميع الاستبيانات المسترجعة كانت صالحة للتحليل، مما يعزز من مصداقية النتائج ودقتها، ويُتيح الاعتماد عليها في التحليل الإحصائي واستخلاص الاستنتاجات.

فيما يلي تحليل وصفي لعينة الدراسة حسب المتغيرات التالية :

■ توزيع العينة حسب اسم البنك

الجدول 03-02 : توزيع العينة حسب اسم البنك

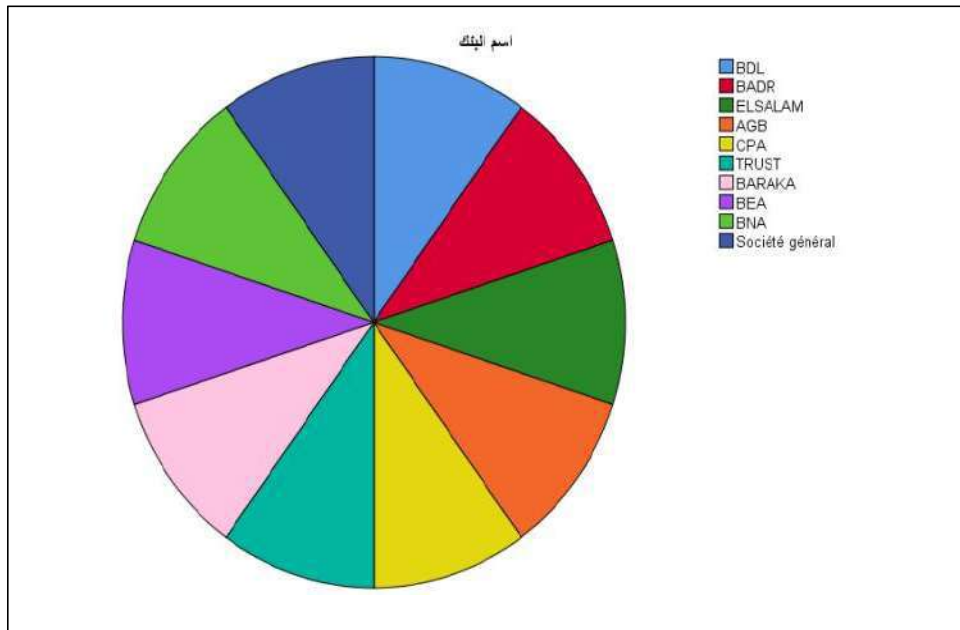
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide BDL	1	10,0	10,0	10,0
BADR	1	10,0	10,0	20,0
ELSALAM	1	10,0	10,0	30,0
AGB	1	10,0	10,0	40,0
CPA	1	10,0	10,0	50,0

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

TRUST	1	10,0	10,0	60,0
BARAKA	1	10,0	10,0	70,0
BEA	1	10,0	10,0	80,0
BNA	1	10,0	10,0	90,0
Société général	1	10,0	10,0	100,0
Total	10	100,0	100,0	

المصدر : من عداد طالبين بناء على مخرجات SPSS

الشكل 01-02 : توزيع العينة حسب اسم البنك



المصدر : من اعداد الطالبين بناء على مخرجات SPSS

يُبيّن الجدول توزيع أفراد العينة وفق البنوك ولاية ورقلة ، حيث تمّ تسجيل عشر (10) استجابات موزعة بالتساوي على

عشرة بنوك مختلفة ، بحيث سجّل كل بنك تكرارًا قدره (1) بنسبة (10%) من إجمالي العينة. وتُظهر نتائج الجدول أن نسب

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

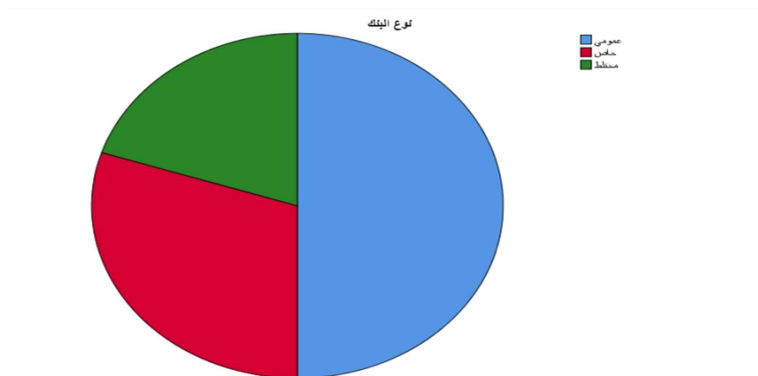
التوزيع والنسب الصحيحة متطابقة، مما يدل على عدم وجود بيانات مفقودة، وهو ما يعزز من دقة التحليل الإحصائي، حيث يبين التراكم النسبي تدرجاً منتظماً إلى غاية 100%، نتيجة التوزيع المتوازن ويتأكد ذلك من خلال الشكل البياني الذي يعكس هذا التوزيع المتساوي، حيث تظهر جميع القطاعات بنفس الحجم، وهو ما يعزز مصداقية النتائج ويؤكد التمثيل المتوازن لمختلف البنوك ضمن العينة.

الجدول 02-04 : توزيع العينة حسب نوع البنك

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	عمومي	5	50,0	50,0	50,0
	خاص	3	30,0	30,0	80,0
	مختلط	2	20,0	20,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على المخرجات SPSS

الشكل 02-02 : توزيع العينة حسب نوع البنك



المصدر : من اعداد الطالبتين بناء على المخرجات

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُبين الجدول أعلاه توزيع أفراد العينة حسب نوع البنك، حيث تم تسجيل عشر (10) استجابات موزعة بين ثلاثة أنواع من البنوك، إذ تمثل البنوك العمومية النسبة الأكبر بـ (50%) أي ما يعادل (5) استجابات، تليها البنوك الخاصة بنسبة (30%) بـ (3) استجابات، في حين تمثل البنوك المختلطة نسبة (20%) بـ (2) استجابتين. وتُظهر النتائج تطابق النسب المئوية مع النسب الصحيحة، مما يدل على عدم وجود بيانات مفقودة، وهو ما يعزز من موثوقية التحليل الإحصائي، كما يبين التراكم النسبي تدرجًا منطقيًا إلى غاية 100%. ويتأكد ذلك من خلال الشكل البياني الذي يعكس هذا التوزيع، حيث تستحوذ البنوك العمومية على الحصة الأكبر من العينة، تليها البنوك الخاصة ثم المختلطة، وهو ما يعكس تمثيلًا نسبيًا لمختلف أنواع البنوك. ومن خلال هذه النتائج، يمكن القول إن العينة تركز بشكل أكبر نحو البنوك العمومية، وهو ما قد يعكس واقع القطاع البنكي في ولاية ورقلة.

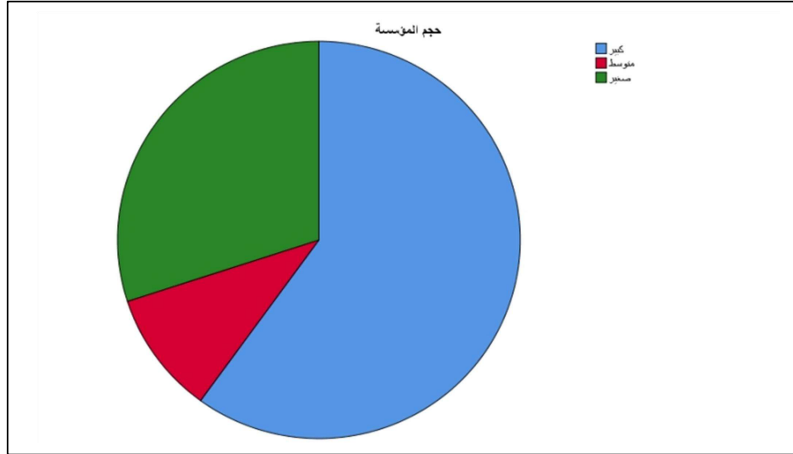
الجدول 02-05 : توزيع العينة حسب حجم البنك

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
كبير Valide	6	60,0	60,0	60,0
متوسط	1	10,0	10,0	70,0
صغير	3	30,0	30,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

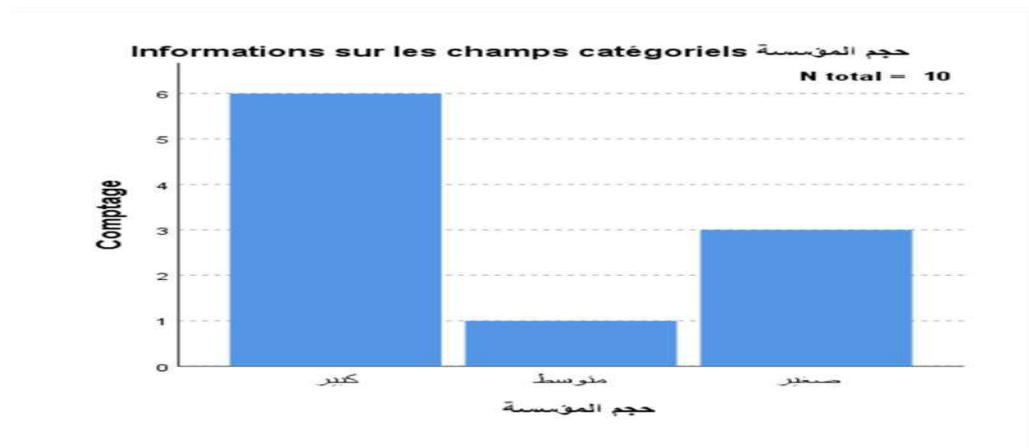
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-03 : توزيع العينة حسب حجم البنك



المصدر : من اعداد الطالبتين بناء على مخرجات SPS S

الشكل 02-04 : توزيع العينة حسب الحجم البنك



المصدر : من اعدا الطالبتين بناء على مخرجات SPSS

يبين جدول توزيع العينة حسب حجم البنك، والموضح بالشكل البياني ، أن العينة المدروسة (N=10) تتسم بهيمنة واضحة للبنوك كبيرة الحجم، حيث سجلت هذه الفئة تكرارًا قدره (6) بنسبة (60%)، تليها البنوك صغيرة الحجم بتكرار (3) ونسبة (30%)، في حين جاءت البنوك متوسطة الحجم في المرتبة الأخيرة بتكرار (1) فقط بنسبة (10%). ويتجلى

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

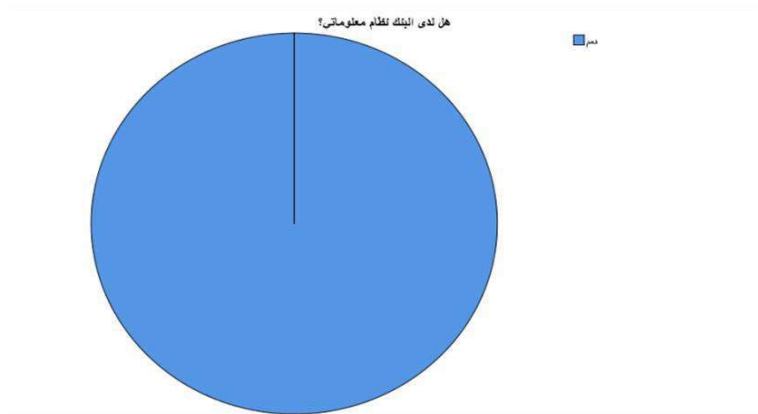
هذا التوزيع بوضوح في الشكل البياني الذي أظهر تفوق فئة البنوك الكبيرة مقارنة بباقي الفئات، كما يؤكد الشكل الذي خصص أكبر قطاع لهذه الفئة، مقابل قطاع متوسط للبنوك الصغيرة وآخر ضيق جداً للبنوك المتوسطة. ويعكس هذا التوافق بين العرض الجدولي والتمثيلين البياني والهندسي دقة المعالجة الإحصائية وموثوقية النتائج. ومن الناحية التفسيرية، يمكن إرجاع هذه الهيمنة إلى طبيعة القطاع البنكي الذي تغلب عليه المؤسسات كبيرة الحجم، نظراً لما تتطلبه أنشطته من موارد مالية وتقنية وتنظيمية معتبرة، خاصة في ما يتعلق بالاعتماد المكثف على نظم المعلومات. ، إذ إن المؤسسات الكبيرة غالباً ما تكون أكثر تبنياً لممارسات أمن نظام المعلومات وأكثر وعياً بضرورة تطبيق استراتيجيات فعالة لإدارة استمرارية الأعمال،

الجدول 02-06 توزيع العينة حسب توفر النظام المعلوماتي

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valides نعم	10	100,0	100,0	100,0

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-05 : توزيع العينة حسب توفر النظام المعلوماتي



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

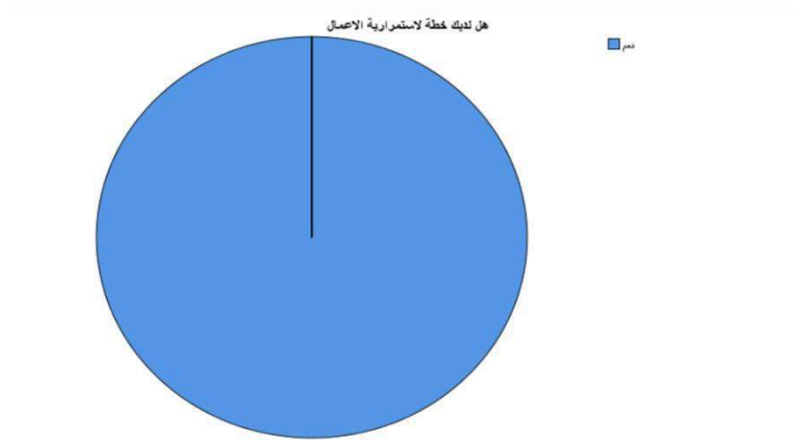
يبيّن جدول توزيع العينة حسب توفر النظام المعلوماتي، والمدعم بالشكل ، أن جميع مفردات العينة (N=10) قد أكدوا توفر نظام معلومات داخل البنوك ولاية ورقلة ، حيث سجلت فئة "نعم" تكرارًا قدره (10) بنسبة (100%)، وهي نفس القيمة في النسبة المئوية الصحيحة والتراكمية. ويظهر هذا بوضوح في الشكل التي تعكس تجانسًا تامًا في إجابات أفراد العينة دون وجود أي تباين. و هذه المعطيات تبين دقة النتائج ووضوحها. ومن الناحية التفسيرية، يعكس هذا المؤشر الاعتماد الكلي للبنوك على نظم المعلومات في مختلف أنشطتها، وهو أمر يتماشى مع طبيعة العمل المصرفي القائم على معالجة البيانات وإدارة العمليات إلكترونياً. كما يشكل هذا المعطى قاعدة أساسية ومنطلقًا ضروريًا لتحليل باقي متغيرات الدراسة، خاصة ما يتعلق بأمن نظام المعلومات وإدارة استمرارية الأعمال

الجدول 02-07: توزيع العينة حسب وجود خطة استمرارية الاعمال

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valides نعم	10	100,0	100,0	100,0

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-06 : توزيع العينة حسب وجود خطة استمرارية الاعمال



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يبين جدول توزيع العينة حسب وجود خطة استمرارية الأعمال، أن جميع مفردات العينة ($N=10$) قد أكدوا وجود خطة لاستمرارية الأعمال داخل البنوك محل الدراسة، حيث سجلت فئة "نعم" تكراراً قدره (10) بنسبة (100%)، وهي نفس القيمة المسجلة في النسبة المئوية الصحيحة والتراكمية. ويترجم هذا المعطيات في الشكل البياني التي تعكس إجماعاً مطلقاً بين أفراد العينة دون أي تباين في الإجابات. ويؤكد هذا التوافق بين الجدول والشكل الدائري دقة ووضوح النتائج المتحصل عليها. و نفس هذا بان المؤشر على وعي مرتفع لدى البنوك بأهمية تبني خطط استمرارية الأعمال، خاصة في ظل التحديات والمخاطر التي قد تهدد سير النشاط المصرفي، سواء كانت تقنية أو تنظيمية. كما يعكس التزام هذه المؤسسات بتطبيق ممارسات إدارية حديثة تتماشى مع المعايير الدولية في هذا المجال، مثل معيار ISO 22301، الأمر الذي يعزز جاهزيتها لمواجهة الأزمات وضمان استمرارية خدماتها..

المطلب الثاني : تقديم أداة الدراسة

يُقصد بالصدق في الدراسات العلمية مدى قدرة أداة الدراسة على قياس الظاهرة المستهدفة بدقة دون الانحراف إلى قياس جوانب أخرى. ولتحقيق ذلك، تم التأكد من صدق محتوى الاستبانة من خلال عرضها أولاً على الأستاذ المشرف للاستفادة من ملاحظاته وتوجيهاته، ثم إخضاعها للتحكيم العلمي من طرف خمسة مختصين في المجال (الملحق رقم 01)، حيث قِيموا فقراتها من حيث الوضوح والملاءمة وقدرتها على قياس أبعاد الدراسة. وبناءً على آرائهم، أُجريت التعديلات اللازمة من حذف وإضافة وتعديل، إلى أن تم التوصل إلى الصيغة النهائية الجاهزة للتوزيع. ونظراً لطبيعة متغيرات الدراسة، والمتمثلة في أمن نظام المعلومات وإدارة استمرارية الأعمال كمتغيرات وصفية، فقد تم الاعتماد على الاستبانة كأداة ملائمة لقياس العلاقة بينهما وفق صياغة علمية دقيقة تخدم أهداف البحث

• الاستبيان

تُعدّ الاستبانة أداة أساسية لجمع البيانات في هذه الدراسة، حيث تم الاعتماد عليها لقياس مستوى أمن نظم المعلومات في البنوك محل الدراسة من جهة، وتقييم مستوى إدارة استمرارية الأعمال من جهة أخرى. كما ساهمت في قياس مختلف الأبعاد بمتغيرات

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الدراسة، من خلال استقصاء آراء أفراد العينة حول واقع تطبيق ممارسات الأمن المعلوماتي ودورها في دعم استمرارية النشاط البنكي، وذلك كما هو موضح في الملحق رقم (...).

اولا: المعلومات العامة

نستعرض فيما يلي أهم الأبعاد التي يمكن من خلالها قياس مستوى أمن نظم المعلومات داخل البنوك محل الدراسة، من خلال مجموعة من المؤشرات.

✓ سرية المعلومات

- سياسة امن المعلومات

- التحكم في الوصول

- المصادقة

- سياسة كلمات المرور

- التشفير

- النوعية الأمنية

✓ سلامة المعلومات

- سجلات التدقيق

- التحقق من صحة البيانات

- كشف التلاعب

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

-تقسيم الصلاحيات

-امن القواعد البيانات

-أنظمة التنبيه الأمني

✓ توافر المعلومات

-استمرارية الخدمة

-النسخ الاحتياطي

-استرجاع البيانات

-مراقبة الأنظمة

-بنية تحتية بديلة

-إدارة الصيانة

❖ تم قياس إدارة استمرارية الأعمال كمتغير مركب من خلال مجموعة من المؤشرات العامة التي تعكس قدرة البنوك على

ضمان استمرار نشاطها واستقرار عملياتها في مختلف الظروف:

-خطة استمرارية الاعمال BCP

-مراجعة الخطة

-خطة التعافي DRP

-فريق إدارة الازمات

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

-زمن الاستجابة

-إجراءات الطوارئ

-سجل المخاطر

-تقييم المخاطر

-زمن استرجاع RTO

-معيار إدارة استمرارية الاعمال ISO 22301

ثانيا : مقاييس الدراسة

1. مقياس تقدير الخماسي : تم الاعتماد في قياس متغيرات الدراسة داخل البنوك محل الدراسة على مقياس تقديري خماسي لدرجة التطبيق، وذلك كما يلي:

الجدول 02-08 : توزيع درجات التطبيق لسلم تقدير الخماسي

تطبيق فعال	جيد التطبيق	متوسط التطبيق	ضعيف التطبيق	غير موجود	بدائل الإجابة
5	4	3	2	1	الدرجة التطبيق

المصدر : من اعداد الطالبتين

2. الأسئلة الاستثنائية :

تم تضمين الاستبيان بعض الأسئلة الثنائية (نعم/لا) لقياس توفر بعض الأنظمة أو الممارسات داخل البنوك، حيث تم

ترميزها كما يلي:

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

نعم تعطى لها 1.

لا تعطى لها 0.

3. المتغيرات الاسمية :

اشتمل الاستبيان على مجموعة من المتغيرات الاسمية المتعلقة بخصائص البنوك، مثل نوع البنك وحجمه، حيث تم ترميز هذه المتغيرات إلى قيم رقمية وفقاً لفتاها، وذلك لتسهيل استخدامها في التحليل الإحصائي والمقارنات بين أفراد العينة.

الجدول 02-09 : يوضح ترميز خصائص (البنك نوع البنك)

نوع البنك	عمومي	خاص	مختلط
ID	1	2	3

المصدر : من اعداد الطالبتين

الجدول 02-10: يوضح ترميز خصائص البنك (حجم البنك)

حجم البنك	كبير	متوسط	صغير
ID	1	2	3

المصدر : من اعداد الطالبتين

4. معامل الثبات (Cronbach's Alpha): من أجل التأكد من ثبات أداة الدراسة ومدى اتساقها الداخلي، تم

الاعتماد على معامل Cronbach's Alpha، والذي يُستخدم لقياس درجة ثبات إجابات أفراد العينة على فقرات

الاستبيان المتعلقة بمتغيرات الدراسة. وقد شمل هذا التحليل مجموعة من الأسئلة السلمية المقدرة بـ 28 سؤالاً، حيث يبين

هذا المعامل مدى تجانس الإجابات، أي إلى أي حد يمكن أن يعطي أفراد العينة نفس الإجابات في حال إعادة تطبيق

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الاستبيان تحت نفس الظروف وسيتم عرض نتائج تقدير معامل الثبات في الجدول الموالي، والذي يوضح درجة ثبات أداة

الدراسة لمختلف أبعاد أمن نظام المعلومات وعلاقتها بدعم إدارة استمرارية الأعمال

الجدول 02-11: تقدير معامل الثبات

Alpha de Cronbach	Nombre d'éléments
,685	28

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يبين الجدول نتائج تقدير معامل الثبات Cronbach's Alpha الخاص بأداة الدراسة، حيث بلغ معامل الثبات (0.685) اعتمادًا على إجابات أفراد العينة على 28 فقرة تمثل متغيرات الدراسة المتعلقة بأمن نظام المعلومات ودوره في دعم إدارة استمرارية الأعمال. وتشير هذه القيمة إلى أن مستوى الثبات مقبول، حيث تعكس درجة مقبولة من تناسق بين فقرات الاستبيان، مما يدل على أن الأداة تقيس نفس المفهوم بدرجة جيدة. وعليه، يمكن اعتبار أداة الدراسة ذات موثوقية مقبولة تسمح بالاعتماد على نتائجها في تحليل العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال

المطلب الثالث: أدوات الإحصائية المستخدمة

تم تحليل بيانات الاستبيان باستخدام برنامج SPSS من خلال تطبيق مجموعة من الاختبارات الإحصائية المناسبة لطبيعة الدراسة، وسيتم توضيحها لاحقًا

✓ المتوسط الحسابي والانحراف المعياري:

تم الاعتماد على المتوسط الحسابي والانحراف المعياري لتحديد الأهمية النسبية لاستجابات أفراد عينة الدراسة تجاه محاور وأبعاد الدراسة، وذلك من أجل تفسير اتجاهات العينة ودرجة موافقتها على العبارات محل القياس.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

✓ الجداول التكرارية والنسب المئوية:

تم استخدام الجداول التكرارية والنسب المئوية لوصف الخصائص الشخصية والوظيفية لأفراد العينة، بهدف تقديم صورة إحصائية واضحة حول توزيع خصائص المشاركين في الدراسة.

✓ اختبار الثبات (كرونباخ ألفا):

تم استخدام معامل كرونباخ ألفا لقياس مدى ثبات أداة الدراسة (الاستبيان)، والتأكد من اتساق فقراته وصلاحيته لجمع ال معاملا الارتباط (Pearson):

✓ معاملا الارتباط (Pearson):

تم استخدام معاملا ارتباط بيرسون لقياس قوة واتجاه العلاقة بين متغيري الدراسة (أمن نظم المعلومات وإدارة استمرارية الأعمال)، وذلك لتحديد مدى وجود علاقة ارتباطية بينهما

✓ القيم الاحتمالية (Sig):

تم استخدام القيم الاحتمالية (Sig) لتحديد مدى الدلالة الإحصائية للنتائج، حيث تم اعتماد مستوى الدلالة ($\alpha \leq 0.05$)، وتُعد القيم ($\text{Sig} \leq 0.05$) دالة إحصائيًا ومعنوية، مما يشير إلى وجود تأثير أو علاقة ذات دلالة إحصائية بين متغيرات الدراسة.

✓ اختبار كولموغوروف-سميرنوف (Kolmogorov-Smirnov):

كما تم استخدام اختبار كولموغوروف-سميرنوف (Kolmogorov-Smirnov) للتحقق من مدى اتباع بيانات الدراسة للتوزيع الطبيعي، وذلك لتحديد ملاءمة استخدام الاختبارات الإحصائية المعلمية في تحليل بيانات الدراسة.

✓ تحليل الفروق وفق خصائص المؤسسات محل الدراسة:

تم استخدام مجموعة من الاختبارات الإحصائية لدراسة الفروق بين إجابات أفراد العينة حسب الخصائص البنوك . حيث تم الاعتماد على اختبار (T-Test) لعينتين مستقلتين لقياس الفروق حسب نوع البنوك، كما تم استخدام تحليل التباين الأحادي (ANOVA) لدراسة الفروق حسب حجم المؤسسة. ونظرًا لاحتمال عدم تحقق شرط التوزيع الطبيعي، تم اللجوء أيضًا إلى

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

اختبار Kruskal-Wallis لقياس الفروق بين أكثر من مجموعتين مستقلتين. وقد تم اعتماد مستوى الدلالة الإحصائية $(\alpha \leq 0.05)$ لتحديد معنوية الفروق.

المبحث الثاني : عرض ومناقشة النتائج

فيما يلي سيتم الاستفادة من الأساليب الكمية التي توفرها كل من نظرية الإحصاء الوصفي ونظرية الاستدلال الإحصائي، وذلك للإجابة على الإشكالية الرئيسية والتساؤلات الفرعية لهذا البحث، بالاعتماد على الاستبيان الموزع على عينة من البنوك محل الدراسة (10 بنوك عبر 10 وكالات بولاية ورقلة). ويهدف ذلك إلى تقييم مستوى تطبيق أمن نظم المعلومات داخل هذه البنوك، ومدى مساهمته في ضمان إدارة استمرارية الأعمال، وذلك بالاعتماد على آراء المسؤولين والعاملين في هذه المؤسسات البنكية.

المطلب الأول : عرض وتحليل نتائج محاور الدراسة

تمهيد

تم في هذا المطلب عرض وتحليل نتائج محاور الدراسة المتعلقة بمتغيري البحث، والمتمثلين في أمن نظام المعلومات كمتغير مستقل، وإدارة استمرارية الأعمال كمتغير تابع. وذلك من خلال تحليل البيانات الميدانية المتحصل عليها من أفراد عينة الدراسة باستخدام برنامج SPSS، بهدف التعرف على مستوى تطبيق أبعاد أمن نظام المعلومات داخل البنوك محل الدراسة، ومدى مساهمتها في دعم إدارة استمرارية الأعمال .

أولا : المتغير امن نظام المعلومات

يهدف هذا المحور إلى تقييم مستوى وواقع أمن نظم المعلومات داخل البنوك محل الدراسة، من خلال التطرق إلى نتائج الدراسة التي شملت أبعاد أمن نظام المعلومات، والمتمثلة في: سرية المعلومات، وسلامتها، وتوافرها، وذلك من أجل تحديد مدى تطبيق هذه الأبعاد ومدى فعاليتها في حماية المعلومات وضمان استمرارية النشاط البنكي.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

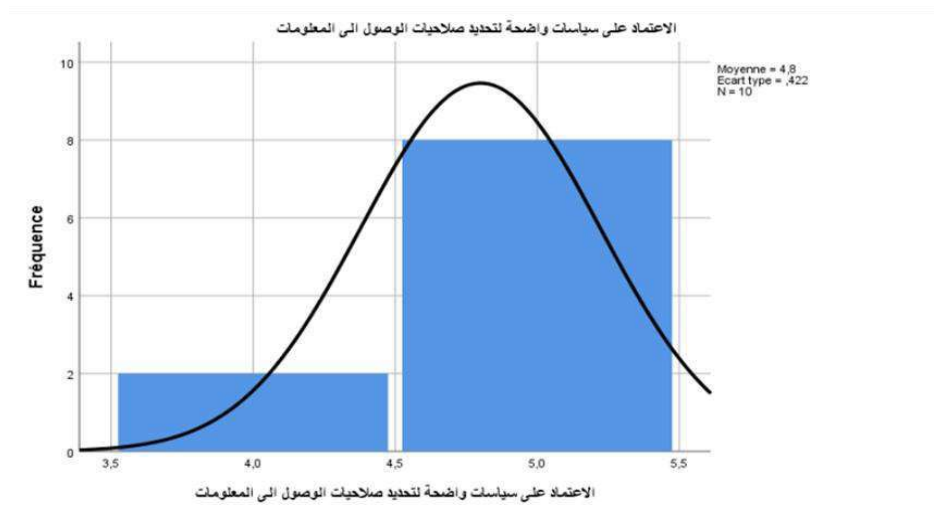
✓ سرية المعلومات

الجدول 02-12 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سياسة امن المعلومات

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valides جيد التطبيق	2	20,0	20,0	20,0
تطبيق فعال	8	80,0	80,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-07 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سياسة امن المعلومات



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تشير نتائج الجدول إلى أن غالبية أفراد العينة المتمثلة في (80%) يعتمدون على سياسة أمن المعلومات داخل ولاية ورقلة بدرجة تطبيق فعال ، مقابل نسبة (20%) فقط يرون أنه في بدرجة جيد التطبيق، وهو ما يعكس توجهاً عاماً نحو تبني سياسات أمن معلومات واضحة ومطبقة بشكل فعال. وتدلل هذه النتائج على وجود إدراك البنوك لأهمية تنظيم الوصول إلى المعلومات وضبطها وفق سياسات واضحة ، بما يعزز أحد الأبعاد الأساسية لأمن نظام المعلومات والمتمثل في سرية المعلومات. ويتأكد هذا التوجه من خلال الشكل البياني المرفق، حيث يظهر تركز القيم في الفئات العليا (بين 4.5 و 5 تقريباً) ما يعكس تجانس إجابات العينة واتفاقها حول فعالية تطبيق سياسة أمن المعلومات. بناءً على ذلك، يمكن استنتاج أن البنوك المدروسة تعتمد بدرجة عالية على سياسات أمن المعلومات، وهو ما يدعم تحقيق مستوى مرتفع من سرية المعلومات كأحد مكونات أمن النظام المعلوماتي حيث تتوافق هذه النتيجة بشكل مباشر مع دراسة بن الطيب إبراهيم (2018) التي أكدت أن تبني سياسات أمن معلومات متكاملة يساهم في تقليل المخاطر وتعزيز استقرار الأنظمة، إضافة إلى دورها في حماية الأصول المعلوماتية للمؤسسة. كما تتطابق مع نتائج دراسة Isabel Maria Lopes & Pedro Oliveira (2016)، والتي بينت أن تطبيق سياسات أمن نظم المعلومات يساهم في تحسين حماية الأنظمة المعلوماتية ورفع فعاليتها، وهو ما ينسجم مع ارتفاع نسبة التطبيق الفعال في هذه الدراسة.

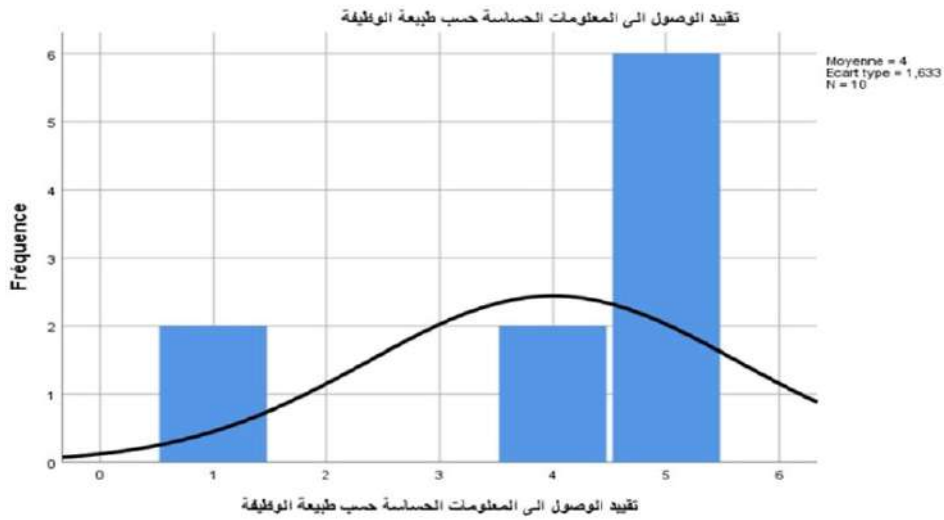
الجدول 02-13: توزيع إجابات أفراد العينة حول مدى الاعتماد على التحكم في الوصول

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide				
غير موجود	2	20,0	20,0	20,0
التطبيق جيد	2	20,0	20,0	40,0
تطبيق فعال	6	60,0	60,0	100,0
Total	10	100,0	100,0	

المصدر: من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-08 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التحكم في الوصول



المصدر: من اعداد الطالبتين بناء مخرجات SPSS

يُظهر الجدول الخاص بمدى الاعتماد على التحكم في الوصول ، أن غالبية أفراد العينة (60%) أكدوا وجود تطبيق فعال، مقابل 20% يرونه جيد التطبيق و20% اخرون يصّرّحون بعدم وجوده. ويتأكد هذا الاتجاه من خلال الشكل البياني الذي يُبرز تركّز القيم في المستويات العليا (4 و5) ويمكن تفسير هذه النتائج باعتماد البنك على سياسات واضحة لتنظيم صلاحيات المستخدمين وتقييد الوصول إلى المعلومات حسب طبيعة الوظائف وهو ما يساهم في الحد من الدخول غير المصرح به وحماية البيانات الحساسة. ورغم تسجيل نسبة محدودة تشير إلى غياب التطبيق ، إلا أنها تبقى ضعيفة ولا تؤثر على الاتجاه العام. تتوافق هذه النتائج مع دراسة كمال مسوس (2022) التي أكدت أن تطبيق ممارسات حوكمة أمن نظم المعلومات، خاصة ما يتعلق بالتحكم في الوصول، يساهم في الحد من الاعتداءات الإلكترونية وتقليل المخاطر السيبرانية. كما تنسجم مع دراسة حلّيمي نبيل، حفصي رشيد، وبن عياد محمد سمير (2022) التي أبرزت أن تقييد الوصول إلى المعلومات يساهم في حماية البيانات وتقليل مخاطر الاختراق والتلاعب، وهو ما يدعم النتائج المحصل عليها ميدانيًا.

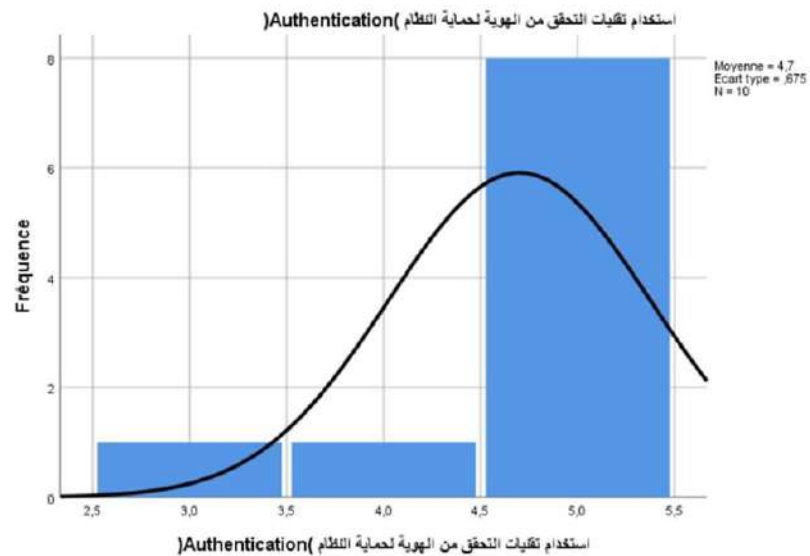
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-14 : توزيع إجابات أفراد العينة حول مدى الاعتماد على المصادقة

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
متوسط التطبيق	1	10,0	10,0	10,0
التطبيق جيد	1	10,0	10,0	20,0
تطبيق فعال	8	80,0	80,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-09 : توزيع إجابات أفراد العينة حول مدى الاعتماد على المصادقة



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُبين الجدول المتعلق بمدى الاعتماد على تقنيات المصادقة أن نسبة 80% من أفراد العينة يؤكدون وجود تطبيق فعال، مقابل 10% يرونه جيد التطبيق و10% اخرون يعتبرونه في مستوى متوسط، وهو ما يعكس توجهاً واضحاً نحو الارتفاع في استخدام آليات التحقق من الهوية داخل البنوك على مستوى ولاية ورقلة. ويؤكد الشكل البياني المرفق ، حيث يظهر تركز الإجابات في المستويات المرتفعة مع تفوق واضح لفئة التطبيق الفعال .ويمكن تفسير على ان المؤسسات البنكية تحرص على تعزيز إجراءات التحقق من هوية المستخدمين من خلال اعتماد تقنيات متعددة للمصادق وهو الأمر الذي يساهم في حماية الأنظمة المعلوماتية والحد من مخاطر الدخول غير المصرح به. بحيث تتوافق هذه النتائج مع دراسة Semlambo et al (2021) التي أكدت أن سياسات أمن المعلومات والعوامل التنظيمية، من بينها آليات التحقق من الهوية، تلعب دوراً أساسياً في تقليل المخاطر الأمنية. كما تنسجم مع دراسة حللمي نبيل وآخرون (2022) التي شددت على أن تعزيز إجراءات الحماية، بما فيها التحقق من الهوية، يساهم في ضمان سرية المعلومات وتقليل الاختراقات، وهو ما يفسر ارتفاع مستوى التطبيق في نتائج هذه الدراسة.

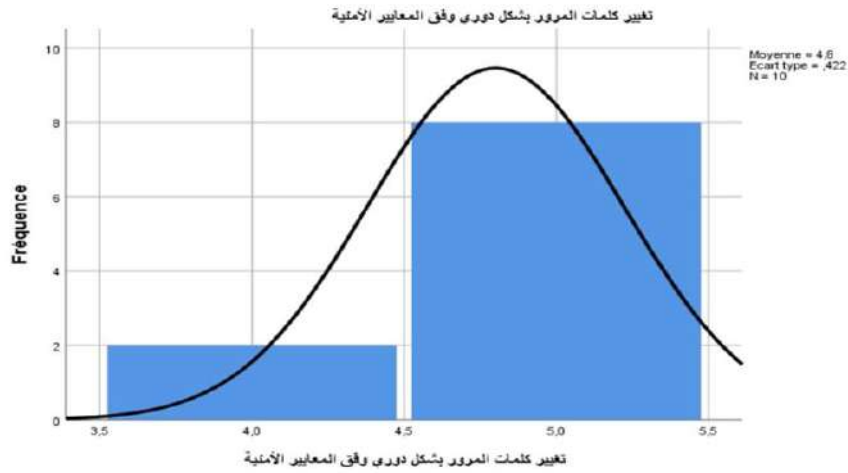
الجدول 02-15 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سياسة كلمات المرور

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valides جيد التطبيق	2	20,0	20,0	20,0
تطبيق فعال	8	80,0	80,0	100,0
Total	10	100,0	100,0	

المصدر :من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-10 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سياسة كلمات المرور



المصدر: من اعداد الطالبتين بناء مخرجات SPSS

يبين الجدول المتعلق بتطبيق كلمات المرور ضمن أمن نظام المعلومات أن معظم أفراد العينة يؤكدون وجود تطبيق فعال بنسبة 80%، مقابل 20% فقط يرون أنه جيد التطبيق، وهو ما يعكس مستوى مرتفعاً من الالتزام بإجراءات حماية كلمات المرور داخل البنوك المدروسة. كما يدعم الشكل البياني هذه النتيجة، حيث يُظهر فارق واضح للفئة التطبيق الفعال مقارنة بباقي الفئات. ويمكن تفسير ذلك بسبب اهتمام المؤسسة بتعزيز سياسات التحكم في الوصول وحماية البيانات من خلال اعتمادها ممارسات قوية لكلمات المرور. وبناءً على ذلك، تتوافق هذه النتائج مع دراسة Adam A. Semlambo وآخرون (2021) التي أكدت أن سياسات أمن المعلومات، خاصة ما يتعلق بإدارة الوصول وكلمات المرور، تمثل أحد العوامل الأساسية المؤثرة في تعزيز أمن نظم المعلومات.

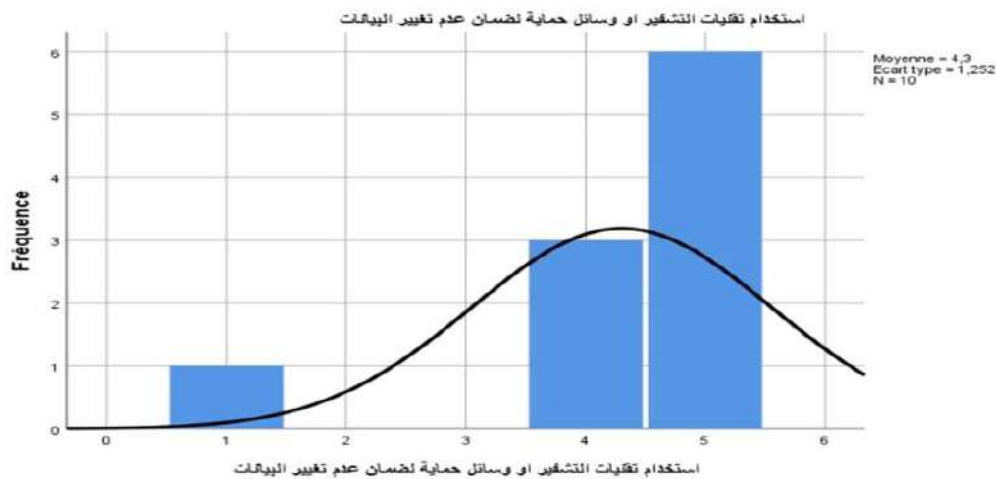
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-16 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التشفير

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	غير موجود	1	10,0	10,0	10,0
	جيد التطبيق	3	30,0	30,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-11 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التشفير



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يُظهر الجدول المتعلق باستخدام تقنيات التشفير في أمن نظام المعلومات تبايناً في آراء أفراد العينة، حيث صرّح 60% بوجود تطبيق فعال للتشفير، في حين أشار 30% إلى أنه جيد التطبيق، مقابل نسبة ضعيفة قدرت بـ 10% ترى أنه غير موجود. تعكس هذه النتائج أن مستوى اعتماد التشفير داخل العينة المدروسة يُعد متوسطاً،. إذ يُظهر الشكل البياني تفوق فئة التطبيق الفعال بشكل واضح مقارنة بباقي الفئات، مع وجود تمثيل أقل للفئتين الأخريين، ويمكن تفسير هذه المعطيات باهتمام البنوك المدروسة بتأمين بياناتها من خلال اعتماد تقنيات التشفير، غير أن هذا التطبيق قد لا يكون شاملاً لجميع الأنظمة أو العمليات، وهو ما يفسر وجود نسبة تشير إلى غيابه، حيث تتوافق هذه النتائج مع دراسة حللمي نبيل، حفصي رشيد، وبن عياد محمد سمير (2022) التي أكدت أن حماية المعلومات داخل المؤسسة تعتمد على مجموعة من الآليات التقنية، من بينها التشفير، لضمان سرية البيانات وتقليل مخاطر الاختراق. كما تنسجم مع دراسة Nataliia Kukharska, Orest Polotai (2019) التي أبرزت أن تعزيز أمن المعلومات، بما في ذلك استخدام وسائل الحماية التقنية، يساهم في تقليل المخاطر وضمان استمرارية الأنظمة، وهو ما يفسر الاتجاه الإيجابي رغم عدم اكتمال التطبيق.

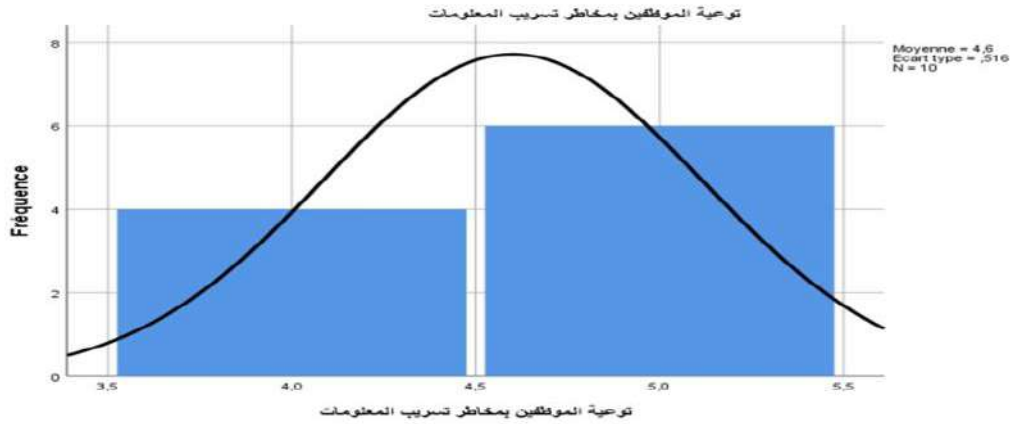
الجدول 02-17 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التوعية الأمنية

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-12 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التوعية الأمنية



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يُظهر الجدول المتعلق بمدى الاعتماد على التوعية الأمنية أن 60% من أفراد العينة يؤكدون وجود تطبيق فعال لبرامج التوعية، مقابل 40% يرون أنه جيد التطبيق، دون تسجيل أي آراء تشير إلى ضعف أو غياب هذا الجانب، وهو ما يعكس مستوى مقبولا في اعتماد التوعية الأمنية داخل البنك . كما يوضح الشكل البياني اتجاه أغلب الإجابات نحو المستويات الإيجابية، مع بروز فئة التطبيق الفعال بشكل أكبر ، ويمكن تفسير هذه المعطيات باهتمام البنك بتسيخ الثقافة الأمنية لدى الموظفين من خلال برامج التكوين والتوعية مما يساهم في التقليل الأخطاء البشرية حيث تتوافق هذه النتائج مع دراسة Semlambo et al. (2021) التي أكدت أن العامل البشري يمثل الحلقة الأضعف في أمن نظم المعلومات، وأن تعزيز التوعية والتكوين الأمني يعد ضرورياً للحد من المخاطر. كما تنسجم مع دراسة كمال مسوس (2022) التي بينت أن ممارسات حوكمة أمن المعلومات تساهم في رفع مستوى الوعي الأمني لدى العاملين، مما يقلل من التهديدات الإلكترونية، وهو ما يدعم النتائج الحالية.

✓ سلامة المعلومات

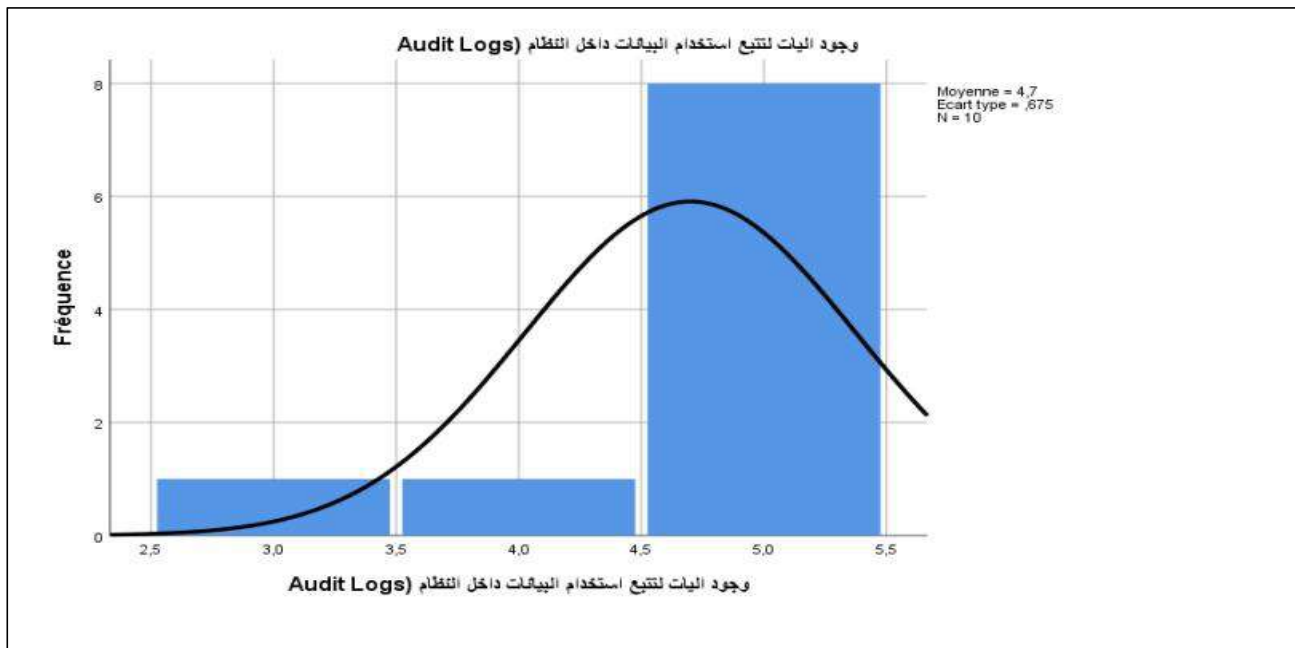
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-18 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سجلات التدقيق

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valid e	متوسط التطبيق	1	10,0	10,0	10,0
	التطبيق جيد	1	10,0	10,0	20,0
	تطبيق فعال	8	80,0	80,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-13 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سجلات التدقيق



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يبين جدول توزيع إجابات أفراد العينة حول مدى الاعتماد على سجلات التدقيق أن نسبة 80% من البنوك المدروسة أن هناك تطبيقاً فعالاً، مقابل 10% فقط يرونه جيداً التطبيق و10% آخرون يعتبرونه متوسط التطبيق، وهو ما يعكس مستوى مرتفعاً لاعتماد سجلات التدقيق داخل البنك. ويمكن تفسير هذه النتيجة بوعي البنك بأهمية سجلات التدقيق في تعزيز سلامة المعلومات، من خلال تتبع العمليات والكشف عن الأخطاء أو الاختراقات المحتملة. ويوضح الشكل البياني بروز تفوق لفئة "تطبيق فعال" مقارنة بباقي الفئات حيث تتوافق هذه النتائج مع دراسة حلومي نبيل وآخرون (2022) التي أكدت أن أمن المعلومات يساهم في ضمان سلامة البيانات من خلال آليات المراقبة والتتبع وتقليل التلاعب بها. كما تنسجم مع دراسة Georg Sven Lampe وآخرون (2020) التي أبرزت أن تحليل المخاطر ومراقبة الأنظمة (ومنها سجلات التدقيق) تساهم في تعزيز قدرة المؤسسة على اكتشاف التهديدات وضمان استمرارية الأنظمة.

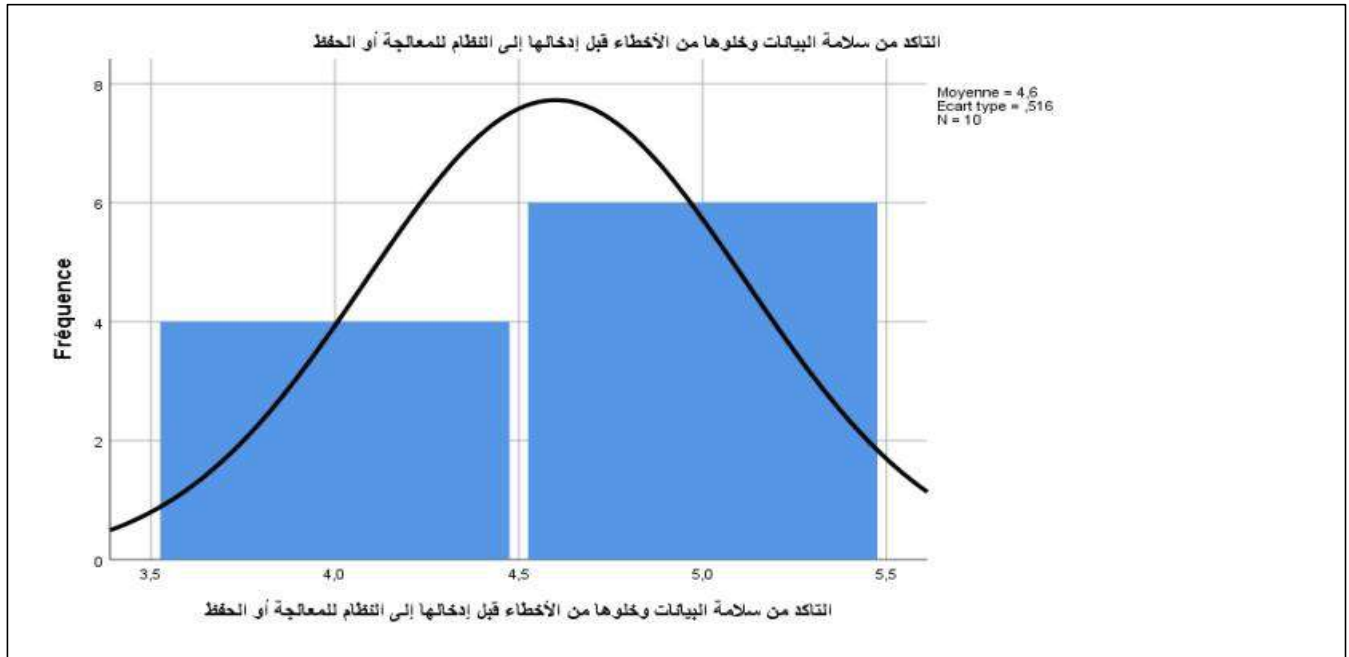
الجدول 02-19 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التحقق من صحة البيانات

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-14 : توزيع إجابات أفراد العينة حول مدى الاعتماد على التحقق من صحة البيانات



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

يبين جدول توزيع إجابات أفراد العينة حول مدى الاعتماد على التحقق من صحة البيانات أن نسبة 60% من البنوك يرون أن هذا الإجراء مطبق بشكل فعال، في حين اعتبر 40% أنه جيد التطبيق، دون تسجيل أي نسبة تدل على مستوى متوسط أو ضعيف، وهو ما يعكس مستوى مرتفعاً لاعتماد التحقق من صحة البيانات داخل البنك. ويمكن تفسير هذه النتيجة باهتمام البنك بضمان دقة وسلامة البيانات المدخلة والمعالجة،. كما يعكس الشكل البياني صحة ذلك من خلال اظهار تفوق فئة تطبيق فعال مقارنة بفئة جيد التطبيق مما يدعم نتائج الجدول ويعزز وضوحها. وعليه نستنتج أن التحقق من صحة البيانات يمثل أحد الركائز الأساسية لتعزيز سلامة المعلومات داخل البنك. تنسجم هذه النتائج بشكل واضح مع ما توصلت إليه دراسة حللمي نبيل، حفصي رشيد، وبن عياد محمد سمير (2022)، والتي أكدت أن ضمان سلامة المعلومات داخل المؤسسة يرتبط بدرجة كبيرة بمدى دقة البيانات ومعالجتها بشكل صحيح، حيث بيّنت الدراسة أن الأخطاء في إدخال أو معالجة البيانات تُعد من أهم مصادر الخلل في نظم المعلومات.

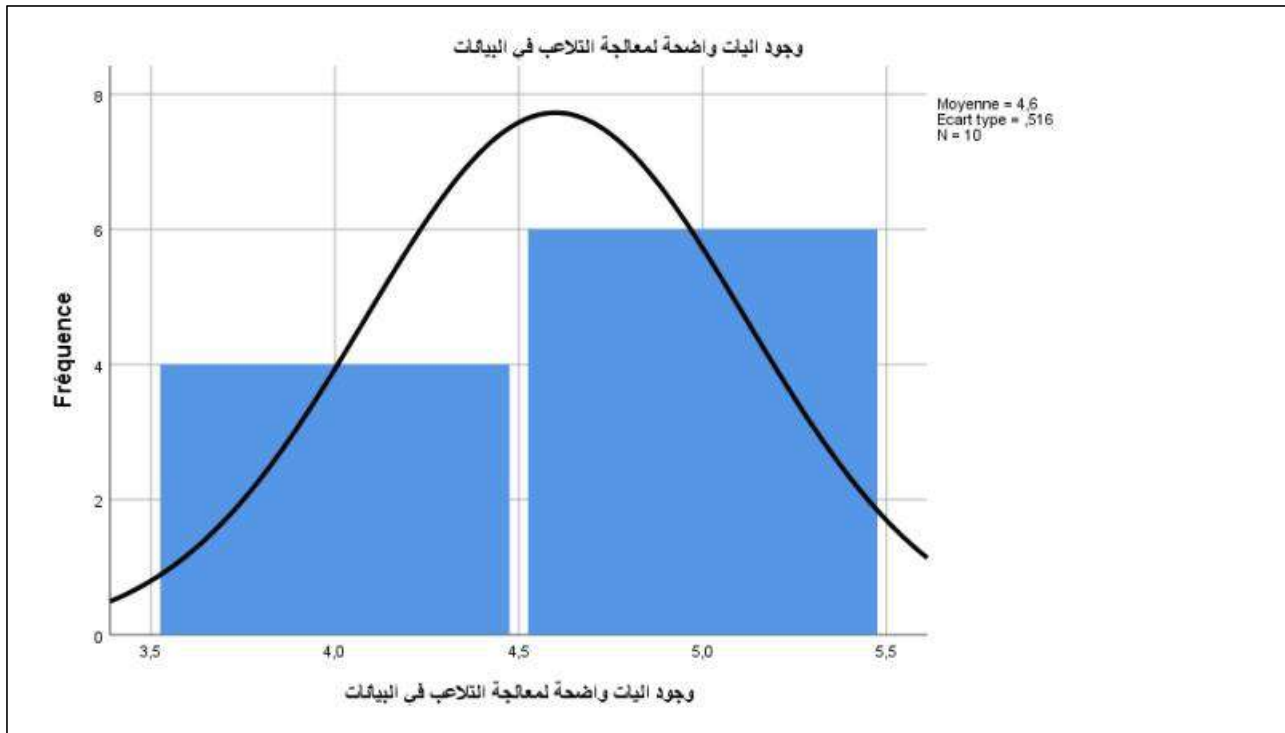
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-20 : توزيع إجابات أفراد العينة حول مدى الاعتماد على كشف التلاعب

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-15 : توزيع إجابات أفراد العينة حول مدى الاعتماد على كشف التلاعب



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تشير نتائج الجدول إلى أن معظم أفراد العينة (60%) يعتبرون أن آليات كشف التلاعب مطبقة بشكل فعال داخل البنك، مقابل نسبة 40% يرون أنها مطبقة بدرجة جيدة، وهو ما يعكس توجهًا إيجابيًا نحو تعزيز هذا الجانب دون تسجيل أي تقييم منخفض. هذه المعطيات توحى بأن البنك يهتم العمليات المراقبة والكشف عن التلاعب، لما لها من دور حيوي في حماية سلامة المعلومات والحد من المخاطر المرتبطة بالتحريف أو الاحتيال. كما أن الشكل البياني يعكس نفس التوزيع، حيث يبرز تفوق فئة "تطبيق فعال" بشكل واضح. وبالتالي يمكن القول إن آليات كشف التلاعب تمثل عنصرًا فعالاً ضمن منظومة أمن المعلومات في المؤسسة. حيث تجدد هذه النتيجة سندًا لها في دراسة كمال مسوس (2022)، التي أبرزت أن اعتماد ممارسات حوكمة أمن نظم المعلومات، خاصة تلك المتعلقة بالرقابة والكشف عن التجاوزات، يساهم بشكل مباشر في الحد من الاعتداءات الإلكترونية والتلاعب بالبيانات. كما أوضحت الدراسة أن وجود آليات فعالة للكشف يعزز من قدرة المؤسسة على التدخل السريع وتقليل الخسائر المحتملة.

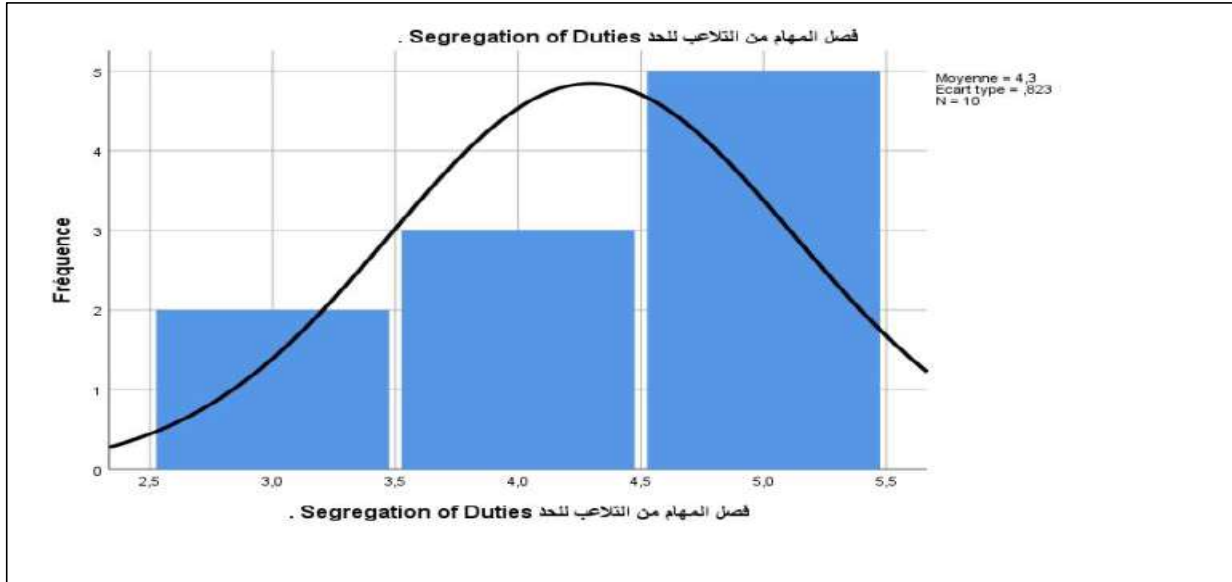
الجدول 21-02 : توزيع إجابات أفراد العينة حول مدى الاعتماد على تقسيم صلاحيات

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
متوسط التطبيق	2	20,0	20,0	20,0
التطبيق جيد	3	30,0	30,0	50,0
تطبيق فعال	5	50,0	50,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-16 : توزيع إجابات أفراد العينة حول مدى الاعتماد على تقسيم صلاحيات



المصدر : من اعداد الطالبتين بناء مخرجات SPSS

تعكس نتائج هذا الجدول تبايناً نسبياً في آراء أفراد العينة حول مدى الاعتماد على تقسيم الصلاحيات، حيث تصدرت فئة "تطبيق فعال" بنسبة 50%، تليها فئة "جيد التطبيق" بـ 30%، في حين بلغت نسبة "متوسط التطبيق" 20%. هذا التوزيع يشير إلى مستوى متوسط، ما يعني أن المؤسسة تعتمد إلى حد معتبر على فصل الصلاحيات، لكنه لا يزال بحاجة إلى تعزيز أكبر ليصل إلى مستوى مرتفع بشكل واضح. ويمكن تفسير ذلك بوجود تطبيق فعلي لهذا الإجراء، غير أنه قد لا يكون شاملاً أو موحدًا عبر جميع العمليات. ويعكس الشكل البياني نفس هذا التدرج في النسب، حيث يظهر تفاوت الفئات بشكل واضح، مما يدعم نتائج الجدول.. يمكن تفسير هذا المستوى المتوسط المرتفع في ضوء ما توصلت إليه دراسة Adam A. Semlambo وآخرون (2021)، والتي أشارت إلى أن تنظيم الصلاحيات داخل المؤسسة يُعد من بين العوامل التنظيمية الأساسية المؤثرة في أمن نظم المعلومات، خاصة فيما يتعلق بتقليل المخاطر المرتبطة بالعامل البشري.

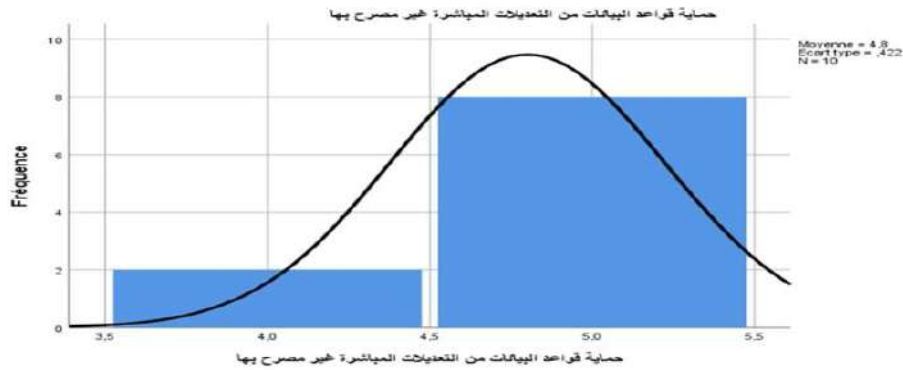
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-22 : توزيع إجابات أفراد العينة حول مدى الاعتماد على امن قواعد البيانات

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
<i>Valide</i> التطبيق جيد	2	20,0	20,0	20,0
تطبيق فعال	8	80,0	80,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-17 : توزيع إجابات أفراد العينة حول مدى الاعتماد على امن قواعد البيانات



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تبرز معطيات هذا الجدول توجّهًا قويًا نحو تأمين قواعد البيانات، حيث صرّح 80% من أفراد العينة بأن حماية قواعد البيانات من التعديلات غير المصرح بها تتم بشكل فعال، مقابل 20% يرون أنها مطبقة بدرجة جيدة، دون تسجيل أي تقييم أقل من ذلك. هذا المؤشر يعكس مستوى مرتفعًا من التحكم في الوصول إلى البيانات الحساسة، ويظهر حرص المؤسسة على تقليل مخاطر التلاعب أو التغيير غير المصرح خاصة وأن قواعد البيانات تمثل جوهر نظام المعلومات. كما يجسد الشكل البياني نفس هذا التفوق الواضح لفئة تطبيق فعال . وبالتالي يمكن اعتبار هذا الجانب من بين النقاط القوية في منظومة الأمن المعلوماتي داخل

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

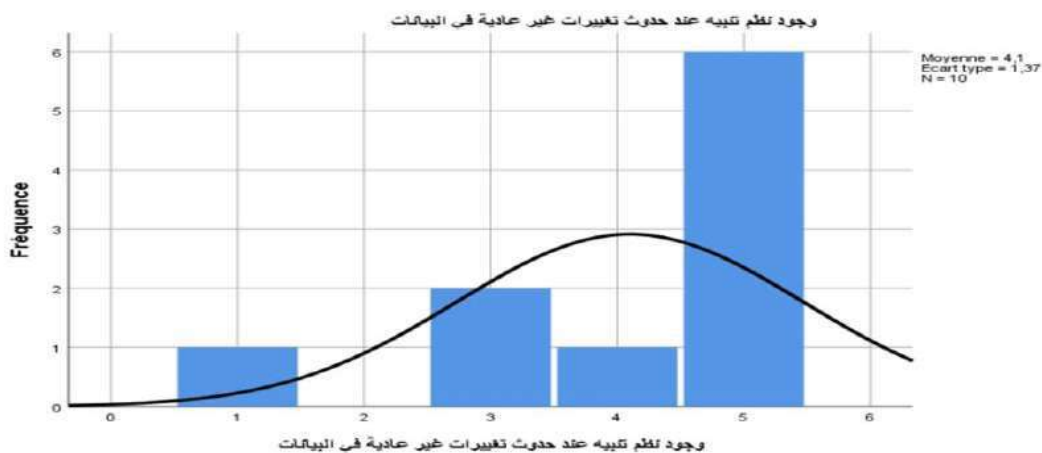
المؤسسة. تتطابق هذه النتائج مع ما توصل إليه بن الطيب إبراهيم (2018)، حيث أكد أن حماية الأصول المعلوماتية، وعلى رأسها قواعد البيانات، تمثل جوهر أمن نظم المعلومات داخل المؤسسات الحديثة، خاصة في ظل تزايد التهديدات الإلكترونية. كما أشار إلى أن تأمين قواعد البيانات من التعديلات غير المصرح بها يساهم بشكل مباشر في الحفاظ على سلامة المعلومات واستقرار الأنظمة.

الجدول 02-23 : توزيع إجابات أفراد العينة حول مدى الاعتماد على أنظمة التنبه الأمني

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	غير موجود	1	10,0	10,0	10,0
	متوسط التطبيق	2	20,0	20,0	30,0
	التطبيق جيد	1	10,0	10,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-18 : توزيع إجابات أفراد العينة حول مدى الاعتماد على أنظمة التنبه الأمني



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

تعكس نتائج هذا الجدول صورة غير متجانسة نسبياً حول مدى الاعتماد على أنظمة التنبيه الأمني، حيث صرّحت أغلبية العينة (60%) بوجود تطبيق فعال، في حين توزعت باقي الآراء بين 20% يرونه متوسط التطبيق، و10% جيد، إضافة إلى 10% أكدوا غياب هذا النظام. هذا التباين يشير إلى أن البنك قطعت شوطاً مهماً في تبني أنظمة التنبيه الأمني، إلا أن تطبيقها لا يزال غير مكتمل أو غير موحد عبر مختلف المستويات. ويظهر الشكل البياني نفس هذا التوزيع، حيث يبرز تفوق فئة "تطبيق فعال" مع وجود فئات أخرى أقل تمثيلاً. وعليه يمكن القول إن أنظمة التنبيه الأمني موجودة وفعالة إلى حد معتبر، لكنها تحتاج إلى تعميم وتعزيز أكبر لتحقيق أقصى فعالية ممكنة. يمكن ربط هذا التباين في النتائج بما توصلت إليه دراسة Adam Aloyce Semlambo وآخرون (2022)، والتي أوضحت أن اختلاف مستويات تطبيق إجراءات الأمن داخل المؤسسات يرجع إلى تفاوت في درجة الوعي الأمني ومستوى التدريب والتطبيق الفعلي للأنظمة التقنية. كما بينت الدراسة أن غياب أو ضعف بعض آليات الكشف المبكر يزيد من احتمالية التعرض للتهديدات. وبالتالي فإن وجود نسبة ترى غياب أنظمة التنبيه في هذه الدراسة ينسجم مع ما أشارت إليه الدراسة السابقة، ويؤكد أن هذا الجانب لا يزال يحتاج إلى مزيد من التعميم والتطوير داخل المؤسسات

✓ توافر المعلومات

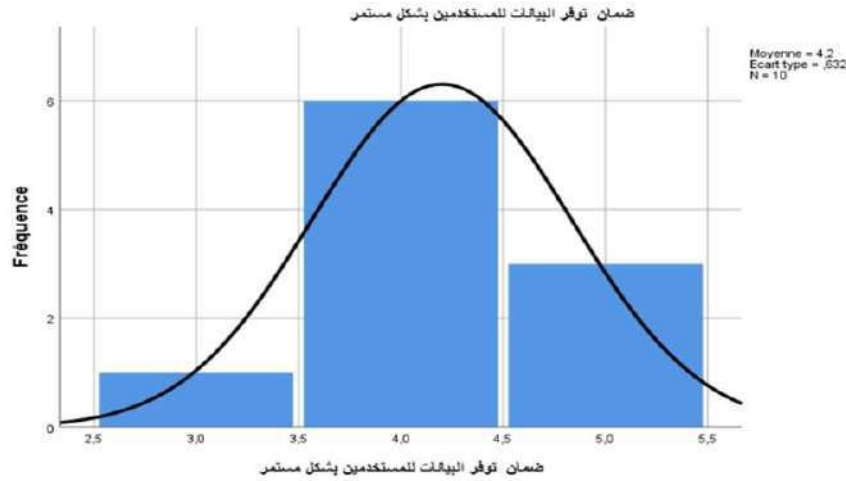
الجدول 02-24 : توزيع إجابات أفراد العينة حول مدى الاعتماد على استمرارية الخدمة

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
متوسط التطبيق	1	10,0	10,0	10,0
التطبيق جيد	6	60,0	60,0	70,0
تطبيق فعال	3	30,0	30,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-19 : توزيع إجابات أفراد العينة حول مدى الاعتماد على استمرارية الخدمة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

توضح نتائج هذا الجدول أن تقييم أفراد العينة لمستوى الاعتماد على استمرارية الخدمة يميل إلى الاعتدال، حيث جاءت النسبة الأكبر ضمن فئة "جيد التطبيق" بـ 60%، تليها فئة "تطبيق فعال" بنسبة 30%، في حين لم تتجاوز فئة "متوسط التطبيق" 10%. هذا التوزيع يعكس مستوى متوسط، ما يدل على أن البنك تسعى إلى ضمان استمرارية خدماتها، لكنها لم تصل بعد إلى مستوى التطبيق الفعال بشكل شامل. ويمكن تفسير ذلك بوجود إجراءات وخطط معتمدة. وكل هذا يؤكد الشكل البياني من خلال إبرازه هيمنة فئة "جيد التطبيق". تنسجم هذه النتائج مع ما توصلت إليه دراسة خديجة يحيى العرياني وهناء علي الضحوي (2019)، التي أكدت أن تطبيق نظام إدارة استمرارية الأعمال وفق معيار ISO 22301 يُعد عاملاً أساسياً في ضمان استمرار الخدمات وتقليل آثار التوقف أثناء الأزمات.

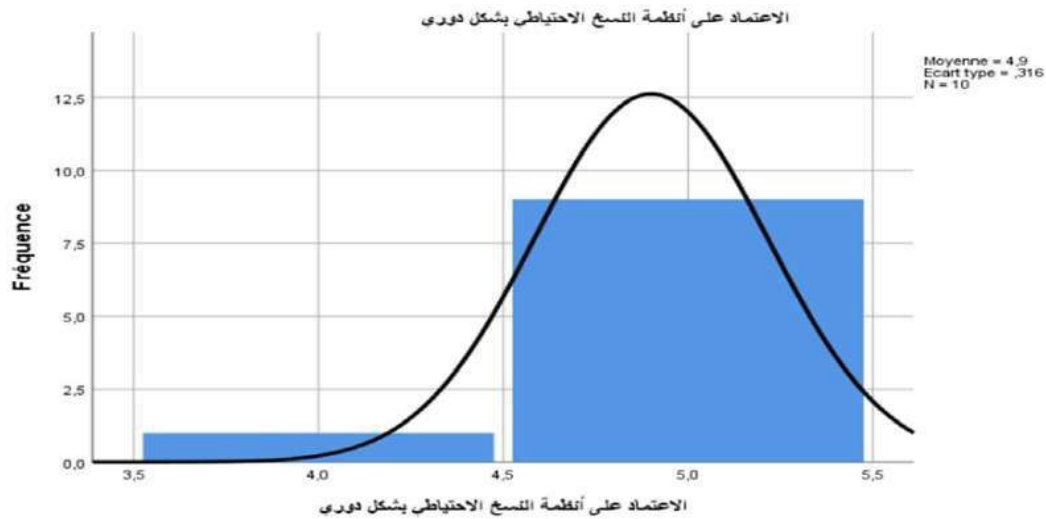
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-25 : توزيع إجابات أفراد العينة حول مدى الاعتماد على النسخ الاحتياطي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-20 : توزيع إجابات أفراد العينة حول مدى الاعتماد على النسخ الاحتياطي



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تعكس نتائج هذا الجدول توجهًا إيجابيًا نحو الاعتماد على النسخ الاحتياطي، حيث يرى 60% من أفراد العينة أنه يُطبق بشكل فعال، مقابل 40% يعتبرونه جيد التطبيق، دون تسجيل أي تقييمات أقل. هذا يدل على مستوى مرتفع من الاهتمام بحماية البيانات وضمان استرجاعها عند الحاجة، وهو ما يعكس إدراك البنك لأهمية النسخ الاحتياطي كآلية أساسية للحد من فقدان

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

المعلومات وضمان استمرارية العمل في حالات الطوارئ. كما يُوضح الشكل البياني بروز فئة "تطبيق فعال" بشكل أكبر، مما يدعم النتائج ويعزز وضوحها. ولهذا يعتبر النسخ الاحتياطي من بين العناصر الفعالة التي تساهم في تعزيز جاهزية البنوك لمواجهة المخاطر. تدعم هذه النتيجة ما توصلت إليه دراسة Kazimierz T. Kosmowski (2021)، التي أكدت أن الاعتماد على النسخ الاحتياطي يُعد من أهم الآليات التي تساهم في تقليل آثار الانقطاع وضمان استمرارية الأنظمة المعلوماتية، خاصة في البيئات المعقدة.

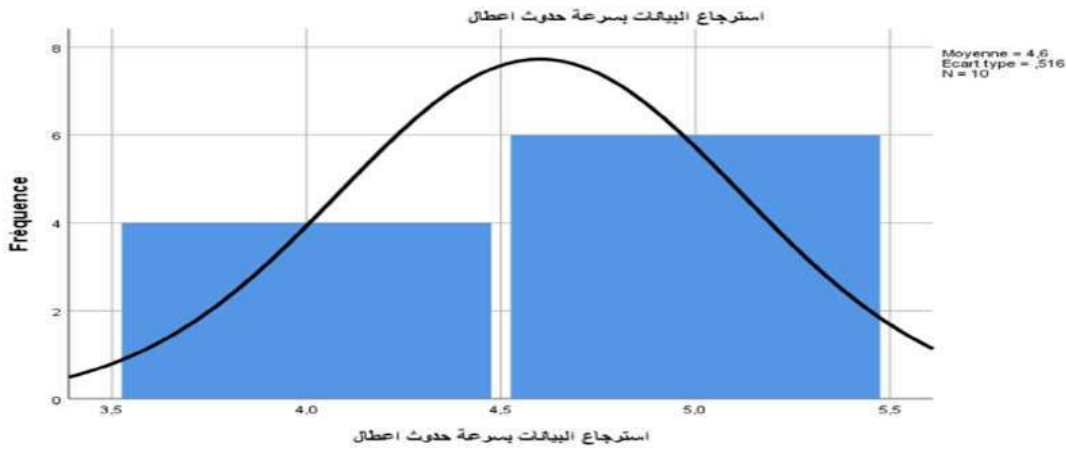
الجدول 02-26 : توزيع إجابات أفراد العينة حول مدى الاعتماد على استرجاع البيانات

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Validé جيد التطبيق	4	40,0	40,0	40,0
تطبيق فعال	6	60,0	60,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 21-02 : توزيع إجابات أفراد العينة حول مدى الاعتماد على استرجاع البيانات



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تكشف نتائج هذا الجدول عن مستوى متقدم في الاعتماد على استرجاع البيانات، حيث أفاد 60% من أفراد العينة بوجود تطبيق فعال، مقابل 40% يرون أنه مطبق بدرجة جيدة، دون تسجيل أي تقييم أقل من ذلك. ويعكس هذا اهتمام البنك بضمان إمكانية استعادة البيانات عند حدوث أعطال أو فقدان. كما يعزز الشكل البياني هذه القراءة من خلال إظهار تفوق فئة تطبيق فعال. وبالتالي يمكن اعتبار آليات استرجاع البيانات من بين الجوانب القوية التي تدعم جاهزية المؤسسة في مواجهة الأزمات. يمكن تفسير هذه النتيجة في ضوء ما توصلت إليه دراسة Zahari Abu Bakar وآخرون (2015)، التي أبرزت أن قدرة المؤسسة على استرجاع البيانات والعمليات بسرعة تُعد من العوامل الأساسية التي تؤثر في الأداء التنظيمي أثناء الأزمات. كما أكدت أن وجود آليات فعالة للاسترجاع يقلل من الخسائر ويضمن استمرارية النشاط

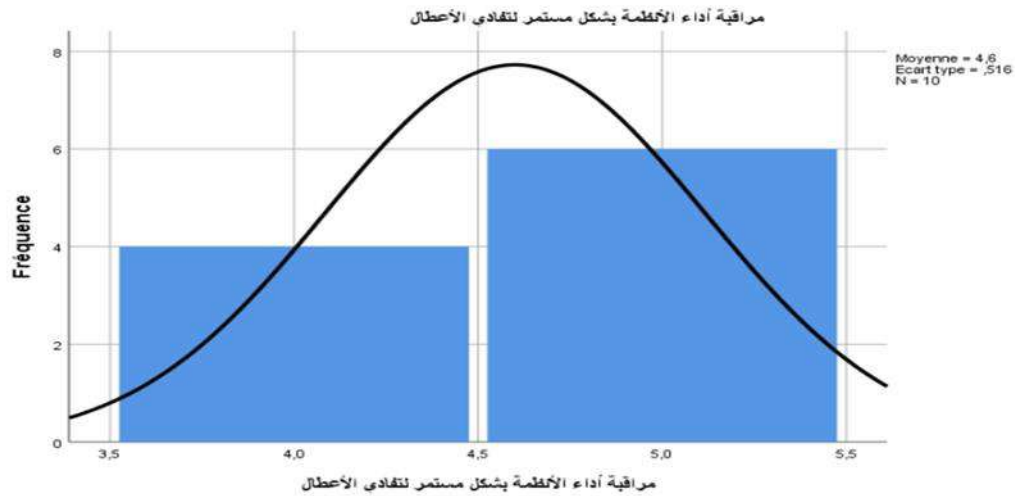
الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-27 : توزيع إجابات أفراد العينة حول مدى الاعتماد على مراقبة الأنظمة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0	40,0
	تطبيق فعال	6	60,0	60,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-23 : توزيع إجابات أفراد العينة حول مدى الاعتماد على مراقبة الأنظمة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يعرض هذا الجدول توزيع إجابات أفراد العينة حول مدى الاعتماد على مراقبة الأنظمة، حيث أن نسبة (60%) من البنوك يرون أن هناك "تطبيقاً فعالاً"، مقابل (40%) يرون أنه "جيد التطبيق"، مع غياب تام لفئة التطبيق الضعيف، وهو ما يعكس مستوى مرتفعاً من الاهتمام بعمليات المراقبة داخل البنوك المدروسة . ويشير هذا إلى أن أغلبية البنوك تعتمد بشكل واضح على آليات متابعة أداء الأنظمة بشكل مستمر، وهذا الأمر الذي يعزز القدرة على الكشف المبكر عن الأعطال وتقليل مخاطر التوقف

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

المفاجئ. وكل هذا بنعكس في الشكل البياني ، حيث يُظهر لنا هيمنة الفئة تطبيق فعال مقارنة بفئة جيد التطبيق . ويُفسر ذلك علميًا بكون المراقبة المستمرة تُعد من الممارسات الأساسية في إدارة أنظمة المعلومات، تتوافق هذه النتائج مع ما توصلت إليه دراسة Georg Sven Lampe وآخرون (2020)، والتي أكدت أن المراقبة المستمرة للأنظمة وتحليل أدائها يُعد من أهم الممارسات التي تساهم في الكشف المبكر عن المخاطر وتعزيز استمرارية النظام المعلوماتي. كما أوضحت الدراسة أن المؤسسات التي تعتمد على المراقبة الدورية تكون أكثر قدرة على الاستجابة السريعة للأعطال

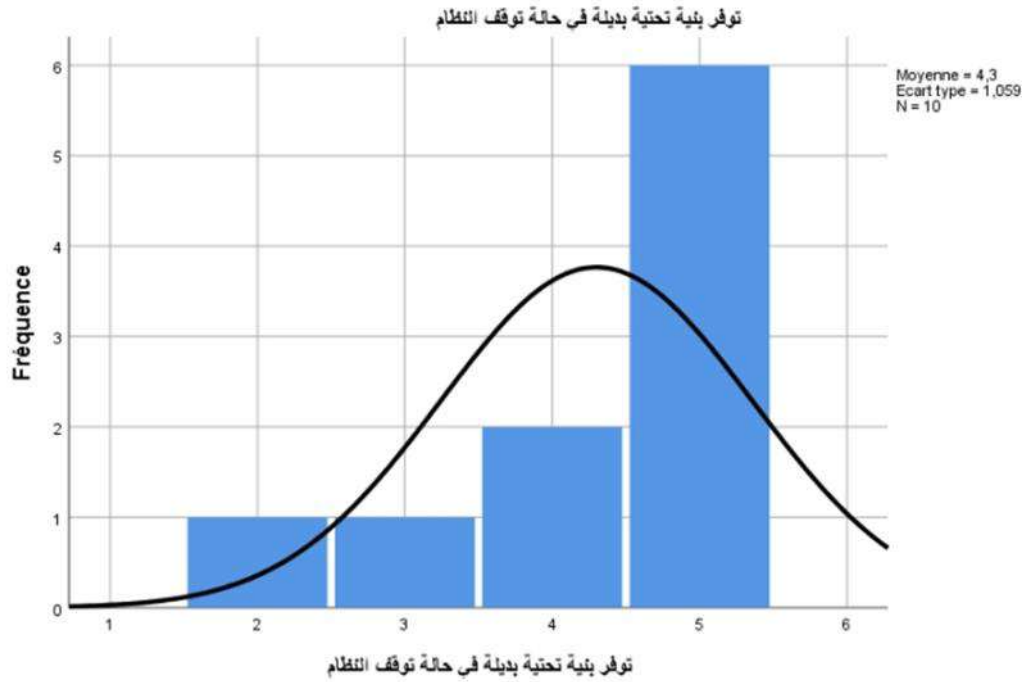
الجدول 28-02 : توزيع إجابات أفراد العينة حول مدى الاعتماد على البنية التحلية البديلة

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide ضيف التطبيق	1	10,0	10,0	10,0
متوسط التطبيق	1	10,0	10,0	20,0
التطبيق جيد	2	20,0	20,0	40,0
تطبيق فعال	6	60,0	60,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الشكل 02-24 : توزيع إجابات أفراد العينة حول مدى الاعتماد على البنية التحتية البديلة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يعرض هذا الجدول توزيع إجابات أفراد العينة حول مدى الاعتماد على البنية التحتية البديلة في حالة توقف النظام، حيث تشير النتائج إلى أن نسبة (60%) من البنوك يرون أن هناك تطبيقًا فعالاً، مقابل (20%) يعتبرونه جيد التطبيق، في حين تسجل فئتا متوسط التطبيق و ضعيف التطبيق نسبًا متساوية ومحدودة بمقدار 10% لكل ا، إذ تمثل الفئات ذات التقييم المرتفع (جيد وفعال) ما نسبته (80%)، وهو ما يعكس إدراكًا واسعًا لأهمية توفير بدائل تشغيلية تضمن استمرارية الأنظمة في حالات الطوارئ أو الأعطال المفاجئة. ويتطابق ذلك من خلال الشكل البياني حيث يظهر لنا بوضوح تفوق فئة "تطبيق فعال" مقارنة ببقية الفئات، مع حضور محدود للفئات الأدنى. ويمكن تفسير ذلك بكون الاعتماد على بنية تحتية بديلة يُعد من الركائز الأساسية في إدارة

استمرارية الأعمال، يمكن تفسير هذه النتائج بالاستناد إلى دراسة Katarina Kampova و Katarina Makka

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

(2024)، التي أكدت أن توفير بنية تحتية بديلة وخطط استمرارية مدروسة يُعد من الركائز الأساسية لتعزيز مرونة المؤسسات في

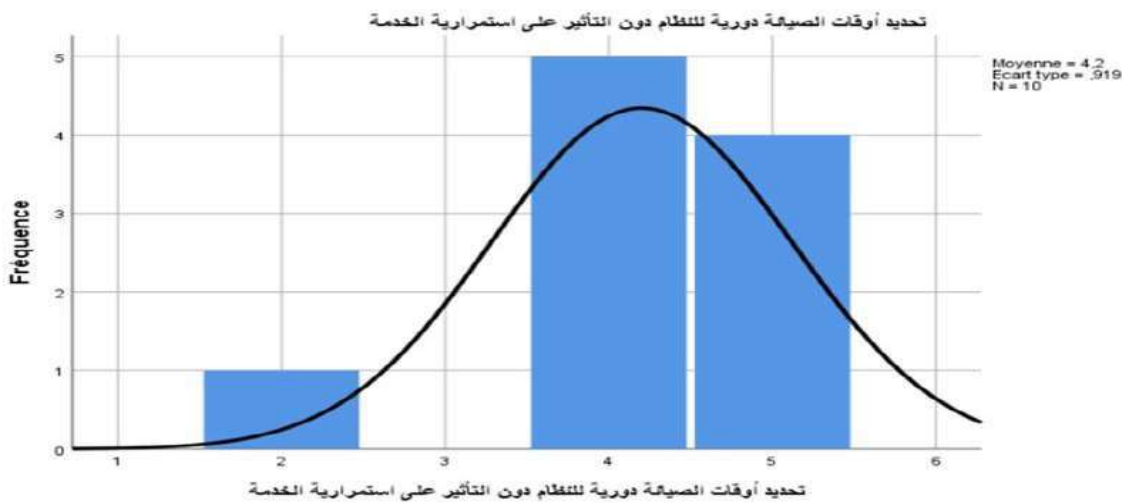
مواجهة الأزمات

الجدول 02-29 : توزيع إجابات أفراد العينة حول مدى الاعتماد على إدارة الصيانة

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide ضيف التطبيق	1	10,0	10,0	10,0
التطبيق جيد	5	50,0	50,0	60,0
تطبيق فعال	4	40,0	40,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء مخرجات SPSS

الشكل 02-25 : توزيع إجابات أفراد العينة حول مدى الاعتماد على إدارة الصيانة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

يعرض الجدول توزيع إجابات أفراد العينة حول مدى الاعتماد على إدارة الصيانة، حيث تشير النتائج إلى تباين نسبي في تقييم هذا الجانب، إذ بلغت نسبة "ضعيف التطبيق" (10%)، مقابل (50%) لفئة "جيد التطبيق"، و(40%) لفئة "تطبيق فعال". و من هنا نجد ان غالبية البنوك الممثلين بمقدار (90%) يتجهون نحو تقييم إيجابي لمستوى إدارة الصيانة، وهو ما يعكس وجود اهتمام ملحوظ بتطبيق برامج الصيانة داخل البنوك بولاية ورقلة، مع تسجيل نسبة معتبرة تميل نحو التطبيق الجيد أكثر من التطبيق الفعال، مما قد يدل على أن هذه الممارسات مطبقة لكن لا تزال بحاجة إلى مزيد من التطوير والانتظام للوصول إلى مستوى الفعالية الكاملة. كما يُظهر الشكل البياني بوضوح هيمنة فئتا "جيد" و"فعال" مقارنة بالفئة الضعيفة. تنسجم هذه النتائج مع ما أشار إليه Marko Niemimaa (2015)، الذي أكد أن تحسين استمرارية نظم المعلومات يتطلب وجود إجراءات تشغيلية وصيانة دورية تضمن جاهزية الأنظمة وتقليل الأعطال. كما أوضح أن غياب الصيانة المنتظمة يؤدي إلى ضعف في الأداء العام للنظام.

الجدول 02-30 : يوضح متوسطات الحساسية والانحرافات المعيارية للإجابات افراد العينة حول سرية المعلومات

N	Moyenne	Ecart type
10	4,80	,422
تغيير كلمات المرور بشكل دوري وفق المعايير الأمنية		
10	4,80	,422
الاعتماد على سياسات واضحة لتحديد صلاحيات الوصول الى المعلومات		
10	4,70	,675
استخدام تقنيات التحقق من الهوية لحماية Authentication(النظام)		
10	4,60	,516
توعية الموظفين بمخاطر تسريب المعلومات		

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

استخدام تقنيات التشفير او وسائل حماية لضمان عدم تغيير البيانات	10	4,30	1,252
تقييد الوصول الى المعلومات	10	4,00	1,633
الحساسية حسب طبيعة الوظيفة			
N valide (liste)	10		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يبين هذا الجدول المتوسطات الحسابية والانحرافات المعيارية لإجابات أفراد العينة حول بعد سرية المعلومات، حيث تتراوح المتوسطات بين (4.00) و(4.80)، وهي قيم مرتفعة تعكس مستوى عالٍ من الاتفاق لدى البنوك حول تطبيق ممارسات حماية سرية المعلومات. وقد سجل مؤشر سياسة كلمات المرور و مؤشر سياسة امن المعلومات أعلى متوسط (4.80) بانحراف معياري منخفض (0.422)، ما يدل على تجانس كبير في آراء العينة حول أهميتهما. في المقابل، جاء مؤشر التحكم في الوصول بأدنى متوسط (4.00) وانحراف معياري مرتفع نسبياً (1.633)، مما يشير إلى وجود تباين في تطبيق هذا الإجراء بين البنوك. كما أن ارتفاع المتوسطات بشكل عام يعكس إدراكاً قوياً لأهمية السرية كعنصر أساسي في أمن نظام المعلومات، رغم وجود بعض التفاوت في تطبيق بعض الممارسات التقنية مثل التشفير. وعليه، يمكن القول إن البنوك بولاية ورقلة و تعتمد بدرجة مرتفعة على آليات ضمان سرية المعلومات

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 31-02 : يوضح متوسطات الحسابية والانحرافات المعيارية للإجابات افراد العينة حول سلامة المعلومات

	N	Moyenne	Ecart type
حماية قواعد البيانات من التعديلات المباشرة غير مصرح بها	10	4,80	,422
وجود اليات لتتبع استخدام (Audit Logs)البيانات داخل النظام	10	4,70	,675
وجود اليات واضحة لمعالجة التلاعب في البيانات	10	4,60	,516
التأكد من سلامة البيانات وخلوها من الأخطاء قبل إدخالها إلى النظام للمعالجة أو الحفظ	10	4,60	,516
فصل المهام من التلاعب للحد Segregation of Duties .	10	4,30	,823
وجود نظم تنبيه عند حدوث تغييرات غير عادية في البيانات	10	4,10	1,370
N valide (liste)	10		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

أظهرت نتائج الجدول ارتفاع مستوى تطبيق ممارسات سلامة المعلومات، حيث تراوحت المتوسطات الحسابية بين (4.10) و(4.80). وقد سجل مؤشر أمن قواعد البيانات أعلى متوسط، مما يعكس إجماع أفراد العينة على أهميته وفعالية تطبيقه، في حين

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

سجل مؤشر أنظمة التنبيه الأمني أدنى متوسط مع تباين نسبي في آراء افراد العينة ، ما يدل على اختلاف مستوى تبني هذه التقنية بين البنوك. كما بينت النتائج وجود آليات رقابية فعالة داخل الأنظمة، مثل كشف التلاعب وسجلات التدقيق..، وهو ما يمكن تفسيره بالاستناد إلى دراسة Isabel Maria Lopes & Pedro Oliveira (2016) التي أشارت إلى أن تطبيق سياسات الأمن المعلوماتي يختلف بين المؤسسات حسب درجة النضج التنظيمي ومدى تبنيها لحوكمة أمن المعلومات، مما يؤدي إلى تفاوت في الممارسات التطبيقية رغم وجود وعي نظري مرتفع. بناءً عليه، يمكن القول إن نتائج هذا البعد تؤكد أن السرية تُعد عنصرًا محوريًا في أمن نظام المعلومات، إلا أن درجة تطبيق بعض الآليات التقنية تختلف حسب مستوى النضج الأمني داخل المؤسسات.

الجدول 02-32 : يوضح متوسطات الحسابية والانحرافات المعيارية للاجابات افراد العينة حول توافر المعلومات

	N	Moyenne	Ecart type
الاعتماد على أنظمة النسخ الاحتياطي بشكل دوري	10	4,90	,316
استرجاع البيانات بسرعة حدوث اعطال	10	4,60	,516
مراقبة أداء الأنظمة بشكل مستمر لتفادي الأعطال	10	4,60	,516
توفر بنية تحتية بديلة في حالة توقف النظام	10	4,30	1,059
تحديد أوقات الصيانة دورية للنظام دون التأثير على استمرارية الخدمة	10	4,20	,919
توفر البيانات ضمان للمستخدمين بشكل مستمر	10	4,20	,632

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

N valide (liste)	10		
------------------	----	--	--

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يبين هذا الجدول تقييم أفراد العينة مدى توفر المعلومات داخل المؤسسات، حيث تراوحت المتوسطات الحسابية بين (4.20) و(4.90)، وهي قيم مرتفعة تعكس مستوى عالٍ من التوافر. وقد احتلت المؤشر النسخ الاحتياطي المرتبة الأولى بمتوسط (4.90) وانحراف معياري منخفض (0.316)، ما يدل على اتفاق كبير حول تطبيقها كإجراء أساسي لضمان استمرارية البيانات. كما سجلت المؤشرات مثل استرجاع البيانات ومراقبة الأنظمة متوسطات مرتفعة (4.60)، مما يعكس كفاءة في التعامل مع الأعطال. في حين جاءت مؤشرات مثل إدارة الصيانة واستمرارية الخدمة بمتوسط (4.20)، وهو مستوى جيد لكنه يشير إلى إمكانية تحسين تنظيم العمليات التشغيلية.. تتوافق هذه النتائج بشكل واضح مع دراسة خديجة يحيى العرياني وهناء الضحوي التي أكدت أن تطبيق نظام إدارة استمرارية الأعمال وفق معيار ISO 22301 يُعد عنصراً أساسياً لضمان استمرار العمليات أثناء الأزمات وتقليل الخسائر الناتجة عن التوقف، وهو ما يفسر ارتفاع مؤشرات النسخ الاحتياطي واسترجاع البيانات. كما تدعم هذه النتائج دراسة Zahari Abu Bakar et al (2015) التي أوضحت أن ممارسات استمرارية الأعمال مثل إدارة المخاطر والتخطيط المسبق واستعادة العمليات تساهم بشكل مباشر في تحسين الأداء التنظيمي وضمان استمرارية الخدمة. إضافة إلى ذلك، تتقاطع النتائج مع دراسة Kazimierz Kosmowski (2021) التي شددت على أهمية وجود خطط استمرارية محدثة باستمرار وبنية تحتية بديلة لضمان تقليل أثر الانقطاعات، وهو ما يفسر النتائج المرتبطة بالبنية التحتية البديلة والصيانة الدورية.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

الجدول 02-33 : الاحصائيات الوصفية للابعاد متغير امن نظام المعلومات

	N	Moyenne	Ecart type
سرية المعلومات	10	4,5333	,39907
سلامة المعلومات	10	4,5167	,32820
توافر المعلومات	10	4,4667	,40673
N valide (liste)	10		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يعرض هذا الجدول المتوسطات العامة لأبعاد أمن نظام المعلومات، حيث سجل بعد سرية المعلومات أعلى متوسط بمقدار (4.5333)، يليه بعد سلامة المعلومات بمقدار (4.5167)، ثم بعد توافر المعلومات قدر ب (4.4667)، وجميعها تقع ضمن المستوى المرتفع، مع انحرافات معيارية منخفضة تدل على تجانس الإجابات. ويشير هذا الترتيب إلى أن البنوك تولي اهتماماً أكبر نسبياً بسرية المعلومات، دون إهمال باقي الأبعاد. كما تعكس هذه النتائج تكامل أبعاد الأمن المعلوماتي داخل البنوك ، حيث يتم تطبيقها بشكل متوازن نسبياً. وبناءً على ذلك، يمكن القول إن مستوى أمن نظام المعلومات مرتفع بشكل عام

الجدول 02-34 : ترتيب عبارات متغير امن نظام المعلومات حسب درجة الموافقة لدى افراد العينة

	N	Moyenne	Ecart type
الاعتماد على أنظمة النسخ الاحتياطي بشكل دوري	10	4,90	,316
تغيير كلمات المرور بشكل دوري وفق المعايير الأمنية	10	4,80	,422
الاعتماد على سياسات واضحة لتحديد صلاحيات الوصول الى المعلومات	10	4,80	,422

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من البنوك الجزائرية بورقلة

حماية قواعد البيانات من التعديلات المباشرة غير مصرح بها	10	4,80	,422
وجود اليات لتتبع استخدام البيانات داخل النظام (Audit Logs	10	4,70	,675
استخدام تقنيات التحقق من الهوية لحماية Authentication(النظام	10	4,70	,675
استرجاع البيانات بسرعة حدوث اعطال	10	4,60	,516
مراقبة أداء الأنظمة بشكل مستمر لتفادي الأعطال	10	4,60	,516
وجود اليات واضحة لمعالجة التلاعب في البيانات	10	4,60	,516
التأكد من سلامة البيانات وخلوها من الأخطاء قبل إدخالها إلى النظام للمعالجة أو الحفظ	10	4,60	,516
توعية الموظفين بمخاطر تسريب المعلومات	10	4,60	,516
توفر بنية تحتية بديلة في حالة توقف النظام	10	4,30	1,059
Segregation of Duties . فصل المهام من التلاعب للحد	10	4,30	,823
استخدام تقنيات التشفير او وسائل حماية لضمان عدم تغيير البيانات	10	4,30	1,252
تحديد أوقات الصيانة دورية للنظام دون التأثير على استمرارية الخدمة	10	4,20	,919
توفر البيانات للمستخدمين بشكل مستمر ضمان	10	4,20	,632
وجود نظم تنبيه عند حدوث تغييرات غير عادية في البيانات	10	4,10	1,370
تقييد الوصول الى المعلومات الحساسة حسب طبيعة الوظيفة	10	4,00	1,633

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

N valide (liste)	10		
------------------	----	--	--

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يوضح هذا الجدول ترتيب عبارات متغير أمن نظام المعلومات حسب درجة الموافقة، حيث احتل مؤشر النسخ الاحتياطي المرتبة الأولى بمتوسط (4.90)، مما يعكس أهميته الكبرى في نظر البنوك . حيث يليه مجموعة من المؤشرات المرتبطة بالتحكم في الوصول بمتوسطات (4.80)، مثل سياسة كلمات المرور وامن قواعد البيانات. كما احتلت مؤشرات المراقبة الانظمة واسترجاع البيانات مراتب متقدمة، مما يدل على تركيز البنوك على الجوانب التشغيلية للأمن. في المقابل، جاءت بعض المؤشرات مثل التحكم في الوصول و أنظمة التنبيه الأمني في المراتب الأخيرة بمتوسطات أقل نسبياً، مع انحرافات معيارية مرتفعة، ما يعكس تفاوتاً في تطبيقها. ونستنتج من هذا الترتيب أن البنوك تركز بشكل أكبر على الإجراءات الأساسية والتقليدية للأمن، في حين تحتاج بعض الآليات المتقدمة إلى تعزيز أكبر.

ثانيا : المتغير إدارة استمرارية الاعمال

يُعد متغير إدارة استمرارية الأعمال متغيراً مركباً في هذه الدراسة، حيث تم تحليله من خلال مجموعة من المؤشرات التي تعكس جوانبه المختلفة، بهدف تقييم مستوى تطبيقه داخل البنوك محل الدراسة.

✓ خطة استمرارية الاعمال

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

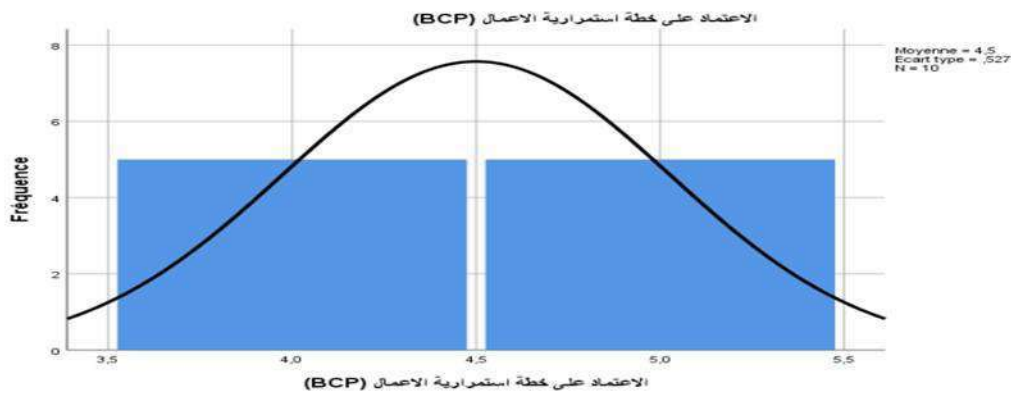
البنوك الجزائرية بورقلة

الجدول 02-35 : توزيع إجابات أفراد العينة حول مدى الاعتماد على خطة استمرارية الاعمال

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	5	50,0	50,0	50,0
	تطبيق فعال	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-26 : توزيع إجابات أفراد العينة حول مدى الاعتماد على خطة استمرارية الاعمال



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يبين هذا الجدول توزيع إجابات أفراد العينة حول مدى الاعتماد على خطة استمرارية الأعمال، حيث تتوزع الآراء بالتساوي بين فئتي "جيد التطبيق" و"تطبيق فعال" بنسبة (50%) لكل منهما، مع غياب تام لفئات التطبيق المتوسط أو الضعيف، وهو ما يعكس مستوى مرتفعاً من تبني هذه الخطط داخل البنوك محل الدراسة. ويوضح التوازن أن نصف العينة المدروسة ترى أن تطبيق الخطة استمرارية الاعمال وصل إلى مستوى الفعالية، في حين يرى النصف الآخر أنها مطبقة بشكل جيد لكنها لم تبلغ بعد الدرجة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

المثلى من الكفاءة. ويتجسد هذا التحليل في الشكل البياني حيث يظهر تقارب واضح بين الفئتين دون وجود تباين حاد، ومن الناحية التفسيرية، يعكس ذلك إدراك البنوك لأهمية التخطيط المسبق لمواجهة الأزمات، مع وجود مجال للتحسين نحو تعزيز فعالية هذه الخطط من خلال الاختبار والتحديث المستمر. وتتوافق هذه النتيجة مع دراسة Piotr Jedynak التي اعتبرت أن إدارة استمرارية الأعمال تمثل أحد المفاهيم الإدارية الحديثة التي تساعد المؤسسات على مواجهة المخاطر والأزمات وتعزيز قدرتها على الاستمرار. كما تدعمها أيضاً دراسة Zahari Abu Bakar التي توصلت إلى أن تطبيق ممارسات استمرارية الأعمال يساهم في تحسين الأداء التنظيمي ورفع قدرة المؤسسة على التعامل مع الأزمات بفعالية.

✓ مراجعة الخطة

الجدول 02-36 : توزيع إجابات أفراد العينة حول مدى الاعتماد على مراجعة الخطة

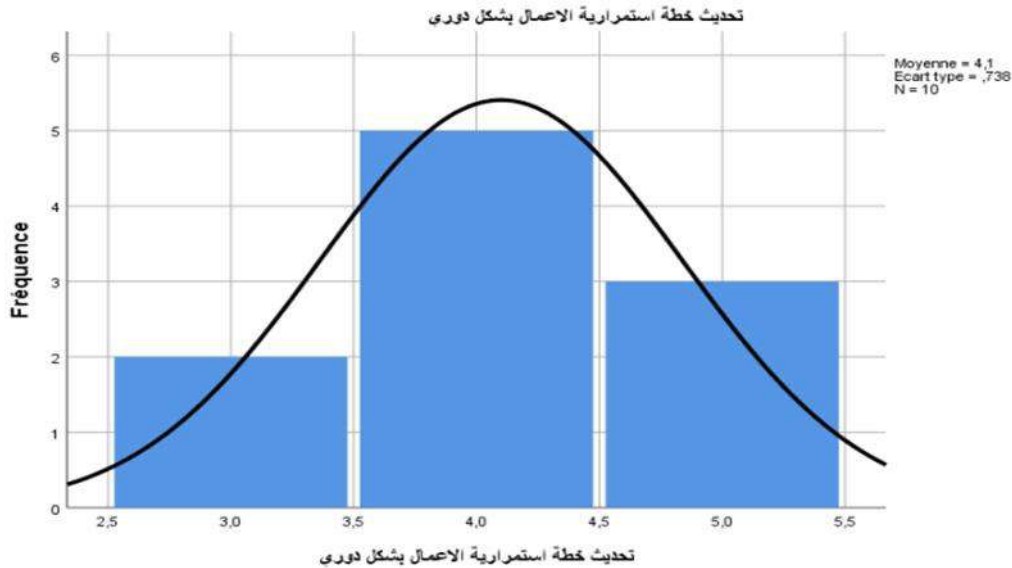
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide متوسط التطبيق	2	20,0	20,0	20,0
التطبيق جيد	5	50,0	50,0	70,0
تطبيق فعال	3	30,0	30,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الشكل 02-27 : توزيع إجابات أفراد العينة حول مدى الاعتماد على مراجعة الخطة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يُظهر كلٌّ من الجدول 1 والشكل البياني الخاص بتوزيع إجابات أفراد العينة حول مدى الاعتماد على مراجعة الخطة وجود مستوى معتبر من التطبيق داخل البنوك ولاية ورقلة . نلاحظ أن غالبية البنوك (50%) يرون أن مراجعة الخطة تتم بدرجة "جيدة"، تليها نسبة (30%) التي تشير إلى "تطبيق فعال"، في حين تمثل نسبة (20%) فقط فئة "متوسط التطبيق". وهو ما يعكس هيمنة التقييمات الإيجابية مقارنة بالتقييمات المتوسطة. ويتأكد هذا الاتجاه من خلال الشكل البياني، حيث تتجمع القيم في المجال المرتفع من سلم التقدير، وترتبط هذه النتيجة بما توصلت إليه دراسة Orest Polotai و Natalia Kukharska التي أكدت أن فعالية إدارة استمرارية الأعمال ترتبط بوجود منهجية قائمة على التخطيط والتنفيذ والمراقبة والتحسين المستمر ، وهو ما يجعل مراجعة الخطط عنصراً أساسياً لضمان الاستجابة السريعة وتقليل الخسائر أثناء الأزمات. كما تتوافق هذه النتيجة مع دراسة katarina kampova و katarina makka التي أوضحت أن تحديث خطط الاستمرارية بصورة مستمرة يساهم

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

في تعزيز قدرة المؤسسة على التكيف مع التهديدات الرقمية والأزمات المفاجئة. إضافة إلى ذلك، تؤكد دراسة Georg Sven Lampe أن مراجعة خطط الاستمرارية وتحليل أثر الأعمال بشكل دوري يساعد المؤسسات على ترتيب أولوياتها وتحسين جاهزيتها لمواجهة الاضطرابات

✓ خطة التعافي

الجدول 02-37 : توزيع إجابات أفراد العينة حول مدى الاعتماد على خطة التعافي

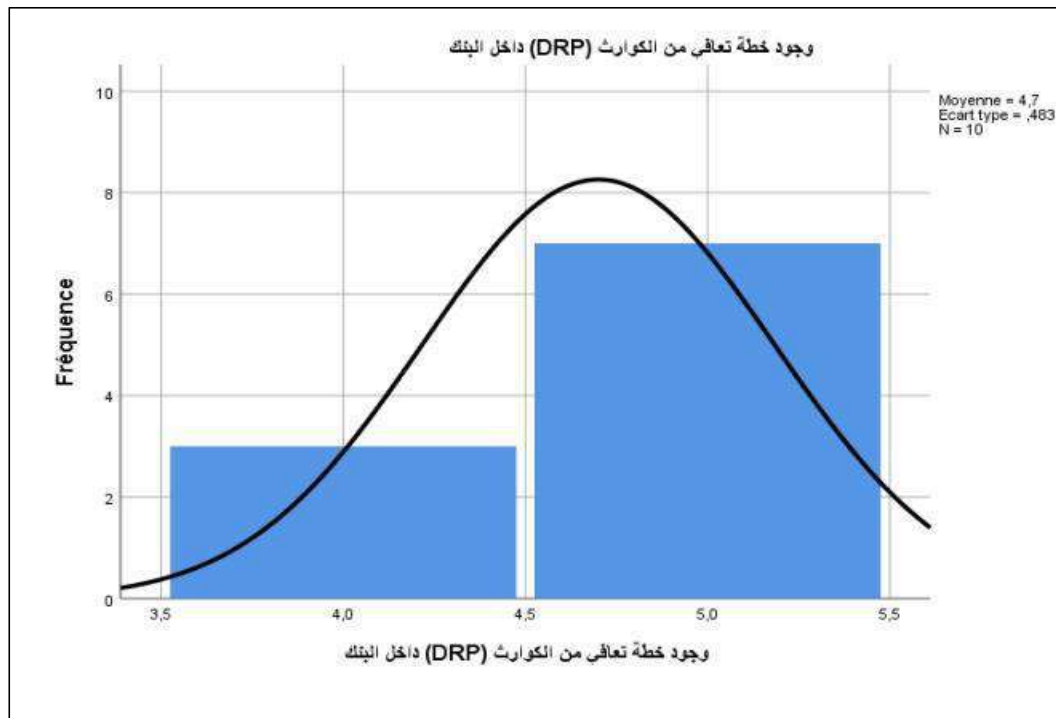
		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	3	30,0	30,0	30,0
	تطبيق فعال	7	70,0	70,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الشكل 02-28 : توزيع إجابات أفراد العينة حول مدى الاعتماد على خطة التعافي



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يعكس هذا الجدول مستوى الاعتماد على خطة التعافي من الكوارث، حيث تشير النتائج إلى أن غالبية أفراد العينة بنسبة (70%) يؤكدون وجود "تطبيق فعال"، مقابل (30%) يرونه "جيد التطبيق"، دون تسجيل أي نسب لفئات الدنيا، وهو ما يدل على مستوى مرتفع جداً من الجاهزية و الاستعداد لمواجهة الأزمات الطارئة. ويبرز هذا التوزيع قوة البنوك على خطط التعافي كجزء أساسي من استراتيجيات استمرارية الأعمال. وهذا ما أكدته الشكل البياني باظهار تفوق الفئة ذات تطبيق الفعال مما يعكس انسجاماً بين التمثيل البياني والمعطيات الرقمية. ويمكن تفسير هذه النتيجة بكون خطط التعافي تُعد من الأولويات الحيوية في البيئات الحساسة كالبنوك، حيث تضمن استرجاع الأنظمة والبيانات في أسرع وقت ممكن بعد الأزمات. وتتفق هذه النتائج مع دراسة Kazimierz T. Kosmowski التي أكدت أن وجود خطط تعافٍ واضحة ومتكاملة يساعد المؤسسات على تقليل تأثير الاضطرابات وتحسين سرعة الاستجابة للأزمات، خاصة في البيئات المعتمدة بشكل كبير على التكنولوجيا.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

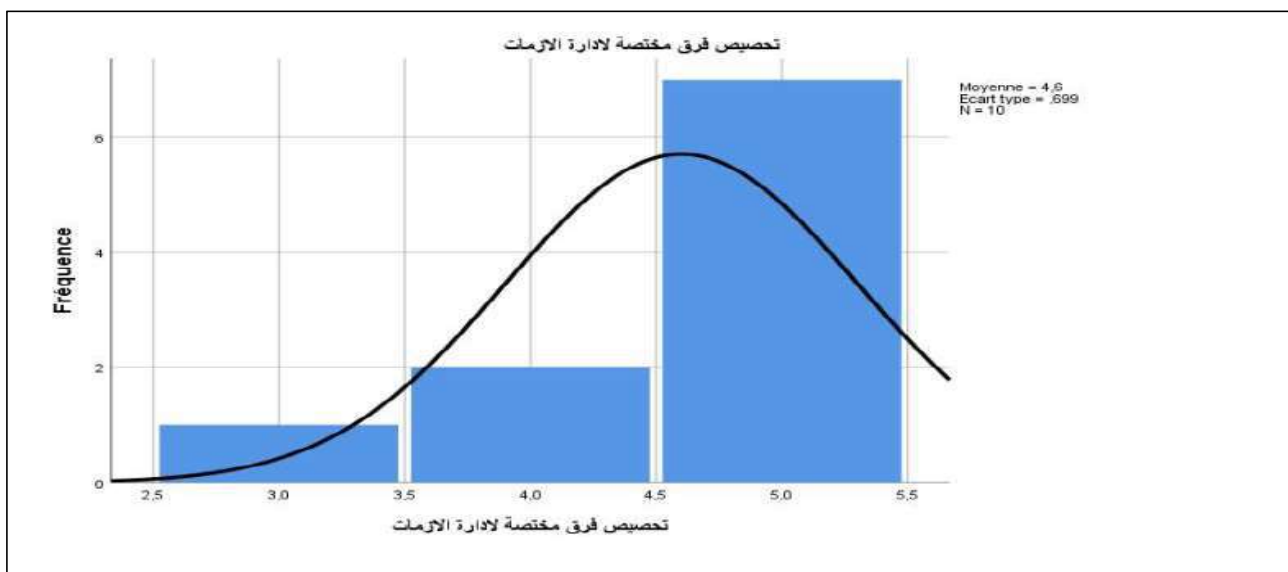
✓ فريق إدارة الازمات

الجدول 02-38 : توزيع إجابات أفراد العينة حول مدى الاعتماد على فريق إدارة الازمات

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	متوسط التطبيق	1	10,0	10,0	10,0
	التطبيق جيد	2	20,0	20,0	30,0
	تطبيق فعال	7	70,0	70,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-29 : توزيع إجابات أفراد العينة حول مدى الاعتماد على فريق إدارة الازمات



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

يعرض هذا الجدول توزيع آراء أفراد العينة حول مدى الاعتماد على فريق إدارة الأزمات، حيث تشير النتائج إلى أن نسبة (70%) من افراد العينة يؤكدون وجود "تطبيق فعال"، مقابل (20%) يرونه "جيد التطبيق"، في حين تسجل نسبة ضعيفة (10%) لفئة "متوسط التطبيق". ويعكس هذا التوزيع توجهًا قويًا نحو تبني فرق متخصصة لإدارة الأزمات داخل البنوك محل الدراسة، ما يدل على إدراك أهمية العنصر البشري المؤهل في التعامل مع الظروف الطارئة. ويتجلى ذلك الشكل البياني من خلال ابرازه لتفوق فئة "تطبيق فعال" مقارنة ببقية الفئات، ،. وعليه، يمكن استنتاج أن البنوك تعتمد بدرجة مرتفعة على فرق إدارة الأزمات كجزء من منظومة استمرارية الأعمال. وتتوافق هذه النتيجة مع دراسة فايز جمعة صالح النجار وأروى محمد الحرايزة التي أكدت أن الجاهزية المسبقة ووجود كوادر قادرة على التخطيط والاستجابة يعززان فعالية إدارة استمرارية الأعمال داخل المؤسسة.

✓ زمن الاستجابة

الجدول 02-39 : توزيع إجابات أفراد العينة حول مدى الاعتماد على زمن الاستجابة

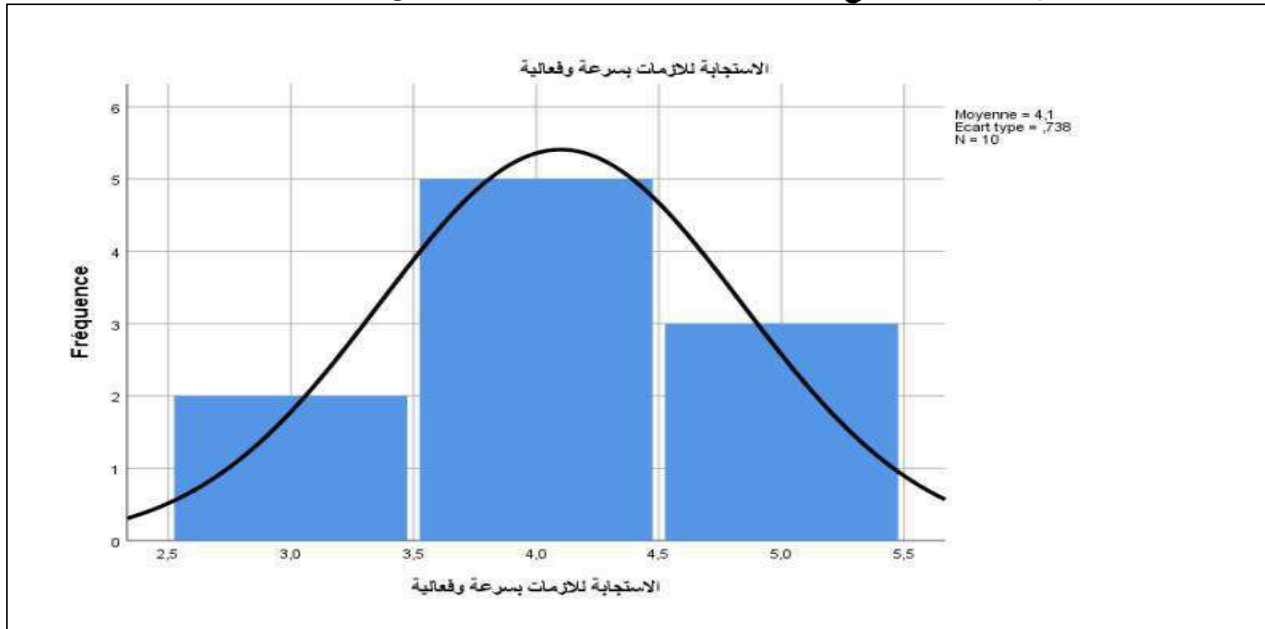
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide متوسط التطبيق	2	20,0	20,0	20,0
التطبيق جيد	5	50,0	50,0	70,0
تطبيق فعال	3	30,0	30,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الشكل 02-30 : توزيع إجابات أفراد العينة حول مدى الاعتماد على زمن الاستجابة



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يوضح هذا الجدول تقييم أفراد العينة لمدى فعالية زمن الاستجابة للأزمات، حيث جاءت نسبة (50%) ضمن "جيد التطبيق"، تليها (30%) "تطبيق فعال"، و(20%) "متوسط التطبيق". يعكس هذا التوزيع مستوى يتراوح بين المتوسط والجيد فيما يتعلق بسرعة وفعالية الاستجابة، مع ملاحظة وجود تباين نسبي بين البنوك. ويتوافق ذلك مع الشكل البياني أعلاه، حيث يظهر تركّز القيم في الفئة المتوسطة (جيد)، مع تمثيل أقل للفئة الأعلى (فعال)، مما يدل على أن الاستجابة موجودة لكنها ليست بالمستوى الأمثل في جميع الحالات. ومنه يمكن تفسير أن زمن الاستجابة يُعد من المؤشرات الحساسة لنجاح إدارة الأزمات وترتبط هذه النتائج بما توصلت إليه دراسة katarina makka و katarina kampova التي أكدت أن تحديد مؤشرات زمن الاسترجاع والاستجابة يساعد المؤسسات على تحسين سرعة التعافي وتقليل الخسائر الناتجة عن الانقطاعات والأزمات.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

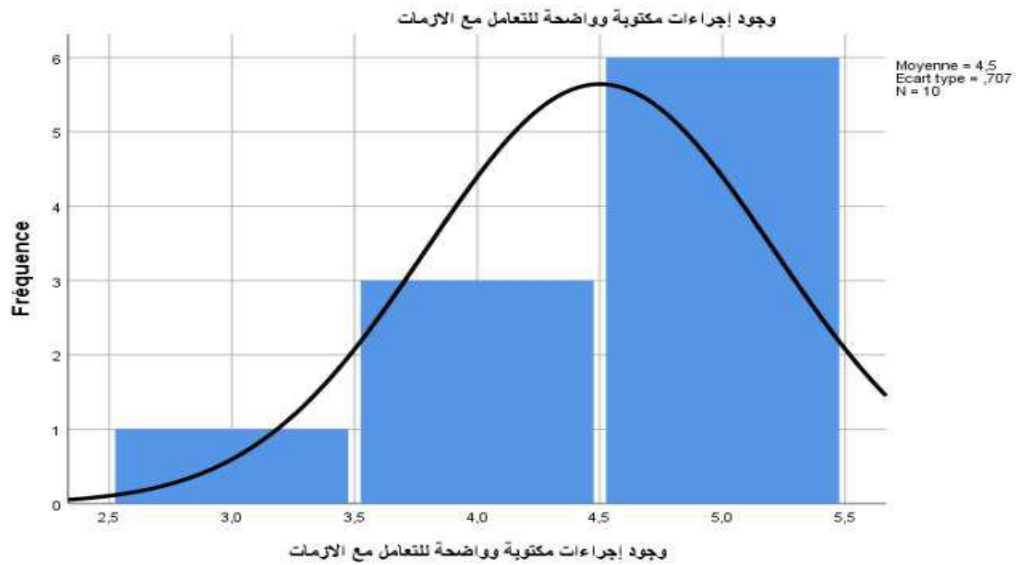
البنوك الجزائرية بورقلة

الجدول 02-40 : توزيع إجابات أفراد العينة حول مدى الاعتماد على إجراءات الطوارئ

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
متوسط التطبيق	1	10,0	10,0	10,0
التطبيق جيد	3	30,0	30,0	40,0
تطبيق فعال	6	60,0	60,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-31 : توزيع إجابات أفراد العينة حول مدى الاعتماد على إجراءات الطوارئ



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

يبين هذا الجدول مدى اعتماد البنوك على إجراءات الطوارئ، حيث تشير النتائج إلى أن مقدار (60%) من أفراد العينة يرون وجود "تطبيق فعال"، مقابل (30%) "جيد التطبيق"، و(10%) فقط "متوسط التطبيق". ويعكس هذا التوزيع مستوى مرتفعاً من اعتماد الإجراءات الرسمية المكتوبة كمرجعية في التعامل مع الأزمات. ويؤكد الشكل البياني هذه النتيجة، حيث يظهر بوضوح سيطرة الفئة ذات التقييم المرتفع، مما يعزز دلالة النتائج الوصفية. ومن الناحية العلمية، فإن توثيق الإجراءات يُعد من الممارسات الأساسية لضمان توحيد الاستجابة وتقليل العشوائية أثناء الأزمات. وعليه، وتتوافق هذه النتيجة مع دراسة خديجة يحيى العرياني وهناء علي الضحوي التي أكدت أن وجود نظام إدارة استمرارية الأعمال وفق معيار ISO 22301 يتطلب توفير إجراءات ووثائق داعمة

تساهم في تحسين مرونة المؤسسة وضمان استمرارية العمليات أثناء الأزمات. كما تنسجم هذه النتيجة مع دراسة Natalia Kukharska التي بينت أن التخطيط المسبق والتدابير الوقائية المكتوبة تساعد المؤسسات على تقليل الخسائر وتعزيز سرعة التعافي بعد الأزمات. كذلك تدعمها دراسة Marko Niemimaa التي أوضحت أن الاستعداد المسبق والإجراءات التنظيمية الواضحة يعززان جاهزية المؤسسات لمواجهة الاضطرابات وتقليل آثار تعطل الأنظمة.

✓ سجل المخاطر

الجدول 02-41 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سجل المخاطر

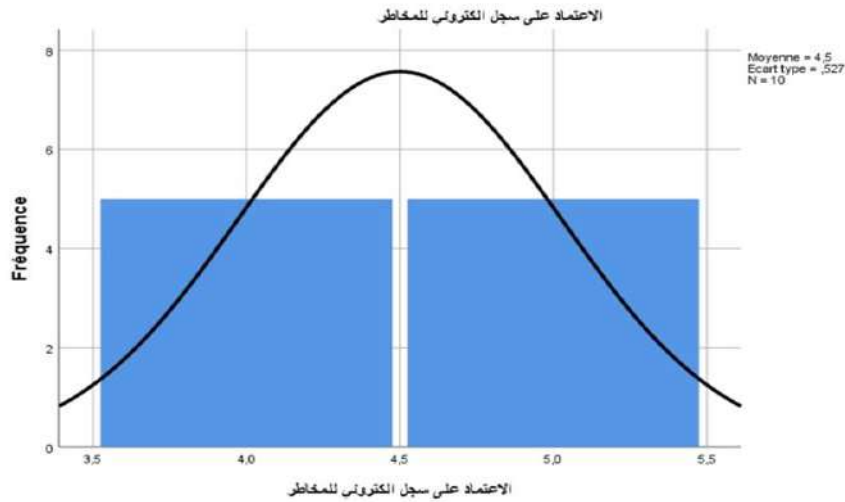
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide التطبيق جيد	5	50,0	50,0	50,0
تطبيق فعال	5	50,0	50,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الشكل 32-02 : توزيع إجابات أفراد العينة حول مدى الاعتماد على سجل المخاطر



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يوضح هذا الجدول توزيع الإجابات حول مدى الاعتماد على سجل المخاطر، حيث تتوزع الآراء بالتساوي بين "جيد التطبيق" و"تطبيق فعال" بنسبة (50%) لكل منهما، مع غياب الفئات الأدنى ما يعكس مستوى مرتفعاً من تبني هذا الإجراء داخل المؤسسات. ويتساوى ذلك مع الشكل البياني ، حيث يظهر توازن واضح بين الفئتين، وهو ما يدل على استقرار نسبي في مستوى التطبيق. ويُفسر ذلك بأهمية سجل المخاطر كأداة استباقية لتحديد وتحليل التهديدات المحتملة وترتبط هذه النتيجة بما توصلت إليه دراسة Zahari Abu Bakar التي أكدت أن إدارة المخاطر تُعد أحد الأبعاد الأساسية لإدارة استمرارية الأعمال وتسهم في تحسين الأداء التنظيمي للمؤسسات. كما تتوافق هذه النتيجة مع دراسة Kazimierz T. Kosmowski التي أوضحت أن تحليل المخاطر وتوثيقها ضمن إطار منظم يساعد على تحسين سرعة الاستجابة وتقليل آثار الاضطرابات داخل المؤسسات. كذلك تنسجم هذه النتائج مع دراسة Adam A. Semlambo التي أبرزت أن وجود سياسات واضحة وإدارة منهجية للمخاطر يساهم في تقليل التهديدات الأمنية وتحسين فعالية حماية نظم المعلومات

✓ تقييم المخاطر

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

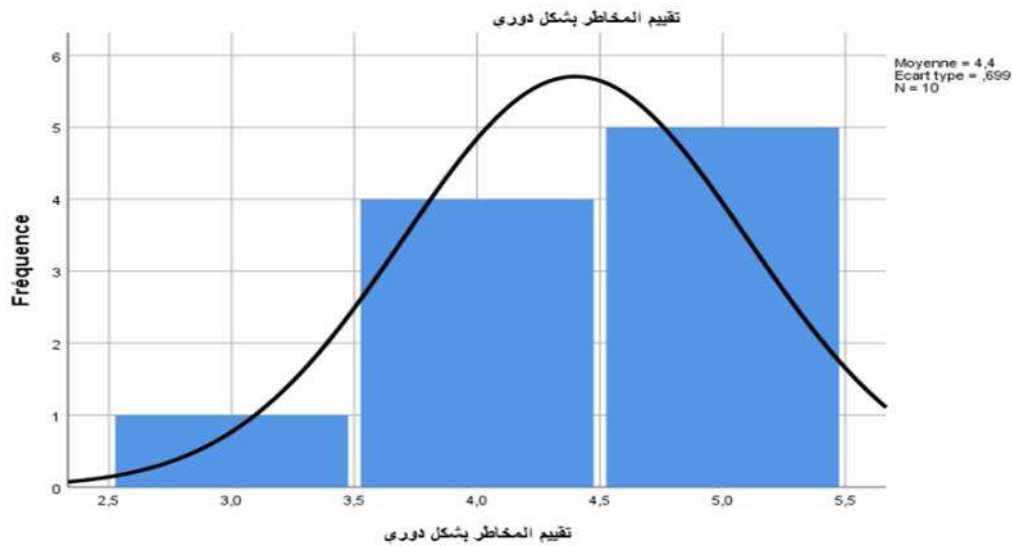
البنوك الجزائرية بورقلة

الجدول 02-42 : توزيع إجابات أفراد العينة حول مدى الاعتماد على تقييم المخاطر

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	متوسط التطبيق	1	10,0	10,0	10,0
	التطبيق جيد	4	40,0	40,0	50,0
	تطبيق فعال	5	50,0	50,0	100,0
	Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-33 : توزيع إجابات أفراد العينة حول مدى الاعتماد على تقييم المخاطر



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

يعكس هذا الجدول مدى اعتماد البنوك على تقييم المخاطر، حيث تبين النتائج أن (50%) من البنوك المدروسة يرون أنه "تطبيق فعال"، مقابل (40%) "جيد التطبيق"، و(10%) "متوسط التطبيق". ويُظهر هذا التوزيع أن غالبية البنوك المدروسة تقوم بعمليات تقييم دوري للمخاطر. حيث يؤكد الشكل البياني هذا الاتجاه، حيث يبرز تفوق الفئة المرتفعة، مما يعكس وعيًا متزايدًا بأهمية التحليل المستمر للمخاطر. ومن الناحية العلمية فإن التقييم الدوري يُعد أساسًا لاتخاذ قرارات استباقية فعالة، وتتفق هذه النتيجة مع دراسة Adam Aloyce Semlambo التي أكدت أن تقييم المخاطر بشكل دوري يساعد المؤسسات على التعرف على مصادر التهديد والثغرات الأمنية وتحسين مستوى الحماية. كما تنسجم مع دراسة Georg Sven Lampe التي أوضحت أن تحليل أثر الأعمال وتقييم المخاطر يمثلان عنصرين أساسيين لتحسين فعالية الاستجابة للأزمات وتعزيز مرونة المؤسسات.

✓ زمن استرجاع

الجدول 02-43 : توزيع إجابات أفراد العينة حول مدى الاعتماد على زمن استرجاع

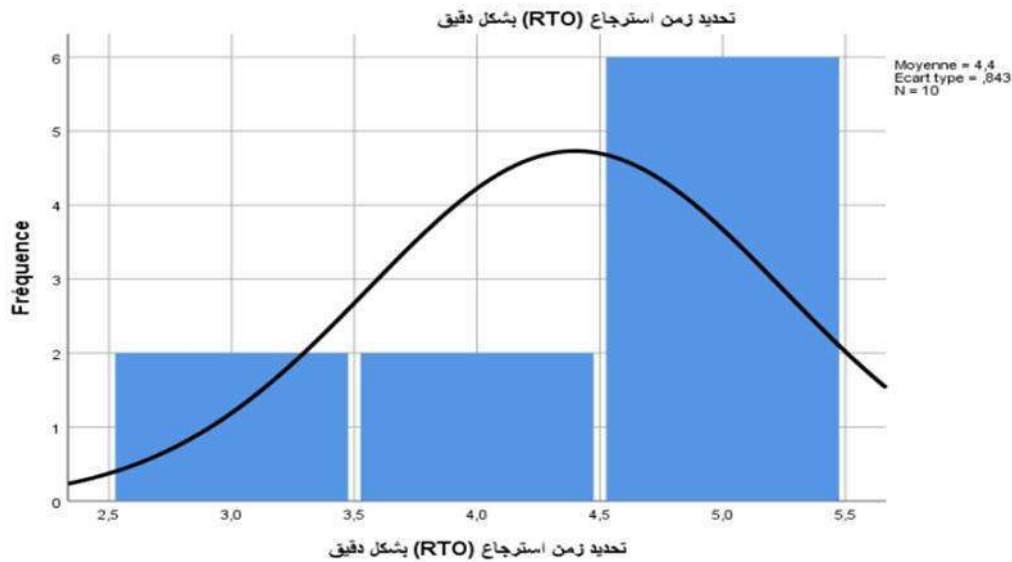
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide متوسط التطبيق	2	20,0	20,0	20,0
التطبيق جيد	2	20,0	20,0	40,0
تطبيق فعال	6	60,0	60,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الشكل 02-34 : توزيع إجابات أفراد العينة حول مدى الاعتماد على زمن استرجاع



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يبين هذا الجدول توزيع الآراء حول تحديد زمن استرجاع الأنظمة، حيث تشير النتائج إلى أن (60%) يرون وجود "تطبيق فعال"، مقابل (20%) "جيد التطبيق" و(20%) "متوسط التطبيق". ويعكس ذلك مستوى مرتفعاً نسبياً في تحديد الزمن اللازم لاستعادة الأنظمة بعد الأعطال. ويتوافق هذا مع الشكل البياني ، حيث يبرز تفوق الفئة المرتفعة بشكل واضح، ومن الناحية العلمية، يُعتبر زمن الاسترجاع أحد المؤشرات الجوهرية لتقييم فعالية خطط التعافي. وبناءً على ذلك، يمكن القول إن البنوك محل الدراسة تمتلك مستوى جيداً من التحكم في زمن التعافي، الأمر الذي يدعم استمرارية الأعمال وتتوافق هذه النتيجة مع دراسة katarina kampova و katarina makka التي أكدت أن تحديد زمن الاسترجاع (RTO) بدقة يساعد المؤسسات على تحسين سرعة التعافي وتقليل الخسائر المرتبطة بالأزمات والانقطاعات التقنية. كما تنسجم هذه النتيجة مع دراسة

Kazimierz T. Kosmowski

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

التي أوضحت أن وجود خطط استرجاع واضحة ومحدثة باستمرار يعزز من قدرة المؤسسات على الحفاظ على استمرارية خدماتها في الظروف الطارئة.

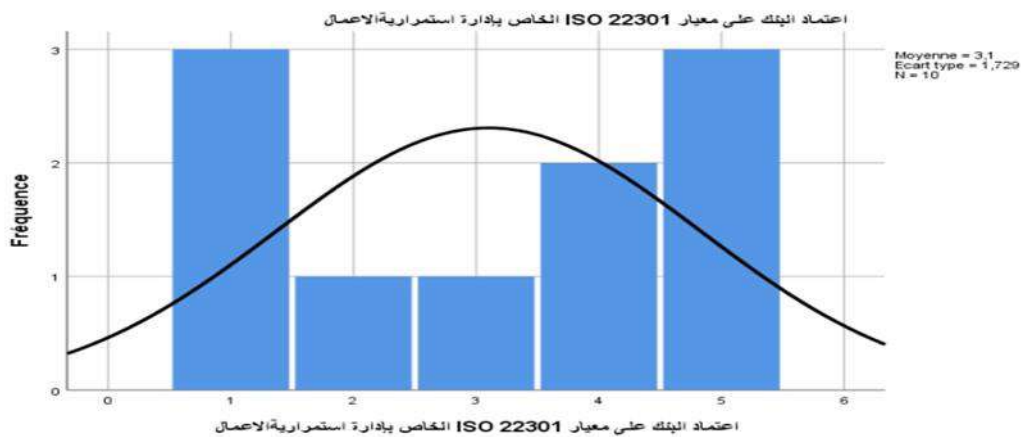
✓ معيار إدارة استمرارية الاعمال ISO 22301

الجدول 02-44 : توزيع إجابات أفراد العينة حول مدى الاعتماد على معيار إدارة استمرارية الاعمال ISO 22301

	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide				
غير موجود	3	30,0	30,0	30,0
ضعيف التطبيق	1	10,0	10,0	40,0
متوسط التطبيق	1	10,0	10,0	50,0
التطبيق جيد	2	20,0	20,0	70,0
تطبيق فعال	3	30,0	30,0	100,0
Total	10	100,0	100,0	

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الشكل 02-35 : توزيع إجابات أفراد العينة حول مدى الاعتماد على معيار إدارة استمرارية الاعمال ISO 22301



المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

يوضح هذا الجدول مدى اعتماد المؤسسات على معيار ISO 22301، حيث تكشف النتائج عن تباين ملحوظ إذ سجلت فئتا "غير موجود" و"تطبيق فعال" النسبة نفسها (30%) لكل منهما، تليهما فئة "جيد التطبيق" بنسبة (20%)، ثم فئتا "ضعيف" و"متوسط" بنسبة (10%) لكل منهما. ويعكس هذا التوزيع درجة من عدم التجانس في تبني هذا المعيار بين البنوك محل الدراسة. ويتجلى هذا التفاوت من خلال الشكل البياني، حيث تتوزع القيم على مختلف الفئات، بما يدل على اختلاف مستويات التطبيق من بنك إلى آخر. يُعد معيار ISO 22301 إطارًا مرجعيًا متقدمًا لإدارة استمرارية الأعمال، وعليه فإن غياب اعتماده بشكل متسق يشير إلى وجود فجوة تنظيمية وتباين في نضج الممارسات البنكية. وعليه يمكن الاستنتاج أن مستوى تطبيق هذا المعيار لا يزال محدودًا نسبيًا. وتتوافق هذه النتيجة مع دراسة أسماء عبد الرحمن الغامدي التي توصلت إلى أن تطبيق معيار ISO 22301 داخل المؤسسات لا يزال متفاوتًا وجزئيًا، رغم دوره في تحسين الأداء المؤسسي وتعزيز القدرة على مواجهة الأزمات. كما تنسجم هذه النتيجة مع دراسة خديجة يحيى العرياني وهناء علي الضحوي التي أكدت أن تطبيق هذا المعيار يمثل عنصرًا أساسيًا لضمان استمرارية العمليات وتقليل آثار الكوارث والاضطرابات. كذلك تدعمها دراسة Georg Sven Lampe التي أوضحت أن التكامل بين نظم أمن المعلومات وإدارة الاستمرارية وفق المعايير الدولية يعزز جاهزية المؤسسات وقدرتها على التعامل مع الأزمات بكفاءة أكبر.

الجدول 02-45 : يوضح متوسطات الحسابية والانحرافات المعيارية للاجابات افراد العينة حول إدارة استمرارية الاعمال

N	Moyenne	Ecart type
داخل البنك (DRP) وجود خطة تعافي من الكوارث	4,70	,483
تخصيص فرق مختصة لإدارة الازمات	4,60	,699
وجود إجراءات مكتوبة وواضحة للتعامل مع الازمات	4,50	,707
الاعتماد على سجل الكتروني للمخاطر	4,50	,527
(BCP) الاعتماد على خطة استمرارية الاعمال	4,50	,527

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

تقييم المخاطر بشكل دوري	10	4,40	,699
بشكل دقيق (RTO)تحديد زمن استرجاع	10	4,40	,843
الاستجابة للالزمات بسرعة وفعالية	10	4,10	,738
تحديث خطة استمرارية الاعمال بشكل دوري	10	4,10	,738
الخاص بإدارة ISO 22301اعتماد البنك على معيار استمراريةالاعمال	10	3,10	1,729
N valide (liste)	10		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يوضح هذا الجدول النتائج الإحصائية الوصفية الخاصة ببعء إدارة استمرارية الأعمال في البنوك محل الدراسة، وذلك من خلال المتوسطات الحسابية والانحرافات المعيارية لإجابات أفراد العينة. يتبين من النتائج أن أغلب المتوسطات الحسابية جاءت مرتفعة، حيث تراوحت بين (3.10) و(4.70)، وهو ما يدل على أن مستوى تطبيق ممارسات استمرارية الأعمال في البنوك محل الدراسة يُعد مرتفعًا بشكل عام. وقد سجلت أعلى قيمة متوسط حسابي في مؤشر خطة تعافي (DRP) داخل البنك بمتوسط قدره (4.70) وانحراف معياري منخفض نسبيًا (0.483)، مما يعكس درجة اتفاق عالية بين أفراد العينة حول أهمية وتطبيق هذه الممارسة بشكل فعال داخل البنوك. كما سجلت مؤشرات أخرى مثل فريق ادارة الأزمات و إجراءات الطوارئ و خطة استمرارية الأعمال (BCP) متوسطات مرتفعة تراوحت بين (4.50 و 4.60). في المقابل، سجل مؤشر معيار ISO 22301 أدنى متوسط حسابي (3.10) مع انحراف معياري مرتفع نسبيًا (1.729)، مما يدل على وجود تباين كبير في آراء أفراد العينة وضعف نسبي في تبني هذا المعيار الدولي بشكل رسمي داخل بعض البنوك. وحيث تعكس النتائج أن البنوك محل الدراسة تمتلك مستوى جيدًا من ممارسات استمرارية الأعمال، مع تفاوت في درجة الالتزام بالمعايير الدولية الحديثة.

ثالثا : عرض وتحليل المؤشرات الإحصائية الاجمالية للمتغيرات الدراسة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-46 : يوضح المتوسطات الحسابية والانحرافات المعيارية لمتغيري الدراسة

	N	Moyenne	Ecart type
مستوى امن نظام المعلومات في البنوك	10	4,5056	,30592
الاعمال في البنوك استمرارية	10	4,2900	,37253
N valide (liste)	10		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

يوضح هذا الجدول المتوسطات الحسابية والانحرافات المعيارية لكل من متغير "مستوى أمن نظام المعلومات في البنوك" ومتغير "إدارة استمرارية الأعمال في البنوك". حيث تشير النتائج إلى أن متوسط مستوى أمن نظام المعلومات بلغ (4.5056) بانحراف معياري منخفض (0.30592)، وهو ما يعكس مستوى مرتفعاً من إدراك وتطبيق ممارسات أمن المعلومات داخل البنوك محل الدراسة، مع تجانس واضح في إجابات أفراد العينة. أما بالنسبة لمتغير إدارة استمرارية الأعمال، فقد بلغ المتوسط الحسابي (4.2900) بانحراف معياري (0.37253)، وهو أيضاً مستوى مرتفع نسبياً، مما يدل على اهتمام البنوك محل الدراسة بتطبيق سياسات وإجراءات استمرارية الأعمال، وإن كان بدرجة أقل قليلاً مقارنة بأمن المعلومات. وبشكل عام ، تشير النتائج إلى أن كلا المتغيرين يتمتعان بمستويات تطبيق جيدة داخل البنوك محل الدراسة، مع تفوق نسبي لمتغير أمن نظام المعلومات، مما يعكس أولوية هذا الجانب في السياسات البنكية.

ربط الفرضيات :

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

أولاً: مستوى أمن نظام المعلومات في البنوك محل الدراسة

من خلال المتوسط العام لمتغير أمن نظام المعلومات المقدر بـ(4.5056) بانحراف معياري قدره (0.30592)، يتضح أن البنوك محل الدراسة تحقق مستوى مرتفعاً من أمن نظام المعلومات، وهو ما يعكس اهتمامها بتطبيق إجراءات وآليات حماية المعلومات بمختلف أبعادها مع وجود تجانس واضح في استجابات أفراد العينة.

مما يؤدي إلى قبول الفرضية التي تنص على أنه يتحقق مستوى مرتفع من أمن نظام المعلومات في البنوك محل الدراسة

ثانياً: مستوى استمرارية الأعمال في البنوك

من خلال المتوسط العام لمتغير إدارة استمرارية الأعمال المقدر بـ(4.2900) بانحراف معياري قدره (0.37253)، يتضح أن البنوك محل الدراسة تتمتع بمستوى مرتفع من تطبيق إدارة استمرارية الأعمال، كما يعكس الانحراف المعياري المنخفض وجود تقارب وتجانس في آراء أفراد العينة حول هذا المتغير.

مما يؤدي إلى قبول الفرضية التي تنص على أن البنوك محل الدراسة تتوفر على تطبيق فعال لإدارة استمرارية الأعمال.

استكمالاً لعرض وتحليل نتائج محاور الدراسة، ولغرض تعميق الفهم الإحصائي للبيانات الحصل عليها، سيتم في هذا الجزء التطرق إلى دراسة بعض الخصائص الإحصائية للمتغيرات محل الدراسة، وذلك من خلال عرض الإحصائيات الوصفية واختبار مدى خضوع البيانات للتوزيع الطبيعي، تمهيداً لتطبيق الأساليب الإحصائية المناسبة لدراسة العلاقة بين المتغيرات واختبار الفرضيات.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-47 : الإحصائيات الوصفية لمستوى أمن نظام المعلومات و ادارة استمرارية الأعمال حسب نوع البنك

نوع البنك		Statistiques	Erreur standard
مستوى امن نظام المعلومات في البنوك	عموم	Moyenne	4,4444
	ي	Intervalle de confiance à 95 % pour la moyenne	4,0027
		Borne inférieure	
		Borne supérieure	4,8861
		Moyenne tronquée à 5 %	4,4414
		Médiane	4,3889
		Variance	,127
		Ecart type	,35573
		Minimum	4,06
		Maximum	4,89
		Plage	,83
		Plage interquartile	,69
		Asymétrie	,267
		Kurtosis	-2,239
	خاص	Moyenne	4,5926
		Intervalle de confiance à 95 % pour la moyenne	3,7053
		Borne inférieure	
		Borne supérieure	5,4799
		Moyenne tronquée à 5 %	.
		Médiane	4,4444
		Variance	,128
		Ecart type	,35717

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

	Minimum		4,33		
	Maximum		5,00		
	Plage		,67		
	Plage interquartile		.		
	Asymétrie		1,545	1,225	
	Kurtosis		.	.	
	مختلط	Moyenne		4,5278	,13889
		Intervalle de confiance à 95 % pour la moyenne	Borne inférieure	2,7630	
			Borne supérieure	6,2925	
		Moyenne tronquée à 5 %		.	
		Médiane		4,5278	
		Variance		,039	
		Ecart type		,19642	
		Minimum		4,39	
		Maximum		4,67	
		Plage		,28	
	Plage interquartile		.		
	Asymétrie		.	.	
	Kurtosis		.	.	
	الاعمال في استمرارية البنوك	عمومي	Moyenne		4,2200
Intervalle de confiance à 95 % pour la moyenne			Borne inférieure	3,7280	
			Borne supérieure	4,7120	
Moyenne tronquée à 5 %			4,2278		
Médiane			4,4000		
Variance			,157		
Ecart type			,39623		
Minimum			3,70		
Maximum			4,60		
Plage			,90		
Plage interquartile			,75		

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

خاص	Moyenne	4,2333	,27285
	Intervalle de confiance à	Borne inférieure	3,0594
	95 % pour la moyenne	Borne supérieure	5,4073
	Moyenne tronquée à 5 %	.	.
	Médiane	4,4000	.
	Variance	,223	.
	Ecart type	,47258	.
	Minimum	3,70	.
	Maximum	4,60	.
	Plage	,90	.
	Plage interquartile	.	.
	Asymétrie	-1,390	1,225
	Kurtosis	.	.
مختلط	Moyenne	4,5500	,05000
	Intervalle de confiance à	Borne inférieure	3,9147
	95 % pour la moyenne	Borne supérieure	5,1853
	Moyenne tronquée à 5 %	.	.
	Médiane	4,5500	.
	Variance	,005	.
	Ecart type	,07071	.
	Minimum	4,50	.
	Maximum	4,60	.
	Plage	,10	.
	Plage interquartile	.	.
	Asymétrie	.	.
	Kurtosis	.	.

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

توضح النتائج الإحصائية الوصفية لمتغيري الدراسة حسب نوع البنك (عمومي، خاص، مختلط) وجود تقارب نسبي في المتوسطات الحسابية بين مختلف أنواع البنوك. فيما يتعلق بأمن نظام المعلومات، سجلت البنوك الخاصة متوسطاً أعلى نسبياً (4.5926) مقارنة بالبنوك العمومية (4.4444)، بينما جاءت البنوك المختلطة في مستوى متوسط (4.5278)، مما يشير إلى

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

تقارب في مستوى التطبيق مع تفوق طفيف للبنوك الخاصة. أما بالنسبة لاستمرارية الأعمال، فقد أظهرت النتائج تقارباً كبيراً بين البنوك العمومية والخاصة، حيث سجلت القيم (4.2200) و(4.2333) على التوالي، بينما سجلت البنوك المختلطة متوسطاً أعلى نسبياً (4.5500)، مع انحراف معياري منخفض جداً، مما يدل على تحانس كبير في الإجابات. وبشكل عام، تشير هذه النتائج إلى عدم وجود فروق جوهرية واضحة بين أنواع البنوك فيما يتعلق بتطبيق أمن نظام المعلومات واستمرارية الأعمال، مع وجود تباينات خفيفة غير مؤثرة إحصائياً..

الجدول 02-48 : نتائج اختبار التوزيع الطبيعي (Shapiro-Wilk و Kolmogorov-Smirnov)

Kolmogorov-Smirnov ^a				Shapiro-Wilk		
نوع البنك	Statistique s	ddl	Sig.	Statistique s	ddl	
عمومي مستوى امن نظام المعلومات في البنوك	,183	5	,200*	,935	5	
	خاص	,328	3	.	,871	3
	مختلط	,260	2	.		
عمومي الاعمال في استمرارية البنوك	,275	5	,200*	,879	5	
	خاص	,304	3	.	,907	3
	مختلط	,260	2	.		

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

ظهر نتائج اختبارات التوزيع الطبيعي أن قيم الدلالة الإحصائية في معظم الحالات تجاوزت مستوى (0.05)، لا سيما بالنسبة للبنوك العمومية، مما يدل على أن البيانات في هذا الصنف تتبع التوزيع الطبيعي. أما فيما يتعلق بالبنوك الخاصة والمختلطة، فقد سُجلت بعض القيم غير المكتملة، غير أن الاتجاه العام للنتائج لا يشير إلى وجود انحرافات جوهرية عن التوزيع الطبيعي. وبالاستناد إلى نتائج اختباري Kolmogorov-Smirnov test و Shapiro-Wilk test، يمكن الاستنتاج أن

بيانات الدراسة تحقق بدرجة كبيرة شرط الاعتدال في التوزيع

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-49 : الإحصائيات الوصفية لمتغيرات الدراسة حسب حجم المؤسسة

حجم المؤسسة			Statistiques	Erreur standard
مستوى امن نظام المعلومات في البنوك	كبير	Moyenne	4,5185	,12228
		Intervalle de confiance à 95 % pour la moyenne	4,2042	
		Borne inférieure		
		Borne supérieure	4,8328	
		Moyenne tronquée à 5 %	4,5237	
		Médiane	4,5278	
		Variance	,090	
		Ecart type	,29952	
		Minimum	4,06	
		Maximum	4,89	
		Plage	,83	
		Plage interquartile	,46	
		Asymétrie	-,459	,845
		Kurtosis	-,377	1,741
	صغير	Moyenne	4,5370	,24498
		Intervalle de confiance à 95 % pour la moyenne	3,4830	
		Borne inférieure		
		Borne supérieure	5,5911	
		Moyenne tronquée à 5 %	.	
		Médiane	4,4444	
		Variance	,180	
		Ecart type	,42431	
		Minimum	4,17	
		Maximum	5,00	
		Plage	,83	
		Plage interquartile	.	
		Asymétrie	,935	1,225
		Kurtosis	.	.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الاعمال في استمرارية البنوك	كبير	Moyenne	4,3000	,16125
		Intervalle de confiance à 95 % pour la moyenne	Borne inférieure	3,8855
			Borne supérieure	4,7145
		Moyenne tronquée à 5 %		4,3167
		Médiane		4,5000
		Variance		,156
		Ecart type		,39497
		Minimum		3,70
		Maximum		4,60
		Plage		,90
	صغير	Plage interquartile		,75
		Asymétrie	-1,022	,845
		Kurtosis	-1,228	1,741
		Moyenne	4,4667	,06667
		Intervalle de confiance à 95 % pour la moyenne	Borne inférieure	4,1798
			Borne supérieure	4,7535
		Moyenne tronquée à 5 %		.
		Médiane		4,4000
		Variance		,013
		Ecart type		,11547
		Minimum		4,40
		Maximum		4,60
		Plage		,20
		Plage interquartile		.
		Asymétrie	1,732	1,225
		Kurtosis		.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

	Minimum	3,70	
	Maximum	4,60	
	Plage	,90	
	Plage interquartile	,75	
	Asymétrie	-1,022	,845
	Kurtosis	-1,228	1,741
صغير	Moyenne	4,4667	,06667
	Intervalle de confiance à 95 % pour la moyenne	Borne inférieure	4,1798
		Borne supérieure	4,7535
	Moyenne tronquée à 5 %	.	
	Médiane	4,4000	
	Variance	,013	
	Ecart type	,11547	
	Minimum	4,40	
	Maximum	4,60	
	Plage	,20	
	Plage interquartile	.	
	Asymétrie	1,732	1,225
	Kurtosis	.	.

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تشير النتائج إلى وجود تقارب كبير في المتوسطات الحسابية بين المؤسسات الكبيرة والصغيرة فيما يتعلق بكل من أمن نظام المعلومات واستمرارية الأعمال. بالنسبة لأمن نظام المعلومات، سجلت المؤسسات الكبيرة متوسطاً قدره (4.5185)، بينما سجلت المؤسسات الصغيرة (4.5370)، مما يدل على تقارب شديد في مستوى التطبيق بين الفئتين. فيما يتعلق باستمرارية الأعمال، سجلت البنوك الكبيرة متوسطاً قدره (4.3000)، مقابل (4.4667) للبنوك الصغيرة، وهو ما يشير إلى تفوق صغير لصالح البنوك الصغيرة، مع ملاحظة درجة عالية من التجانس في استجابات أفراد العينة. وبشكل عام ، لا تُظهر النتائج وجود فروق ذات دلالة واضحة تُعزى إلى حجم المؤسسة فيما يتعلق بمستوى تطبيق أمن المعلومات واستمرارية الأعمال، مما يشير إلى

تقارب الممارسات بين مختلف فئات البنوك المدروسة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-50 : نتائج اختبار التوزيع الطبيعي (Kolmogorov-Smirnov و Shapiro-Wilk)

		Kolmogorov-Smirnov ^a			Shapiro-Wilk
		Statistiqu	ddl	Sig.	Statistiqu
حجم	المؤسسة	es			es
كبير	مستوى امن نظام	,190	6	,200*	,953
صغير	المعلومات في البنوك	,253	3	.	,964
كبير	الاعمال في استمرارية	,360	6	,014	,770
صغير	البنوك	,385	3	.	,750

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تُظهر نتائج اختبارات Kolmogorov-Smirnov و Shapiro-Wilk الخاصة بتوزيع البيانات حسب حجم المؤسسة (كبير/صغير) أن أغلب قيم الدلالة الإحصائية كانت أعلى من (0.05)، خصوصًا بالنسبة لمتغير أمن نظام المعلومات في المؤسسات الكبيرة والصغيرة، مما يشير إلى أن البيانات تتبع التوزيع الطبيعي في هذا المتغير. وكم جهة أخرى يظهر متغير إدارة استمرارية الأعمال بعض الانحراف عن التوزيع الطبيعي في البنوك الكبيرة، حيث بلغت قيمة الدلالة (0.014) في اختبار Kolmogorov-Smirnov، وهي أقل من (0.05)، مما يدل على عدم تحقق شرط التوزيع الطبيعي في هذا الجزء من البيانات. أما البنوك الصغيرة فقد لم تُسجل قيم دالة بشكل كافٍ بسبب صغر حجم العينة، إلا أن الاتجاه العام يشير إلى اقتراب البيانات من التوزيع الطبيعي. وبناءً على هذه النتائج، يمكن القول إن شرط التوزيع الطبيعي متحقق جزئيًا،

المطلب الثاني : عرض وتحليل نتائج اختبار فرضيات الدراسة

في إطار هذه الدراسة، سيتم العمل على الإجابة عن الإشكالية الرئيسية والتساؤلات الفرعية المتعلقة بدور أمن نظام المعلومات في دعم إدارة استمرارية الأعمال في البنوك محل الدراسة. ولتحقيق ذلك، سيتم الاعتماد على مجموعة من الأساليب الإحصائية التي تسمح بقياس طبيعة وقوة العلاقة بين المتغيرات المدروسة، وفي مقدمتها معامل الارتباط الخطي

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

لبيرسون. ويُعد هذا المعامل من أهم الأدوات الإحصائية المستخدمة في تحليل العلاقات بين المتغيرات، حيث يوضح اتجاه العلاقة (موجبة أو سالبة) إضافة إلى درجة قوتها، إذ تتراوح قيمته بين (-1) و $(+1)$ ، بحيث تشير القيم الموجبة إلى علاقة طردية، بينما تشير القيم السالبة إلى علاقة عكسية. كما أن القيم القريبة من الحدين الأعلى أو الأدنى تعكس قوة العلاقة بين المتغيرات، في حين أن القيم القريبة من الصفر تدل على ضعفها أو عدم وجودها. ورغم أهمية هذا المعامل في تحليل العلاقات، إلا أنه من الضروري التحقق من دلالة الإحصائية قبل الاعتماد على نتائجه، لضمان دقة التفسير وموضوعية النتائج.

الجدول 51-02 : مصفوفة الارتباط لابعاد امن نظام المعلومات

توافر المعلومات	سلامة المعلومات	سرية المعلومات		
سرية المعلومات	Corrélation de Pearson	1	,655*	,179
	Sig. (bilatérale)		,040	,621
	N	10	10	10
سلامة المعلومات	Corrélation de Pearson	,655*	1	,675*
	Sig. (bilatérale)	,040		,032
	N	10	10	10
توافر المعلومات	Corrélation de Pearson	,179	,675*	1
	Sig. (bilatérale)	,621	,032	
	N	10	10	10
الاعمال في استمرارية البنوك	Corrélation de Pearson	,040	,274	,401
	Sig. (bilatérale)	,913	,443	,251
	N	10	10	10

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

توضح نتائج مصفوفة الارتباط وجود علاقات ارتباطية متفاوتة بين أبعاد أمن نظام المعلومات (سرية المعلومات، سلامة المعلومات، توافر المعلومات). حيث سجلت العلاقة بين سرية المعلومات وسلامة المعلومات معامل ارتباط موجب ($r = 0.655$) وهو دال إحصائيًا عند مستوى (0.05)، مما يدل على وجود علاقة طردية قوية نسبيًا بين البعدين، أي أنه كلما ارتفع مستوى سرية المعلومات ارتفع مستوى سلامتها. و سجلت العلاقة بين سلامة المعلومات وتوافر المعلومات معامل ارتباط ($r = 0.675$) وهو أيضًا دال إحصائيًا، مما يعكس وجود ترابط قوي بين هذين البعدين. في المقابل، لم تسجل العلاقة بين سرية المعلومات وتوافر المعلومات دلالة أو ($p = 0.621$)، مما يشير إلى ضعف أو غياب العلاقة بينهما. أما فيما يتعلق بعلاقة أبعاد أمن نظام المعلومات مع استمرارية الأعمال، فقد كانت معاملات الارتباط ضعيفة جدًا، حيث لم تتجاوز القيم (0.274)، مما يدل على أن العلاقة بين الأبعاد الفرعية لأمن المعلومات واستمرارية الأعمال ليست مباشرة أو قوية في هذه البنوك.

اختبار الفرضيات

وبناءً على ذلك، يتم رفض الفرضيات التي تنص على وجود علاقة ارتباطية دالة بين كل من سرية المعلومات وسلامة المعلومات وتوافر المعلومات مع إدارة استمرارية الأعمال في البنوك محل الدراسة، وذلك لعدم تحقق الدلالة الإحصائية المطلوبة رغم وجود اتجاهات ارتباطية موجبة ضعيفة

الجدول 02-52 : مصفوفة الارتباط للمتغيرات الدراسة

مستوى امن نظام المعلومات		الاعمال في البنوك استمرارية	
في البنوك			
البنوك	Corrélation de Pearson	1	,293
	Sig. (bilatérale)		,411
	N	10	10
الاعمال في البنوك استمرارية	Corrélation de Pearson	,293	1
	Sig. (bilatérale)	,411	
	N	10	10

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

تُظهر نتائج مصفوفة الارتباط بين المتغيرين الرئيسيين للدراسة، والمتمثلين في أمن نظام المعلومات وإدارة استمرارية الأعمال إلا أنّ هذه العلاقة لم تكن ذات دلالة، ($r = 0.293$) في البنوك، وجود علاقة ارتباط موجبة ضعيفة، حيث بلغ معامل الارتباط ويشير ذلك إلى وجود اتجاه طردي ضعيف بين المتغيرين، غير أنّه لا يمكن الاعتماد عليه في تفسير ($p = 0.411$) إحصائية التأثير المباشر لأمن نظام المعلومات على إدارة استمرارية الأعمال ضمن عينة الدراسة. وبناءً على ذلك، يمكن الاستنتاج أنّ أمن نظام المعلومات لا يُظهر تأثيراً مباشراً ذا دلالة إحصائية قوية على إدارة استمرارية الأعمال في البنوك محل الدراسة، رغم وجود اتجاه عام يعكس علاقة إيجابية بين المتغيرين.

اختبار الفرضيات

بناءً على نتائج التحليل يتم: رفض الفرضية الصفرية التي تنص على وجود علاقة قوية ودالة إحصائية بين أمن نظام المعلومات واستمرارية الأعمال. وفي المقابل، يتم قبول الفرضية البديلة التي تفترض عدم وجود علاقة ذات دلالة إحصائية قوية بين المتغيرين.

وعليه، يمكن الاستنتاج أن أمن نظام المعلومات لا يُظهر تأثيراً مباشراً قوياً على استمرارية الأعمال في البنوك محل الدراسة، رغم وجود علاقة إيجابية ضعيفة

في هذه النقطة، سيتم التطرق إلى دراسة الفروق في إجابات أفراد العينة وفقاً لخصائص البنوك محل الدراسة، والمتمثلة في نوع و حجم البنك، وذلك من خلال الاعتماد على مجموعة من الاختبارات الإحصائية المناسبة، مثل اختبار (T-Test) لعينتين مستقلتين، وتحليل التباين الأحادي (ANOVA)، بالإضافة إلى اختبار (Kruskal-Wallis) بهدف الكشف عن مدى وجود فروق ذات دلالة إحصائية بين هذه الفئات.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-53 : الاحصائيات الوصفية لمستوى امن نظام المعلومات و إدارة استمرارية الاعمال حسب نوع البنك

N	نوع البنك	Moyenne	Ecart type	Moyenne erreur standard
5	عمومي مستوى امن نظام المعلومات في البنوك	4,4444	,35573	,15909
3	خاص	4,5926	,35717	,20621
5	عمومي الاعمال في البنوك استمرارية	4,2200	,39623	,17720
3	خاص	4,2333	,47258	,27285

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

الجدول 02-54 : نتائج اختبار Test T لقياس الفروق حسب نوع البنك

Test de Levene sur l'égalité des variances		Test t pour égalité des moyennes	
	F	Sig	t
مستوى امن نظام المعلومات في البنوك	Hypothèse de variances égales	,027	,874
	Hypothèse de variances inégales		-,569
الاعمال في استمرارية البنوك	Hypothèse de variances égales	,033	,862
			-,043

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

Hypothèse de variances inégales		-,041
------------------------------------	--	-------

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تُظهر نتائج اختبار (T-Test) لعينتين مستقلتين عدم وجود فروق ذات دلالة إحصائية بين البنوك العمومية والخاصة فيما يتعلق بكل من أمن نظام المعلومات و إدارة استمرارية الأعمال. حيث قدرت قيمة الدلالة الإحصائية في اختبار ليفين (Sig = 0.874 و 0.862)، وهي أكبر من (0.05)، مما يدل على تجانس التباينات بين المجموعات. كما أن قيم اختبار (t) لم تكن دالة إحصائية، حيث لم تتجاوز القيم الحرجة، مما يعني عدم وجود فروق معنوية بين متوسطات البنوك العمومية والخاصة. ومنه ، يمكن استنتاج أن نوع البنك لا يؤثر بشكل جوهري على مستوى تطبيق أمن نظام المعلومات أو إدارة استمرارية الأعمال.

اختبار الفرضيات :

بناءً على نتائج التحليل الوصفي ونتائج اختبار (T-Test)، يتبين عدم وجود فروق ذات دلالة إحصائية بين البنوك العمومية والخاصة فيما يتعلق بكل من أمن نظام المعلومات وإدارة استمرارية الأعمال.

وعليه، يتم قبول الفرضية الصفرية التي تنص على أنه: لا توجد فروق ذات دلالة إحصائية بين البنوك العمومية والخاصة في مستوى أمن نظام المعلومات وإدارة استمرارية الأعمال.

وبالتالي، يمكن استنتاج أن نوع البنك لا يؤثر بشكل جوهري على مستوى تطبيق المتغيرين في البنوك محل الدراسة.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

الجدول 02-55 : تحليل التباين الأحادي (ANOVA) الخاص بامن نظام المعلومات

	Somme des carrés	ddl	Carré moyen	F	Sig.
Intergroupes	,034	2	,017	,146	5,867
Intragroupes	,809	7	,116		
Total	,842	9			

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

تُظهر نتائج تحليل (ANOVA) الخاصة بأمن نظام المعلومات حسب نوع البنك عدم وجود فروق ذات دلالة إحصائية بين المجموعات. حيث بلغت قيمة ($F = 0.146$) مع مستوى دلالة ($\text{Sig} = 0.867$)، وهي قيمة أكبر من 0.05، مما يشير إلى عدم وجود فروق معنوية بين البنوك حسب هذا المتغير. وبالتالي، يمكن القول إن اختلاف نوع البنك لا يؤدي إلى اختلاف في مستوى أمن نظام المعلومات، مما يعكس تجانساً في السياسات والإجراءات الأمنية بين المؤسسات البنكية محل الدراسة.

اختبار فرضيات

بناءً على نتائج اختبار (ANOVA)، يمكن استنتاج ما يلي:

يتم قبول الفرضية الصفرية التي تنص على أنه لا توجد فروق ذات دلالة إحصائية في مستوى إدارة استمرارية الاعمال حسب نوع البنك. ويتم رفض الفرضية البديلة التي تفترض وجود فروق بين البنوك (عمومي، خاص، مختلط) في مستوى إدارة

استمرارية الاعمال

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

وعليه، يمكن القول إن اختلاف نوع البنك لا يؤثر بشكل جوهري على مستوى أمن نظام المعلومات في البنوك محل الدراسة، مما يعكس تجانساً في السياسات والإجراءات الأمنية المعتمدة بين مختلف المؤسسات البنكية

الجدول 02-56 : اختبار Kruskal-Wallis

Récapitulatif du test Kruskal-Wallis pour échantillons indépendants

N total	10
Statistiques de test	2,027 ^{a,b}
Degré de liberté	2
Sig. asymptotique (test bilatéral)	,363

المصدر : من اعداد الطالبتين بناء على مخرجات SPSS

توضح نتائج اختبار Kruskal-Wallis عدم وجود فروق ذات دلالة إحصائية بين الفئات ، حيث بلغت قيمة الدلالة (Sig = 0.363)، وهي أكبر من (0.05). وبناءً عليه، يمكن استنتاج أن الفروق بين المجموعات المدروسة ليست جوهريّة، وأن مستوى أمن نظام المعلومات و إدارة استمرارية الأعمال متقارب بين مختلف الفئات.

اختبار الفرضيات

بناءً على نتائج اختبار Kruskal-Wallis يتم: قبول الفرضية الصفرية التي تنص على عدم وجود فروق ذات دلالة إحصائية بين المجموعات المدروسة. رفض الفرضية البديلة التي تفترض وجود فروق معنوية بين الفئات. وعليه، يمكن الاستنتاج أن مستوى

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

أمن نظام المعلومات واستمرارية الأعمال لا يختلف باختلاف الفئات محل الدراسة، مما يشير إلى تجانس عام في إدراك وتطبيق هذه المتغيرات داخل البنوك محل الدراسة

المطلب الثالث : مناقشة نتائج الدراسة

بعد تحليل الاستبيان واختبار فرضيات الدراساتنا بالاساليب الإحصائية الموائمة ، توصلنا إلى النتائج التالية:

أولا : فيما يخص واقع متغيرات الدراسة

كما تطرقنا سابقا فإن متغيرات الدراساتنا أمن نظام المعلومات كمتغير مستقل و إدارة استمرارية الاعمال

كمتغير تابع.

1. مستوى أمن نظام المعلومات في البنوك على مستوى ولاية ورقلة

✧ البعد سرية المعلومات

أظهرت نتائج الدراسة أن بُعد سرية المعلومات سجل أعلى متوسط حسابي ضمن أبعاد أمن نظام المعلومات، حيث بلغ (4.5333)، وهو ما يعكس المستوى المرتفع من الاهتمام الذي توليه البنوك محل الدراسة لحماية المعلومات والبيانات الحساسة. وتُبرز هذه النتيجة إدراك المؤسسات البنكية لأهمية السرية باعتبارها أحد الركائز الأساسية للأمن المعلوماتي، خاصة في ظل طبيعة النشاط البنكي الذي يعتمد بشكل كبير على تداول البيانات المالية والشخصية للزبائن.

كما يبيّن تحليل المؤشرات المرتبطة بهذا البعد أن البنوك تعتمد بدرجة عالية على مجموعة من الإجراءات والتدابير الأمنية، من بينها سياسات أمن المعلومات، واستخدام كلمات المرور، وآليات التحكم في الوصول إلى البيانات والأنظمة، حيث حققت هذه المؤشرات مستويات تطبيق مرتفعة، ما يدل على وجود وعي تنظيمي وتقني بأهمية الحد من الوصول غير المصرح به وحماية المعلومات من التسريب أو الاختراق. ومن جهة أخرى، أظهرت بعض المؤشرات المتعلقة بالتشفير وآليات التحكم في الوصول وجود تباين

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

نسبي بين البنوك، وهو ما يمكن تفسيره باختلاف الإمكانيات التقنية ومستوى الاستثمار في البنية التحتية الرقمية، إضافة إلى تفاوت السياسات والإجراءات المعتمدة من مؤسسة إلى أخرى. ومع ذلك، فإن هذا التباين لا يؤثر على الاتجاه العام للنتائج، والذي يعكس مستوى إيجابياً ومرتفعاً في تطبيق متطلبات سرية المعلومات. ويمكن تفسير هذه النتائج بكون القطاع البنكي من أكثر القطاعات تعرضاً للمخاطر السيبرانية ومحاولات الاختراق، الأمر الذي يدفع المؤسسات البنكية إلى تشديد إجراءات الحماية وتعزيز أنظمة الأمن المعلوماتي حفاظاً على ثقة العملاء وضمان استمرارية الخدمات البنكية دون اضطرابات. كما أن الالتزام بالمعايير والإجراءات التنظيمية المتعلقة بحماية البيانات ساهم بدوره في رفع مستوى الاهتمام بسرية المعلومات داخل هذه البنوك. وبناءً على ما سبق، يمكننا القول إن البنوك محل الدراسة تتمتع بمستوى مرتفع من تطبيق ممارسات سرية المعلومات، وهو ما يعكس توجهًا واضحًا نحو تعزيز حماية البيانات وتقليل مخاطر التسريب والاختراق، رغم استمرار وجود بعض الفروقات البسيطة في مستوى تطبيق بعض الجوانب التقنية بين بنك وأخرى.

✧ البعد سلامة المعلومات

أظهرت النتائج أن بعد سلامة المعلومات جاء في المرتبة الثانية بمتوسط (4.5167)، وهو مستوى مرتفع أيضاً، مما يعكس اهتماماً واضحاً من طرف البنوك بالحفاظ على دقة وصحة البيانات. وتشير النتائج التفصيلية إلى أن مؤشرات مثل سجلات التدقيق، كشف التلاعب، والتحقق من صحة البيانات حققت مستويات تطبيق مرتفعة، وهو ما يدل على وجود أنظمة رقابة فعالة داخل البنوك. في المقابل، سجلت بعض المؤشرات مثل أنظمة التنبيه الأمني وتوزيع الصلاحيات تفاوتاً نسبياً، ما يعكس أن هذا الجانب لا يزال بحاجة إلى تطوير أكبر. ويمكن تفسير هذه النتائج بأن البنوك تعتمد بشكل كبير على آليات المراقبة الداخلية والتدقيق لضمان سلامة المعلومات، باعتبار أن أي خطأ في البيانات قد يؤثر مباشرة على القرارات المالية والإدارية. وعليه، يمكن استنتاج أن سلامة المعلومات داخل البنوك محل الدراسة في مستوى جيد جداً، مع قابلية للتحسين في بعض الآليات التقنية المتقدمة.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

✧ البعد توافر المعلومات

أظهرت نتائج الدراسة أن بُعد توافر المعلومات حقق متوسطاً حسابياً مرتفعاً بلغ (4.4667)، وهو ما يعكس حرص البنوك محل الدراسة على ضمان استمرارية الوصول إلى المعلومات والأنظمة في مختلف الظروف. وتُعد هذه النتيجة مؤشراً إيجابياً على فعالية البنية التحتية التقنية المعتمدة، ومدى اهتمام المؤسسات البنكية بتوفير المعلومات للمستخدمين المصرح لهم في الوقت المناسب دون انقطاع. كما بينت النتائج أن مؤشرات النسخ الاحتياطي للبيانات، واسترجاع المعلومات عند الطوارئ، إضافة إلى مراقبة الأنظمة والشبكات، سجلت مستويات تطبيق مرتفعة جداً، وهو ما يدل على اعتماد البنوك على آليات تقنية متطورة تهدف إلى حماية البيانات من الضياع وضمان استمرارية الخدمات البنكية. ويعكس ذلك كذلك وجود وعي متزايد بأهمية إدارة المخاطر التقنية وتفاذي الآثار السلبية للأعطال أو الهجمات الإلكترونية. وفي المقابل، أظهرت بعض المؤشرات المتعلقة بإدارة الصيانة واستمرارية الخدمة مستويات أقل نسبياً مقارنة ببقية العبارات، وهو ما قد يشير إلى وجود تفاوت في كفاءة الجوانب التشغيلية أو الحاجة إلى تطوير خطط الصيانة الدورية وتحسين سرعة الاستجابة للأعطال التقنية. كما يمكن تفسير هذا التفاوت باختلاف الإمكانيات التقنية والتنظيمية بين البنوك محل الدراسة. ومن الناحية التفسيرية، فإن الارتفاع المسجل في هذا البعد يعكس اعتماد البنوك على نظم معلومات متقدمة وبنية رقمية قوية تساهم في ضمان استمرارية الأعمال وتقليل مخاطر فقدان البيانات أو توقف الخدمات. كما أن طبيعة النشاط البنكي، الذي يعتمد على التدفق المستمر للمعلومات والمعاملات الإلكترونية، تفرض على المؤسسات البنكية توفير أنظمة عالية الجاهزية والكفاءة. وبناءً على هذه النتائج، يمكن القول إن مستوى توافر المعلومات داخل البنوك محل الدراسة يُعد مرتفعاً بشكل عام، وهو ما يساهم بصورة مباشرة في دعم استمرارية النشاط البنكي وتعزيز قدرة المؤسسات على تقديم خدماتها بكفاءة واستقرار، رغم الحاجة إلى مزيد من التحسين في بعض الجوانب التشغيلية المرتبطة بالصيانة واستمرارية الخدمة.

2. مستوى إدارة استمرارية الاعمال البنوك على مستوى ولاية ورقلة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

أظهرت نتائج الدراسة أن مستوى تطبيق إدارة استمرارية الأعمال في البنوك محل الدراسة جاء مرتفعاً، وهو ما تؤكدته المتوسطات الحسابية المرتفعة لمعظم المؤشرات، حيث بلغ المتوسط العام للمتغير (4.2900) بانحراف معياري منخفض، مما يعكس اتفاق أفراد العينة على وجود اهتمام واضح بضمان استمرارية الأنشطة والخدمات أثناء الأزمات. وتدل هذه النتيجة على إدراك البنوك لأهمية استمرارية الأعمال باعتبارها عنصراً أساسياً للحفاظ على الاستقرار التشغيلي وتقليل آثار المخاطر والاضطرابات. وقد سجل مؤشر خطة التعافي من الكوارث أعلى متوسط حسابي، وهو ما يعكس اهتمام البنوك باسترجاع الأنظمة والبيانات بسرعة بعد الأعطال أو الأزمات، خاصة في ظل الاعتماد الكبير على الأنظمة المعلوماتية في تقديم الخدمات البنكية. كما أظهرت النتائج ارتفاع مستوى الاعتماد على فرق إدارة الأزمات، مما يدل على أهمية العنصر البشري المؤهل في التعامل مع الحالات الطارئة واتخاذ القرارات المناسبة في الوقت المناسب. كما بينت النتائج أن البنوك تعتمد بدرجة مرتفعة على إجراءات الطوارئ وخطط استمرارية الأعمال، وهو ما يعكس وجود تنظيم وإجراءات واضحة تساعد على مواجهة الأزمات وتقليل حالة الارتباك أثناء حدوثها. إضافة إلى ذلك، أظهرت مؤشرات مراجعة الخطط وتقييم المخاطر وسجل المخاطر مستويات جيدة من التطبيق، مما يشير إلى وجود توجه نحو التحسين المستمر والتخطيط الاستباقي لمواجهة التهديدات المحتملة. أما فيما يتعلق بزمان الاستجابة وزمان الاسترجاع، فقد أظهرت النتائج مستويات جيدة وفعالة نسبياً، وهو ما يعكس قدرة البنوك على التعامل مع الأزمات واستعادة الأنظمة والخدمات خلال فترات زمنية مقبولة، رغم وجود تفاوت بسيط بين البنوك في سرعة الاستجابة والجاهزية. في المقابل، سجل مؤشر معيار ISO 22301 أدنى متوسط مقارنة ببقية المؤشرات، مما يدل على وجود تفاوت بين البنوك في تبني هذا المعيار الدولي، حيث أن بعض البنوك تطبق ممارسات استمرارية الأعمال دون الاعتماد الرسمي على المعيار، بينما لا تزال بنوك أخرى في مراحل محدودة من تطبيقه. وبصفة عامة، تؤكد نتائج الدراسة أن البنوك محل الدراسة تتمتع بمستوى مرتفع نسبياً من تطبيق إدارة استمرارية الأعمال، خاصة فيما يتعلق بخطط التعافي وإدارة الأزمات والإجراءات التنظيمية، مع بقاء الحاجة إلى تعزيز الاعتماد على المعايير الدولية الحديثة لضمان مزيد من التكامل والفعالية في إدارة استمرارية الأعمال.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

ثانيا : مناقشة النتائج المتعلقة بالعلاقة بين متغيري الدراسة والفروق حسب خصائص البنوك

1. مناقشة العلاقات الارتباطية بين متغيري الدراسة

تشير النتائج المتوصل إليها إلى وجود علاقة ارتباطية موجبة ضعيفة بين متغير أمن نظام المعلومات ومتغير إدارة استمرارية الأعمال في البنوك محل الدراسة، حيث بلغ معامل الارتباط ($r = 0.293$)، غير أن هذه العلاقة لم تكن ذات دلالة إحصائية، إذ بلغت قيمة الدلالة ($\text{Sig} = 0.411$)، وهي قيمة أكبر من مستوى الدلالة المعتمد (0.05). ويعكس ذلك وجود اتجاه طردي ضعيف بين المتغيرين، إلا أن هذا الاتجاه لا يسمح بإثبات وجود تأثير مباشر وقوي لأمن نظام المعلومات على إدارة استمرارية الأعمال داخل البنوك محل الدراسة. كما أظهرت نتائج مصفوفة الارتباط الخاصة بأبعاد أمن نظام المعلومات وجود تفاوت في طبيعة العلاقات بين الأبعاد الثلاثة، حيث سجلت العلاقة بين سرية المعلومات وسلامة المعلومات معامل ارتباط موجب متوسط ودال إحصائياً ($r = 0.655$)، وهو ما يدل على وجود تكامل واضح بين حماية سرية البيانات والمحافظة على سلامتها. كذلك سجلت العلاقة بين سلامة المعلومات وتوافر المعلومات معامل ارتباط موجب متوسط ($r = 0.675$)، مما يعكس الترابط بين سلامة الأنظمة وضمان استمرارية الوصول إلى المعلومات والخدمات البنكية. في المقابل، لم تظهر علاقة ذات دلالة إحصائية بين سرية المعلومات وتوافر المعلومات، وهو ما قد يشير إلى اختلاف أولويات التطبيق بين الجوانب الأمنية داخل بعض البنوك. ويمكن تفسير ضعف العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال بعدة عوامل محتملة، من بينها أن البنوك محل الدراسة قد تتعامل مع إدارة استمرارية الأعمال باعتبارها منظومة مستقلة نسبياً لا ترتبط فقط بالجوانب التقنية والأمنية، بل تشمل أيضاً الجوانب التنظيمية والإدارية والبشرية. فنجاح استمرارية الأعمال لا يعتمد فقط على حماية المعلومات، وإنما يرتبط كذلك بوجود خطط تعافٍ، وفرق لإدارة الأزمات، وإجراءات للطوارئ، وآليات لاتخاذ القرار أثناء الأزمات، وهي عناصر قد تُطبق بدرجات متفاوتة بغض النظر عن مستوى أمن نظام المعلومات. كما يمكن تفسير هذه النتيجة بكون البنوك محل الدراسة تركز بدرجة أكبر على الجوانب التشغيلية الأساسية لأمن نظام المعلومات، مثل النسخ الاحتياطي وكلمات المرور وتأمين قواعد البيانات، في حين أن التكامل الشامل بين أمن نظام المعلومات وإدارة استمرارية الأعمال وفق المعايير الدولية لا يزال محدوداً نسبياً، وهو ما ظهر من

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

خلال انخفاض مستوى الاعتماد على معيار ISO 22301 مقارنة ببقية المؤشرات. إضافة إلى ذلك، قد يرجع ضعف العلاقة الإحصائية إلى طبيعة العينة وصغر حجمها، حيث أن محدودية عدد البنوك قد تؤثر على قوة العلاقات الإحصائية بين المتغيرات، رغم وجود مؤشرات عملية تعكس اهتمام البنوك بكل من أمن نظام المعلومات و إدارة استمرارية الأعمال بشكل منفصل. كما يمكن أن يعكس ذلك تقارب السياسات البنكية المعتمدة، خاصة في ظل خضوع البنوك لتعليمات تنظيمية موحدة تتعلق بحماية الأنظمة و ضمان استمرارية الخدمات. بناءً على هذه النتائج، يمكن القول إن البنوك محل الدراسة تمتلك مستوى مرتفعاً نسبياً من أمن نظام المعلومات ومستوى جيداً من إدارة استمرارية الأعمال، إلا أن العلاقة المباشرة بين المتغيرين لم تظهر بصورة قوية ودالة إحصائية، وهو ما يدل على أن إدارة استمرارية الأعمال داخل البنوك لا تتحدد فقط بمدى قوة أمن نظام المعلومات، بل تتأثر أيضاً بعوامل تنظيمية وإدارية وتقنية أخرى تساهم مجتمعة في تعزيز قدرة المؤسسة على مواجهة الأزمات و ضمان استمرارية نشاطها تتفق نتائج الدراسة الحالية، التي أظهرت وجود علاقة ارتباطية موجبة ضعيفة وغير دالة إحصائية بين أمن نظام المعلومات وإدارة استمرارية الأعمال، مع عدد من الدراسات السابقة التي أكدت أن استمرارية الأعمال لا ترتبط فقط بالجوانب التقنية لأمن نظام المعلومات، وإنما تتأثر أيضاً بعوامل تنظيمية وإدارية وبشرية متعددة. فقد أشارت دراسة Piotr Jedynak (2013) إلى أن إدارة استمرارية الأعمال تعد مفهوماً إدارياً واستراتيجياً شاملاً يتجاوز مجرد حماية الأنظمة التقنية، ويرتبط بالتخطيط وإدارة المخاطر والاستجابة للأزمات، وهو ما يفسر ضعف العلاقة المباشرة بين المتغيرين في الدراسة الحالية. كما تتوافق هذه النتيجة مع دراسة Marko Niemimaa (2015) التي أكدت أن استمرارية نظم المعلومات تعتمد على مجموعة من العوامل الاجتماعية والتنظيمية والتكنولوجية مجتمعة، وأن غياب التكامل الكامل بين هذه العناصر قد يؤدي إلى ضعف الترابط بين أمن المعلومات واستمرارية الأعمال. وهو ما يتوافق مع دراسة حليمي نبيل وآخرون (2022) التي أكدت أن حماية المعلومات تقوم أساساً على ضمان السرية والسلامة والتوافر باعتبارها عناصر مترابطة ومتكاملة داخل النظام المعلوماتي. كما تتفق هذه النتائج مع دراسة Adam A. Semlambo وآخرون (2021) التي أبرزت أن فعالية أمن نظم المعلومات ترتبط بتكامل السياسات الأمنية

والبيئة التنظيمية والعوامل البشرية داخل المؤسسة

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

2. مناقشة سبب عدم وجود علاقة ذات دلالة إحصائية قوية بين أمن نظام المعلومات وإدارة استمرارية الأعمال

أظهرت نتائج تحليل الارتباط عدم وجود علاقة ذات دلالة إحصائية قوية بين أمن نظام المعلومات وإدارة استمرارية الأعمال في البنوك محل الدراسة، رغم وجود علاقة موجبة ضعيفة بين المتغيرين. ويمكن تفسير هذه النتيجة انطلاقاً من عدة اعتبارات تنظيمية وتقنية.

✓ قد يعكس ذلك أن البنوك تنظر إلى أمن نظام المعلومات باعتباره جانباً تقنياً يركز أساساً على حماية البيانات والأنظمة من الاختراق أو فقدان، في حين تُعتبر إدارة استمرارية الأعمال مفهوماً أشمل يرتبط باستمرارية العمليات والخدمات والموارد البشرية والإدارية أثناء الأزمات، وبالتالي فإن نجاح استمرارية الأعمال لا يعتمد بصورة كلية على أمن نظام المعلومات فقط.

✓ تشير النتائج إلى أن البنوك تركز بدرجة أكبر على الإجراءات الأمنية التقليدية مثل النسخ الاحتياطي، كلمات المرور، وتأمين قواعد البيانات، بينما لا يزال التكامل المؤسسي بين أمن المعلومات وإدارة استمرارية الأعمال محدوداً نسبياً، خاصة فيما يتعلق بتبني المعايير الدولية الحديثة مثل ISO 22301، الذي سجل أدنى متوسط حسابي ضمن مؤشرات استمرارية الأعمال؛

✓ يمكن تفسير هذه النتيجة بوجود تأثير لعوامل أخرى أكثر ارتباطاً باستمرارية الأعمال، مثل فعالية خطط التعافي، كفاءة فرق إدارة الأزمات، وضوح إجراءات الطوارئ، وسرعة الاستجابة أثناء الأزمات، وهي عناصر أظهرت نتائج الدراسة أنها تغطي بمستويات تطبيق مرتفعة داخل البنوك محل الدراسة؛

✓ كما قد يكون لخصوصية القطاع البنكي دور في تفسير هذه النتيجة، إذ تخضع البنوك إلى تعليمات وإجراءات تنظيمية موحدة تفرض حداً أدنى من متطلبات أمن نظام المعلومات وإدارة استمرارية الخدمات، وهو ما يؤدي إلى تقارب مستويات التطبيق بين البنوك ويقلل من ظهور فروق أو علاقات قوية إحصائياً بين المتغيرين.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

وبناءً على ما سبق، يمكن الاستنتاج أن أمن نظام المعلومات يمثل عنصرًا داعمًا لإدارة استمرارية الأعمال، لكنه ليس العامل الوحيد المحدد لها، حيث تتداخل معه مجموعة من العوامل التنظيمية والإدارية والتقنية التي تسهم مجتمعة في تعزيز قدرة البنوك على مواجهة الأزمات وضمان استمرارية نشاطه. تنسجم نتائج الدراسة الحالية، التي أظهرت عدم وجود علاقة قوية ودالة إحصائية بين أمن نظام المعلومات وإدارة استمرارية الأعمال، مع عدد من الدراسات التي أكدت أن استمرارية الأعمال تعتمد على منظومة متكاملة من العوامل، وليس على أمن المعلومات فقط. فقد أشارت دراسة Zahari Abu Bakar وآخرون (2015) إلى أن إدارة استمرارية الأعمال ترتبط بعناصر متعددة مثل التخطيط للاستمرارية، إدارة المخاطر، الاستجابة للأزمات، واستعادة العمليات، وهو ما يفسر كون أمن المعلومات يمثل عنصرًا داعمًا وليس العامل الوحيد المؤثر في استمرارية الأعمال. كما تتوافق هذه النتيجة مع دراسة خديجة العرياني وهناء الضحوي التي أكدت أن نجاح إدارة استمرارية الأعمال وفق معيار ISO 22301 يتطلب وجود إدارة متكاملة تشمل التخطيط، التوعية، إدارة الأزمات، وتقييم المخاطر، وليس فقط تطبيق إجراءات أمنية تقنية. كذلك دعمت دراسة Kosmowski (2021) هذه الفكرة من خلال تأكيدها أن فعالية استمرارية الأعمال في المؤسسات الحديثة تعتمد على الدمج بين الجوانب التقنية والتنظيمية وثقافة المؤسسة، إلى جانب التحديث المستمر لخطط الاستمرارية. ومن جهة أخرى، تتفق نتائج الدراسة مع دراسة Natalia Kukharska & Orest Polotai (2019) التي أوضحت أن غياب التخطيط المسبق والتكامل بين أمن المعلومات وإدارة الاستمرارية قد يؤدي إلى ضعف فعالية النظام ككل، رغم وجود إجراءات أمنية جيدة داخل المؤسسة. كما تنسجم مع دراسة Georg Sven Lampe وآخرون (2020) التي أكدت أن تطبيق معايير ISO 22301 و ISO 27001 بصورة منفصلة دون وجود تكامل فعلي بينهما قد يقلل من كفاءة مواجهة الأزمات واستعادة النشاط.

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

3. مناقشة نتائج الفروق حسب خصائص البنوك

أظهرت نتائج الدراسة عدم وجود فروق ذات دلالة إحصائية بين البنوك محل الدراسة فيما يتعلق بمستوى أمن نظام المعلومات وإدارة استمرارية الأعمال حسب نوع البنك أو حجم البنك، وهو ما أكدته نتائج اختبارات (T-Test)، وتحليل التباين الأحادي (ANOVA)، واختبار (Kruskal-Wallis). ففيما يتعلق بنوع البنك، بينت النتائج أن الفروق بين البنوك العمومية والخاصة والمختلطة لم تكن دالة إحصائية، سواء بالنسبة لأمن نظام المعلومات أو إدارة استمرارية الأعمال. ويمكن تفسير ذلك بكون البنوك، مهما اختلف نوعها، تخضع لنفس البيئة التنظيمية والرقابية، مما يدفعها إلى اعتماد سياسات وإجراءات متقاربة في مجالات حماية المعلومات وضمان استمرارية الخدمات البنكية. كما يمكن تفسير غياب الفروق بأن طبيعة النشاط البنكي تفرض مستوى مرتفعاً من الجاهزية الأمنية والتنظيمية على جميع البنوك دون استثناء، نظراً لحساسية البيانات المالية وأهمية استمرارية الخدمات بالنسبة للعملاء.

ولذلك أصبحت أغلب البنوك تعتمد ممارسات متشابهة نسبياً في مجالات النسخ الاحتياطي، خطط التعافي، إدارة الأزمات، وإجراءات الطوارئ. أما فيما يتعلق بحجم المؤسسة، فقد أظهرت النتائج كذلك عدم وجود فروق جوهرية بين البنوك الكبيرة والصغيرة، وهو ما يدل على أن تطبيق ممارسات أمن المعلومات واستمرارية الأعمال لا يرتبط مباشرة بحجم البنك بقدر ما يرتبط بدرجة الالتزام بالتعليمات التنظيمية ومتطلبات العمل البنكي الحديث. كما يمكن تفسير هذه النتيجة بكون التطور التكنولوجي أصبح متاحاً لمختلف البنوك بغض النظر عن حجمها، مما سمح حتى للبنوك الصغيرة بتطبيق إجراءات أمنية وتنظيمية متقدمة نسبياً للحفاظ على استمرارية خدماتها وتقليل آثار الأزمات. وبصفة عامة، تعكس هذه النتائج وجود نوع من التجانس بين البنوك محل الدراسة في مستوى تطبيق أمن نظام المعلومات وإدارة استمرارية الأعمال، وهو ما يشير إلى تنامي الوعي بأهمية هذين المتغيرين داخل القطاع البنكي، بغض النظر عن نوع البنك أو حجمه

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

تتفق نتائج الدراسة الحالية، التي أظهرت عدم وجود فروق ذات دلالة إحصائية بين البنوك حسب نوع البنك أو حجم البنك فيما يتعلق بأمن نظام المعلومات وإدارة استمرارية الأعمال، مع عدد من الدراسات السابقة التي أكدت أن المؤسسات العاملة في القطاعات الحساسة تخضع غالبًا لمتطلبات تنظيمية موحدة تجعل ممارساتها متقاربة نسبيًا. فقد أشارت دراسة أسماء عبد الرحمن الغامدي (2022) إلى أن تطبيق إدارة استمرارية الأعمال وفق معيار ISO 22301 في القطاع العام يتم وفق متطلبات تنظيمية ورقابية موحدة، وهو ما يؤدي إلى تقارب مستويات التطبيق بين المؤسسات. كما تتوافق هذه النتائج مع دراسة كمال مسوس (2022) التي أكدت أن ممارسات حوكمة أمن نظم المعلومات أصبحت ضرورة مشتركة بين المؤسسات لمواجهة الاعتداءات الإلكترونية، بغض النظر عن طبيعة البنك أو حجمه ، نتيجة تصاعد المخاطر السيبرانية وتوحيد متطلبات الحماية. وتنسجم الدراسة الحالية كذلك مع دراسة Isabel Maria Lopes & Pedro Oliveira (2016) التي أوضحت أن تطبيق سياسات أمن نظم المعلومات أصبح ممكنًا حتى داخل المؤسسات الصغيرة والمتوسطة، بفضل تطور التكنولوجيا وسهولة الوصول إلى الحلول الأمنية الحديثة، وهو ما يفسر عدم وجود فروق جوهرية بين البنوك الكبيرة والصغيرة في الدراسة الحالية. كما دعمت دراسة Katarina Makka & Katarina Kampova (2024) هذه النتيجة عندما أكدت أن التهديدات السيبرانية الحديثة دفعت مختلف المؤسسات، بغض النظر عن حجمها أو طبيعتها، إلى تبني سياسات متقاربة في مجال الأمن السيبراني واستمرارية الأعمال من أجل الحفاظ على استقرار الخدمات والقدرة على مواجهة الأزمات

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

خلاصة الفصل

سعيًا من خلال هذا الفصل المخصص للدراسة الميدانية إلى تحليل واقع أمن نظام المعلومات ودوره في دعم إدارة استمرارية الأعمال داخل البنوك محل الدراسة، وذلك بالاعتماد على مجموعة من الأساليب الإحصائية الوصفية والاستدلالية بهدف اختبار فرضيات الدراسة والإجابة عن الإشكالية الرئيسية المتعلقة بما مدى مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال. وقد تم في المبحث الأول عرض المنهجية المعتمدة في الدراسة، من خلال توضيح مجتمع الدراسة وعينتها، وأداة جمع البيانات، إضافة إلى الأساليب الإحصائية المستخدمة في تحليل المعطيات. أما المبحث الثاني فقد خُصص لعرض النتائج المتوصل إليها وتحليلها ومناقشتها في ضوء أهداف الدراسة والدراسات السابقة.

وقد توصلت الدراسة الميدانية إلى مجموعة من النتائج يمكن تلخيصها فيما يلي:

✓ وجود مستوى مرتفع من تطبيق أمن نظام المعلومات داخل البنوك محل الدراسة، حيث سجلت أبعاد سرية المعلومات وسلامتها وتوافرها متوسطات حسابية مرتفعة، مما يعكس اهتمام البنوك بحماية المعلومات وتعزيز الإجراءات الأمنية المرتبطة بها؛

✓ وجود مستوى مرتفع من تطبيق إدارة استمرارية الأعمال داخل البنوك محل الدراسة، من خلال اعتماد خطط استمرارية الأعمال، وخطط التعافي، وإجراءات الطوارئ، وفرق إدارة الأزمات، مع تسجيل تفاوت نسبي في تبني معيار ISO 22301 بين البنوك؛

✓ أظهرت النتائج وجود علاقة ارتباطية موجبة لكنها ضعيفة جدا وغير دالة إحصائيا بين أمن نظام المعلومات وإدارة استمرارية الأعمال، حيث بلغ معامل الارتباط ($r = 0.293$) بمستوى دلالة غير معنوي، مما يدل على أن تأثير أمن نظام المعلومات على استمرارية الأعمال لم يظهر بشكل مباشر وقوي داخل البنوك محل الدراسة؛

✓ بينت نتائج مصفوفة الارتباط وجود علاقات ارتباطية دالة بين بعض أبعاد أمن نظام المعلومات، خاصة بين سرية المعلومات وسلامتها، وكذلك بين سلامة المعلومات وتوافرها، وهو ما يعكس تكامل هذه الأبعاد داخل البيئة البنكية؛

الفصل الثاني : الدراسة الميدانية لمساهمة امن نظام المعلومات في دعم إدارة استمرارية الاعمال لمجموعة من

البنوك الجزائرية بورقلة

✓ أظهرت نتائج اختبارات الفروق الإحصائية (Kruskal-Wallis، ANOVA، T-Test) عدم وجود فروق ذات

دلالة إحصائية في مستوى أمن نظام المعلومات وإدارة استمرارية الأعمال تعزى إلى نوع البنك أو حجم البنك، مما يدل

على وجود تقارب في السياسات والممارسات المعتمدة بين البنوك محل الدراسة؛

✓ كما أظهرت نتائج اختبارات التوزيع الطبيعي أن بيانات الدراسة تحقق بدرجة كبيرة شرط الاعتدال في التوزيع، الأمر الذي

سمح بالاعتماد على الاختبارات الإحصائية المناسبة لتحليل الفرضيات.

وبناءً على ما سبق، يمكن القول إن البنوك محل الدراسة تولي اهتمامًا واضحًا بمجالي أمن نظام المعلومات وإدارة استمرارية الأعمال،

غير أن العلاقة المباشرة بين المتغيرين لم تظهر بالقوة الكافية إحصائيًا، وهو ما قد يُفسر بوجود عوامل تنظيمية أو تقنية أخرى

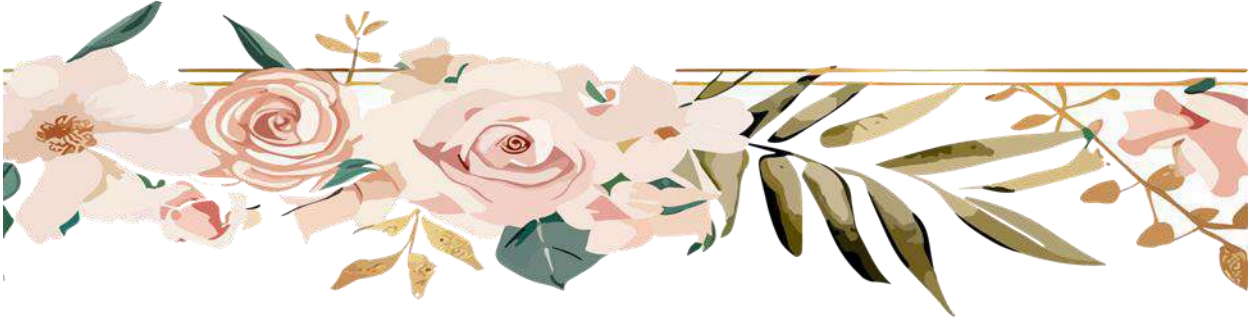
تتدخل في دعم إدارة استمرارية الأعمال إلى جانب أمن نظام المعلومات. كما تؤكد هذه النتائج أهمية تعزيز التكامل بين

السياسات الأمنية وخطط الاستمرارية، مع ضرورة توسيع تبني المعايير الدولية الحديثة مثل معيار ISO 22301 بما يضمن رفع

جاهزية البنوك لمواجهة الأزمات والاضطرابات المختلفة.



خاتمة



خاتمة

في ختام هذه الدراسة التي تناولت مدى مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال، يمكن التأكيد على أن أمن نظام المعلومات يُعد من الركائز الأساسية التي تعتمد عليها المؤسسات الحديثة لضمان استمرارية نشاطها، خاصة في ظل البيئة الرقمية المتسارعة وما يرافقها من تهديدات ومخاطر سيبرانية متزايدة، حيث أصبح من غير الممكن فصل استمرارية الأعمال عن مستوى الحماية والأمن المعلوماتي داخل المؤسسة. ويكتسب هذا الموضوع أهمية متزايدة بالنظر إلى طبيعة المؤسسات العمومية والخدمات التي تقدمها، والتي تتطلب استمرارية دائمة ودقة عالية في معالجة المعلومات وحمايتها من أي اختراق أو خلل قد يؤثر على سير العمل. وفي هذا السياق، يبرز أمن نظام المعلومات كعنصر استراتيجي يساهم في ضمان استمرارية العمليات، وتقليل الانقطاعات، وتعزيز الثقة في النظام المعلوماتي للمؤسسة.

وقد تمت معالجة هذا الإشكال من خلال فصلين أساسيين؛ حيث حُصص الفصل الأول للجانب النظري الذي تناول مختلف المفاهيم المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال، إضافة إلى إبراز العلاقة بينهما من خلال الأدبيات والدراسات السابقة، مما سمح ببناء إطار نظري متكامل لفهم الموضوع. أما الفصل الثاني، فقد حُصص للدراسة الميدانية، حيث تم إسقاط الجانب النظري على واقع البنوك محل الدراسة، بالاعتماد على أداة الاستبيان كوسيلة رئيسية لجمع البيانات، ثم تحليلها باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية SPSS، وهو ما سمح بالوصول إلى نتائج دقيقة تعكس واقع الظاهرة المدروسة. وقد أظهرت النتائج المتوصل إليها أن أمن نظام المعلومات يلعب دوراً محورياً في دعم إدارة استمرارية الأعمال داخل البنوك، من خلال مساهمته في حماية البيانات، وضمان تدفق المعلومات بشكل آمن ومستمر، إلا أن هذا الدور يبقى مرتبطاً بعدة عوامل من بينها مستوى التكوين والتأهيل لدى العاملين، ومدى مواكبة المؤسسة للتطورات التكنولوجية الحديثة، إضافة إلى توفر الموارد التقنية والبشرية اللازمة لتعزيز منظومة الأمن المعلوماتي. كما بينت الدراسة وجود بعض النقائص التي قد تحد من فعالية أمن نظام المعلومات، من أبرزها الحاجة إلى تعزيز الوعي الأمني لدى العاملين، وضعف التكوين المستمر في مجال حماية المعلومات، إضافة إلى ضرورة تدعيم البنية التحتية التقنية، وتوسيع نطاق الحماية ليشمل مختلف المستويات التنظيمية داخل المؤسسة وليس فقط المستوى

خاتمة

المركزي. ومن خلال ربط النتائج الميدانية بالإطار النظري، تبين أن تحقيق استمرارية الأعمال بشكل فعال لا يعتمد فقط على توفر الأنظمة المعلوماتية، بل يتطلب أيضاً تكاملاً بين العنصر البشري والتقني والتنظيمي، حيث يشكل العامل البشري محورياً أساسياً في نجاح سياسات أمن المعلومات، من خلال الالتزام بالإجراءات، والوعي بالمخاطر، والمساهمة في حماية النظام المعلوماتي.

توصيات الدراسة :

في ضوء النتائج التي توصلت إليها الدراسة، والتي أبرزت أهمية أمن نظام المعلومات في دعم إدارة استمرارية الأعمال داخل البنوك محل الدراسة، يمكن تقديم مجموعة من التوصيات العملية التي من شأنها تعزيز هذا الدور وتحسين الأداء التنظيمي، وذلك كما يلي:

1- تكوين وتدريب العاملين في مجال أمن المعلومات

من الضروري تنظيم دورات تكوينية دورية لفائدة الموظفين حول أسس حماية المعلومات، وطرق التعامل مع المخاطر السيبرانية، بما يساهم في رفع مستوى الوعي الأمني لديهم وتقليل الأخطاء البشرية التي قد تؤثر على النظام المعلوماتي.

2- تعزيز الوعي المستمر بأمن نظام المعلومات و إدارة استمرارية الأعمال

العمل على نشر ثقافة تنظيمية داخل تُعنى بأهمية أمن نظام المعلومات و إدارة استمرارية النشاط، من خلال حملات تحسيسية، وورشات عمل، ومذكرات إرشادية تواكب المستجدات التقنية.

3- الاطلاع المستمر على مستجدات أنظمة المعلومات

ضرورة مواكبة التطورات الحديثة في تكنولوجيا المعلومات وأنظمة الحماية، وتحديث المعارف بشكل دوري لضمان فعالية الإجراءات الأمنية واستمرارية الخدمات دون انقطاع.

4- توفير طاقم متخصص في أمن المعلومات

خاتمة

تخصيص فرق عمل مؤهلة على مستوى كل الوكالات أو الفروع، وليس فقط على المستوى المركزي، لضمان المتابعة الميدانية المستمرة والتدخل السريع في حالة حدوث أي خلل أو تهديد.

5- دعم التكوين المستمر للعاملين

إدراج برامج تدريبية منتظمة ومستمرة لجميع العمال، بما يسمح بتطوير مهاراتهم التقنية وتعزيز قدرتهم على التعامل مع أنظمة المعلومات الحديثة بكفاءة.

6- تزويد المؤسسة بأحدث التقنيات والبرمجيات

الاستثمار في تحديث البنية التحتية الرقمية، واعتماد حلول تقنية متطورة في مجال أمن المعلومات، بما يضمن حماية أفضل للبيانات واستمرارية أعلى للخدمات.

افاق الدراسة

✓ التوسع في دراسة المعايير الدولية الخاصة بأمن المعلومات ونظام ادارة استمرارية الأعمال مثل: ISO و ISO 27001 و ISO 22301.

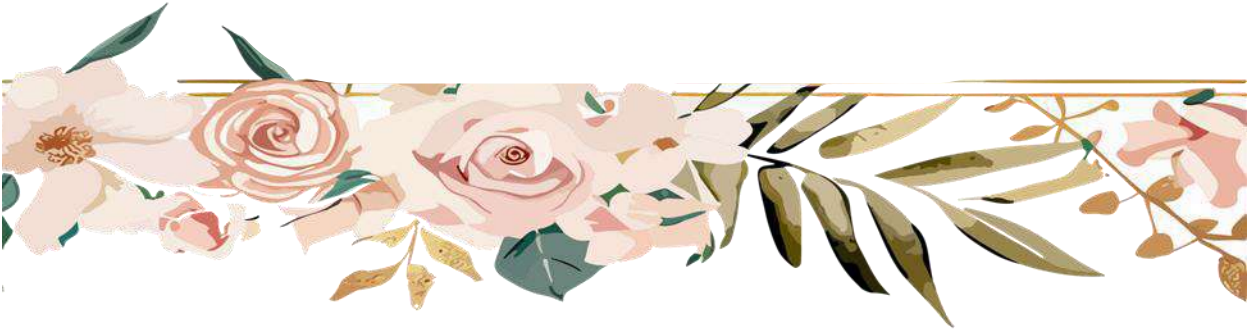
✓ دراسة تأثير التحول الرقمي والتهديدات السيبرانية على استمرارية الأعمال داخل المؤسسات الجزائرية.

✓ فتح المجال أمام دراسات مستقبلية حول أمن نظام المعلومات وإدارة استمرارية الأعمال في قطاعات أخرى

✓ .دراسة التحديات التي تواجه تطبيق إدارة استمرارية الأعمال واقتراح الآليات المناسبة لتطويرها في البنوك الجزائرية



قائمة المراجع



قائمة المراجع

المصادر والمراجع باللغة العربية :

اولا:المقالات المنشورة :

- نبيل حليمي ,رشيد حفصي, أهمية الامن المعلوماتي بالمؤسسة الاقتصادية دراسة حالة مديرية توزيع الكهرباء والغاز بورقلة مجلة الجزائرية للدراسات الاقتصادية والإدارية, المجلد 02, العدد 01 , 2022
- بن طيب إبراهيم, أهمية امن نظم المعلومات لدى المؤسسات الاقتصادية الحديثة ,مجلة التنمية والاقتصاد التطبيقي, العدد03, مارس 2018
- عبد الحكيم بن بختي ,دور نظم المعلومات في تحسين الأداء الوظيفي للإدارة الجزائرية الحديثة, مجلة العلوم الانسان والمجتمع, المجلد 13, العدد 03, السنة 2024
- أسماء عبد الرحمن الغامدي ,واقع إدارة استمرارية الاعمال ايزو 220301 في القطاع العام لمواجهة الازمات : الممكلة العربية السعودية نموذا , مجلة إدارة المخاطر والأزمات, المجلد 4, العدد 1
- خديجة يحيى العرياني هناء علي ضحوي ,إدارة المعلومات بفاعلية اثناء الازمات من خلال نظام إدارة استمرارية الاعمال في المؤسسات ,المجلة الدولية لنشر والبحوث والدراسات, المجلد الثالث, 20 أكتوبر 2021
- كمال مسوس, ممارسات حوكمة أمن نظم المعلومات في المؤسسة: بين التقبل أو الحد من الاعتداءات الإلكترونية, المجلة الجزائرية للعملة والسياسات الاقتصادية, المجلد 13, الجزائر, 2022.
- فايز جمعة صالح النجار اروى محمد الحرايزة ,الذكاء الاستراتيجي واثره في إدارة الاستمرارية الاعمال دراسة حالة في امانة عمان الكبرى ,مجلة العالمية للاقتصاد والاعمال2022

قائمة المراجع

ثانيا :الرسائل الجامعية

- قدور مقراني, تقييم مدى مساهمة امن نظم المعلومات الالكترونية في الحد من مخاطر نظم المعلومات : دراسة حالة مؤسسة الاتصالات الجزائر, مذكرة نيل شهادة الماستر ,كلية علوم الاقتصادية والتجارية وعلوم التسيير, جامعة قاصدي مرباح ورقلة, 2016
- ابن محمد فارس الدنف, واقع إدارة امن نظم المعلومات في الكليات التقنية في غزة ,مذكرة نيل شهادة الماجستير كلية التجارة ,جامعة الإسلامية غزة 2013
- /دليلة العوفي ,محاضرات أنظمة المعلوماتية ,كلية الاعلام والاتصال ,جامعة الجزائر 3ابراهيم سلطان شسبوط , 2020, 2021,
- الدام محمد, الامن السيبراني ,مذكرة ماستر لنيل شهادة الماستر في الحقوق تخصص جريمة وامن ,كلية الحقوق والعلوم السياسية ,جامعة الشهيد حمه لخضر ,الوادي
- حمودي كاهنة, نظام امن المعلومات في الجزائر دراسة حالة بلدية سوق الاثنين ولاية تيزي وزو ,مذكرة لنيل شهادة الماستر في العلوم السياسية والعلاقات الدولية ,جامعة مولود معمري ,كلية الحقوق والعلوم السياسية, سنة 2016
- الطاهر بن عمارة، تقييم مدى مساهمة نظام الامن الالكترونية في الحد من مخاطر نظم المعلومات: دراسة مقارنة لعينة /المؤسسات, مذكرة نيل شهادة الماستر كلية العلوم الاقتصادية والتجارية وعلوم التسيير, جامعة قاصدي مرباح، ورقلة 2016 2017

قائمة المراجع

ثالثا : المواقع الالكترونية

● ISO/IEC 27005:2022 - Guidance on managing information security risks

● : <https://hbrarabic>

● : ISO/TS 22317:2021 - Business Impact Analysis Guidelines for BCMS

المصادر والمراجع باللغة الاجنبية : 🔍

_Adam A. Semlambo, Catherine G. Mkude, Edison Wazoel Lubua, **Factors Influencing Information Systems Security**, International Journal of Engineering and Science, Vol. 10, No. 1, 2021.

_Adam Aloyce Semlambo, Didas Malekia Mfoi, Yona Sangula, **Security Threats and Vulnerabilities of Information Systems: A Case Study of the Institute of Accountancy Arusha (IAA)**, Journal of Computer and Communications, Vol. 10, 2022.

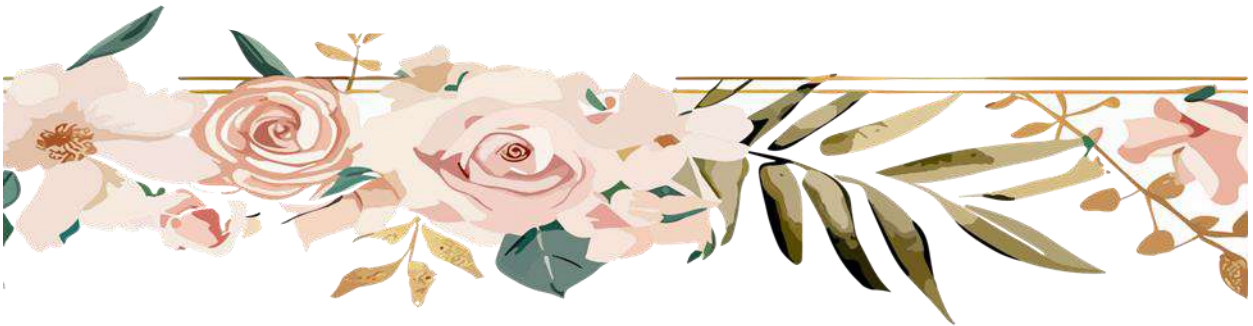
Isabel Maria Lopes, Pedro Oliveira, “Information Systems Security Policies in Small and Medium Enterprises”, Information Systems Engineering and Management, Vol. 1, No. 2, 2016.

,Zahari Abu Bakar, Noorulsadiqin Azbiya Yaacob, Zulkifli Mohamed Udin **The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework**”, International Journal of Economics and Financial Issues, Vol. 5, No. 4, 2015.

-
- Piotr Jedynak, **Business Continuity Management – A Management Science Perspective**, International Journal of Contemporary Management, No. 4 .2013
- Kazimierz T. Kosmowski, **“Business Continuity Management Framework for Industry 4.0 Companies Regarding Dependability and Security of ICT ,and ICS/SCADA System”**, Summer Safety and Reliability Seminar, Vol. 34 .2021
- Katarina Makka, Katarina Kampova, **“Integration of Cybersecurity and Business Continuity Management to Ensure Organizational Resilience in the Digital Environment”**, Challenges to National Defence in Contemporary .Geopolitical Situation, 2024
- Nataliia Kukharska, Orest Polotai, **“Relationship Between Information ,”Security and Business Continuity Management in Organizations** 2019 ,Information Technology and Security, Vol. 7, No. 2
- Georg Sven Lampe, Mihaela Maftai, Ioana Surugiu, Răzvan Cristian Ionescu **Study on Information Security Management System and Business Continuity Management in the Context of the Global Crisis**, BASIQ International Conference on New Trends in Sustainable Business and .2020 ,Consumption, Vol. 6
- Marko Niemimaa, **Interdisciplinary Review of Business Continuity from an ,”Information Systems Perspective: Toward an Integrative Framework ,Communications of the Association for Information Systems**, Vol. 37, No. 1 2015



الملاحق



الملاحق

الملحق رقم 01 : استمارة الاستبيان

جامعة قاصدي مرباح ورقلة
كلية العلوم الاقتصادية وعلوم التسيير وعلوم التجارية
قسم : علوم التسيير

المستوى : ثانية ماستر
تخصص إدارة أعمال

الاستبيان

تحية طيبة وبعد...

في إطار إنجاز مذكرة تخرج لنيل شهادة الماستر في علوم التسيير تخصص إدارة أعمال، يشرفنا أن نضع بين أيديكم هذه الاستبيان التي تهدف إلى دراسة مساهمة أمن نظام المعلومات في دعم استمرارية الأعمال . ونظرا لكفاءتكم وخبرتكم المهنية وانتمائكم لهذه المؤسسة، فإننا نأمل منكم المساهمة الجادة من خلال الإجابة على عبارات هذا الاستبيان بكل موضوعية وصدق، وذلك بوضع علامة (X) في الخانة التي تعبر عن رأيكم.

نؤكد لكم أن جميع المعلومات المقدمة ستعامل بسرية تامة، ولن تستخدم إلا لأغراض البحث العلمي فقط.

شاكرين تعاونكم ومساهمتمكم القيمة.

الطالبة: داهش شيما / بوليف ايمان هبة الرحمان

أولا : البطاقة التعريفية للبنك

اسم البنك: اسم الفرع:

نوع البنك: ☐ عمومي ☐ خاص ☐ مختلط

حجم المؤسسة : ☐ صغير ☐ متوسط ☐ كبير

هل لدى البنك نظام معلوماتي؟ ☐ نعم ☐ لا

هل لديك خطة لاستمرارية الأعمال : ☐ نعم ☐ لا

الابعاد	العبارات	غير موجود	ضعيف التطبيق	متوسط التطبيق	جيد التطبيق	تطبيق فعال
المتغير الأول : أمن نظام المعلومات						
سرية المعلومات	تعتمد المؤسسة على سياسات واضحة لتحديد صلاحيات الوصول الى المعلومات					
	يتم تقييد الوصول الى المعلومات الحساسة حسب طبيعة الوظيفة					
	يتم استخدام تقنيات التحقق من الهوية (Authentication) لحماية النظام					
	يتم تغيير كلمات المرور بشكل دوري وفق المعايير الامنية					
	يتم استخدام تقنيات التشفير او وسائل حماية لضمان عدم تغيير البيانات					
	يتم توعية الموظفين بمخاطر تسريب المعلومات					
سلامة المعلومات	توجد اليات لتتبع استخدام البيانات داخل النظام (Audit Logs).					
	يتم التحقق من صحة البيانات قبل المعالجة او تخزينها					
	توجد اليات واضحة لمعالجة التلاعب في					

قائمة الملاحق

البيانات					
				يتم مراجعة البيانات بشكل دوري للتأكد من سلامتها	توافر المعلومات
				يتم حماية قواعد البيانات من التعديلات المباشرة غير مصرح بها	
				توجد نظم تنبيه عند حدوث تغييرات غير عادية في البيانات	
				تضمن المؤسسة توفر البيانات للمستخدمين بشكل مستمر	
				تعتمد المؤسسة على أنظمة النسخ الاحتياطي بشكل دوري	
				يتم استرجاع البيانات بسرعة حدوث أعطال	
				يتم مراقبة أداء الأنظمة بشكل مستمر لتفادي الأعطال	
				يتم توفير بنية تحتية بديلة في حالة توقف النظام	
				يتم تحديد أوقات الصيانة دورية للنظام دون التأثير على استمرارية الخدمة	
البعد الثاني : استمرارية الأعمال					
				تعتمد المؤسسة على خطة استمرارية الأعمال (BCP).	
				يتم تحديث خطة استمرارية الأعمال بشكل دوري	
				توجد خطة تعافي من الكوارث (DRP) داخل البنك	
				يوجد فرق مختصة لإدارة الالتزامات	
				تتم استجابة للالتزامات بسرعة وفعالية	
				توجد إجراءات مكتوبة وواضحة للتعامل مع الالتزامات	
				تعتمد المؤسسة على سجل الكتروني للمخاطر	
				يتم تقييم المخاطر بشكل دوري	
				يتم تحديد زمن استرجاع (RTO) بشكل دقيق	
				يعتمد البنك على معيار ISO 22301 في إدارة استمرارية الأعمال	

أسئلة المفتوحة :

هل سبق للمؤسسة أن تعرضت لحوادث أمنية معلوماتية أدت إلى تعطل أو توقف بعض الخدمات؟

☐ نعم ☐ لا

ما هو نوع الحادث الذي تم تسجيله؟

☐ اختراق نظام ☐ فيروس أو برمجيات خبيثة ☐ أخطاء بشرية ☐ تسريب بيانات

ما رأيك في طريقة تعامل البنك مع الاختراقات والحوادث الأمنية؟ وهل السياسات الأمنية فعالة؟

قائمة الملاحق

ما الإجراءات أو الحلول التي تقترحها لتعزيز حماية المعلومات البنكية واستمرارية العمل؟

قائمة الملاحق

رقم الملحق 02 : حول معيار ISO المطبق في بنك السلام



**CERTIFICAT
D'ENREGISTREMENT**

Le Système de Management de :

AL SALAM BANK ALGERIA

Site principal : 233, Rue Ahmed Ouaked, Dely Brahim, Alger, Algérie
Se référer à l'annexe pour la liste des sites et leurs champs de certification spécifiques.

a été enregistré par Intertek comme étant conforme aux exigences de la norme :

ISO 9001:2015

Le Système de Management est applicable à :

Qualité de service :

- Du Conseil à la Clientèle,
- Des Opérations de Caisse et Portefeuille,
- Des Opérations du Commerce Extérieur,
- Des Financements octroyés aux entreprises et particuliers.

Certificat n° :
0201493

Date de certification initiale :
30 Décembre 2024

Date de certification :
30 Décembre 2024

Date d'émission du certificat :
30 Décembre 2024

Date d'expiration :
29 Décembre 2027



Intertek



Calin Moldovean
Président, Business Assurance

Intertek Algeria Ltd Zone urbaine Garidi 01, N
*C7 CB Bâtiment F1, 1er étage Local N°1,
Kouba, Alger, Algérie



L'émission de ce certificat n'engage la responsabilité d'Intertek envers aucun tiers autre que le client. Le présent certificat est soumis au maintien de la conformité du système de l'organisation par rapport aux règles de certification du système d'Intertek. Sa validité peut être confirmée sur demande par email à certificate.validation@intertek.com ou en scannant le code QR. Le droit de revendre ou d'exploiter ce certificat est la propriété d'Intertek, à qui il devra être retourné en cas de demande.





**CERTIFICAT
D'ENREGISTREMENT**

ANNEXE

Cette annexe liste les sites certifiés de :

AL SALAM BANK ALGERIA

Cette annexe est rattachée au certificat principal n°0201493 et ne peut être ni présentée ni reproduite sans celui-ci.

Agence El Anna'sser

218 rue Hassiba ben Bouali, Alger

Qualité de service :

- Du Conseil à la Clientèle,
- Des Opérations de Caisse et Portefeuille,
- Des Opérations du Commerce Extérieur,
- Des Financements octroyés aux entreprises et particuliers.

Agence Sidi Yahia

04 rue hamdani lahcen sidi yahia Hydra, Alger

Qualité de service :

- Du Conseil à la Clientèle,
- Des Opérations de Caisse et Portefeuille,
- Des Opérations du Commerce Extérieur,
- Des Financements octroyés aux entreprises et particuliers.

L'émission de ce certificat n'engage la responsabilité d'Intertek envers aucun tiers autre que le client, et uniquement de termes définis par le contrat. La validité du présent certificat est soumise au maintien de la conformité du système de l'organisme par rapport aux exigences de certification de système d'Intertek. Sa validité peut être confirmée sur demande par email à certificate.validation@intertek.com ou en scannant le code sur la droite avec un smartphone. Ce certificat est la propriété d'Intertek, à qui il devra être retourné en cas de demande.



الملحق رقم: 03 معيار ISO المطبق في بنك الخليج



Système de Management de la Sécurité de l'Information

Communication mensuelle – avancement, prochaines étapes et focus cybersécurité

Chers collègues,

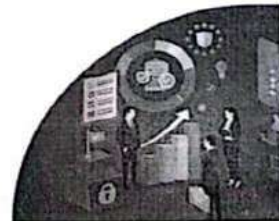
1. État d'avancement

Au cours des dernières semaines, plusieurs étapes clés ont été réalisées :

- Définition du contexte de l'organisation, incluant la réalisation d'une analyse SWOT, une analyse PESTEL et l'identification des acteurs internes et externes et leurs exigences en matière de sécurité de l'information.
- Finalisation de l'analyse des écarts à l'égard des exigences de la norme ISO 27001:2022 couvrant les clauses obligatoires (de 4 à 10) et les 93 mesures de l'annexe A.
- Identification et documentation de trois trajectoires du périmètre du SMSI.

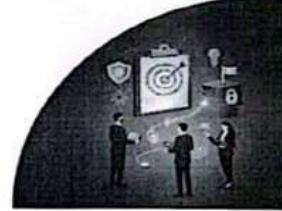
Ces travaux permettent de consolider une vision claire de notre exposition aux risques inhérents à notre capital informationnel et de structurer les mesures de sécurité adaptées à notre contexte.

2. Prochaines étapes



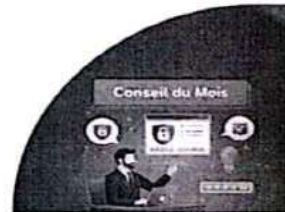
Pour consolider les fondations de notre SMSI et assurer une couverture exhaustive de nos enjeux de sécurité, les prochaines phases du projet porteront notamment sur :

- **Méthodologie de gestion des risques** – Définir une approche structurée et documentée pour identifier et évaluer les risques liés à la sécurité de l'information.
- **Cartographie des risques** – Établir une vue claire de notre exposition actuelle et potentielle aux risques inhérents à la sécurité de l'information.
- **Plan de traitement des risques** – Déterminer les actions correctives et préventives adaptées à notre contexte.
- **Déclaration d'applicabilité** – Documenter les mesures de sécurité retenues et justifier celles non applicables à notre contexte.
- **Définition du périmètre** – Documenter le périmètre du SMSI et les déclinaisons des domaines d'application.



3. Focus thématique du mois

Avec l'émergence des outils d'intelligence artificielle, il est crucial de comprendre les risques associés à leur utilisation dans notre environnement bancaire. Ce mois-ci, nous vous rappelons les bonnes pratiques essentielles. Les outils d'IA générative tels que ChatGPT, Gemini ou Copilot ne garantissent pas la sécurité des données professionnelles, car toute information saisie peut être enregistrée, analysée et potentiellement réutilisée par des tiers.



✕ Usages Interdits

Il vous est strictement interdit de saisir, transmettre ou copier dans ces outils :

- Données clients (IBAN, KYC...)
- Contrats & données partenaires
- Informations RH confidentielles
- Documents & procédures internes
- Projets et décisions stratégiques

🛡️ L'IA peut se tromper

Les réponses fournies par ces outils ne doivent en aucun cas être considérées comme fiables sans validation préalable par les services compétents. Elles peuvent sembler convaincantes, mais peuvent contenir des erreurs ou des informations inexactes.



Système de Management de la Sécurité de l'Information

Communication mensuelle – avancement, prochaines étapes et focus cybersécurité

قائمة الملاحق

Chers collègues,

1. État d'avancement

Au cours des dernières semaines, plusieurs étapes clés ont été réalisées :

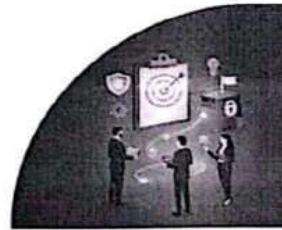
- Définition du contexte de l'organisation, incluant la réalisation d'une analyse SWOT, une analyse PESTEL et l'identification des acteurs internes et externes et leurs exigences en matière de sécurité de l'information.
- Finalisation de l'analyse des écarts à l'égard des exigences de la norme ISO 27001:2022 couvrant les clauses obligatoires (de 4 à 10) et les 93 mesures de l'annexe A.
- Identification et documentation de trois trajectoires du périmètre du SMSI.

Ces travaux permettent de consolider une vision claire de notre exposition aux risques inhérents à notre capital informationnel et de structurer les mesures de sécurité adaptées à notre contexte.

2. Prochaines étapes

Pour consolider les fondations de notre SMSI et assurer une couverture exhaustive de nos enjeux de sécurité, les prochaines phases du projet porteront notamment sur :

- **Méthodologie de gestion des risques** – Définir une approche structurée et documentée pour identifier et évaluer les risques liés à la sécurité de l'information.
- **Cartographie des risques** – Établir une vue claire de notre exposition actuelle et potentielle aux risques inhérents à la sécurité de l'information.



- **Plan de traitement des risques** – Déterminer les actions correctives et préventives adaptées à notre contexte.
- **Déclaration d'applicabilité** – Documenter les mesures de sécurité retenues et justifier celles non applicables à notre contexte.
- **Définition du périmètre** – Documenter le périmètre du SMSI et les déclinaisons des domaines d'application.

3. Focus thématique du mois

Avec l'émergence des outils d'intelligence artificielle, il est crucial de comprendre les risques associés à leur utilisation dans notre environnement bancaire. Ce mois-ci, nous vous rappelons les bonnes pratiques essentielles. Les outils d'IA générative tels que ChatGPT, Gemini ou Copilot ne garantissent pas la sécurité des données professionnelles, car toute information saisie peut être enregistrée, analysée et potentiellement réutilisée par des tiers.



✗ Usages Interdits

Il vous est strictement interdit de saisir, transmettre ou copier dans ces outils :

- Données clients (IBAN, KYC...)
- Contrats & données partenaires

قائمة الملاحق

- Informations RH confidentielles
- Documents & procédures internes
- Projets et décisions stratégiques

L'IA peut se tromper

Les réponses fournies par ces outils ne doivent en aucun cas être considérées comme fiables sans validation préalable par les services compétents. Elles peuvent sembler convaincantes, mais peuvent contenir des erreurs ou des informations inexacts.



« Politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par une organisation, dans le but de protéger ses actifs informationnels. »

[ISO/CEI 27000]

الملحق رقم 04 محاور التدريب في بنك BNA

GLOBAL BANKING SOLUTION	
01	CHANGEMENT DU MOT DE PASSE
02	Consultation Specimen de singature
03	ADMINISTRATION GENERALE
04	COMPTABILITE CENTRALE
05	GESTION CLIENTELE
06	AGENCE
07	PLACEMENTS
08	ENGAGEMENTS
09	ETRANGER
10	MONETIQUE
11	EXPLOITATION INFORMATIQUE

Votre Choix : evgesmdp

قائمة الملاحق

الملحق رقم 05 اسئلة المقابلة

البنك : BNA,BDL,BADR,BEA,CPA,TRUSK,AGB ;بنك البركة ,بنك السلام ,بنك الجمعية العامة

المقابل : مسؤولي الامن المعلوماتي

الموضوع :مساهمة امن نظام المعلومات في دعم ادارة استمرارية الاعمال

تهدف هذه المقابلة إلى استكشاف مساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال داخل البنوك محل الدراسة، من خلال تحليل مدى إسهام إجراءات وضوابط أمن المعلومات في حماية الأنظمة والبيانات وضمان استمرارية العمليات الحيوية. كما تسعى إلى فهم كيفية تأثير عناصر أمن المعلومات مثل السرية والسلامة والتوافر في الحد من المخاطر التقنية والتشغيلية، وتقليل احتمالية الانقطاعات، بما يساهم في تعزيز قدرة المؤسسة على الاستجابة للأزمات وضمان استمرارية تقديم خدماتها بكفاءة وفعالية.

أسئلة حول النظام الخاص بالوكالة:

1. تقديم نبذة عن النظام المستخدم + واجهة النظام.
2. هل هو نظام خاص أم هل له أنظمة أخرى تابعة له؟
3. كم تبلغ تكلفة اقتناء النظام وما هو مصدره؟
4. ما هي الفترة الزمنية لبدء عمل النظام؟
5. كم بلغت مدة التدريب حول هذا النظام؟
6. هل التدريب حول النظام يقتصر على المستخدمين فقط؟
7. هل التدريب يكون في حدود صلاحيات الوصول الخاصة بالمستخدم؟

قائمة الملاحق

8. هل هناك نموذج حول حضور الدورات؟ + وثيقة
9. في أي مدة زمنية (رسالة أسبوعية أو شهرية) يتم التحكم في النظام؟
10. ما هي الأخطاء أو المشاكل المتكررة في حالة استخدام النظام؟
11. هل يتم صيانة النظام بصفة دورية أو سنوية؟
12. هل هناك خطة أو نموذج للتعامل مع مشاكل الشبكة التي يمكن أن تتسبب في توقف النظام؟ + وثيقة
13. هل النظام موحد على مستوى جميع الوكالات للبنك؟

أسئلة حول النظام المعلوماتي:

- (1) هل يمكن وصف البنية التحتية لنظام المعلومات؟
- (2) ما نوع الأنظمة المستخدمة؟ هل سيرفرات محلية أو مركزية؟
- (3) هل تعتمدون على شبكة محلية أم مركزية؟
- (4) كيف يتم الربط بين الوكالة والمقر الرئيسي للبنك؟
- (5) هل هناك وثيقة رسمية توضح هيكلية النظام المعلوماتي؟ + وثيقة مثل ربط الحواسيب بالسيرفرات - خريطة النظام المعلوماتي
- (6) هل لديكم نموذج لمختلف الأعطال السابقة التي تعرض لها النظام؟ + وثيقة

أسئلة حول المعايير:

1. هل تعتمدون على المعايير الدولية في أمن المعلومات مثل ISO 27001؟
2. هل يتم القيام بعمليات تدقيق دورية على الأنظمة المستخدمة؟ على مستوى الفحص والمراجعة - من أين تُؤخذ - هل الإجراءات مطبقة؟ + وثيقة

قائمة الملاحق

أسئلة لدعم النسخ الاحتياطي:

- (1) هل يتم الوصول إلى عدد الحوادث الأمنية خلال مدة عمل النظام؟
- (2) عدد الأعطال التقنية أو اختفاء النظام.
- (3) من هو المسؤول عن إدارة النظام المعلوماتي داخل الوكالة؟
- (4) هل يوجد مختص في أمن المعلومات؟

قائمة الملاحق

الملحق رقم 06 قائمة اساتذة الاعضاء المحكمين للاستبيان

الرقم	الأستاذ	الرتبة	القسم / الكلية
01	سعيدات نجمي		قسم العلوم التجارية / كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
02	هتهات المهدي		قسم العلوم التجارية / كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
03	بالا طرش حورية	أستاذة التعليم العالي	قسم العلوم التجارية / كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
04	خميس نفيسة	محاضر ب	قسم العلوم التجارية / كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
05	سميرة صالح	أستاذة التعليم العالي	قسم العلوم التجارية / كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير

قائمة الملاحق

الملحق رقم 07 مخرجات spss نسخة 27

Statistiques de fiabilité	
Alpha de Cronbach	Nombre d'éléments
,685	28

Remarques		
Sortie obtenue	02-MAY-2026 18:57:52	
Commentaires		
Entrée	Données	D:\mémoires encadrées\2025-2026\autres\ben zine\APP BENZINE.sav
	Jeu de données actif	Jeu_de_données0
	Filtre	<sans>
	Pondération	<sans>
	Scinder un fichier	<sans>
	N de lignes dans le fichier de travail	10
Gestion des valeurs manquantes	Définition de la valeur manquante	Les valeurs manquantes définies par l'utilisateur sont traitées comme étant manquantes.
	Observations utilisées	Les statistiques sont basées sur toutes les observations comportant des données valides.
Syntaxe	FREQUENCIES VARIABLES=BANK TYP5 SIZE IS BCP /PIECHART FREQ /ORDER=ANALYSIS.	
Ressources	Temps de processeur	00:00:02,00
	Temps écoulé	00:00:01,02

Statistiques					
		البنك اسم	البنك نوع	المؤسسة حجم	نظام البنك لدى هل معلوماتي؟
N	Valide	10	10	10	10
	Manquant	0	0	0	0

Récapitulatif de traitement des observations

		N	%
Observations	Valide	10	100,0
	Exclue ^a	0	,0
	Total	10	100,0

التطبيق ضيف	1	10,0	10,0	40,0
التطبيق متوسط	1	10,0	10,0	50,0
التطبيق جيد	2	20,0	20,0	70,0
فعال تطبيق	3	30,0	30,0	100,0
Total	10	100,0	100,0	

		البنك اسم			
		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	BDL	1	10,0	10,0	10,0
	BADR	1	10,0	10,0	20,0
	ELSALAM	1	10,0	10,0	30,0
	AGB	1	10,0	10,0	40,0
	CPA	1	10,0	10,0	50,0
	TRUST	1	10,0	10,0	60,0
	BARAKA	1	10,0	10,0	70,0
	BEA	1	10,0	10,0	80,0
	BNA	1	10,0	10,0	90,0
	Société général	1	10,0	10,0	100,0
	Total	10	100,0	100,0	

قائمة الملاحق

البنك نوع			
		Fréquence	Pourcentage
Valide	عمومي	5	50,0
	خاص	3	30,0
	مختلط	2	20,0
	Total	10	100,0

Audit Logs النظام داخل البيانات استخدام لتتبع اليات وجود				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	1	10,0	20,0
	فعال تطبيق	8	80,0	100,0
	Total	10	100,0	100,0

معلوماتي؟ نظام البنك لدى هل				
		Fréquence	Pourcentage	Pourcentage valide
Valide	نعم	10	100,0	100,0

الاعمال لاستمرارية خطة لديك هل				
		Fréquence	Pourcentage	Pourcentage valide
Valide	نعم	10	100,0	100,0

Authentication النظام لحماية الهوية من التحقق تقنيات استخدام				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	1	10,0	20,0
	فعال تطبيق	8	80,0	100,0
	Total	10	100,0	100,0

الوظيفة طبيعة حسب الحساسة المعلومات الى الوصول تقييد				
		Fréquence	Pourcentage	Pourcentage valide
Valide	موجود غير	2	20,0	20,0
	التطبيق جيد	2	20,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

البيانات تغيير عدم لضمان حماية وسائل او التشفير تقنيات استخدام				
		Fréquence	Pourcentage	Pourcentage valide
Valide	موجود غير	1	10,0	10,0
	التطبيق جيد	3	30,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

الامنية المعايير وفق دوري بشكل المرور كلمات تا				
		Fréquence	Pourcentage	Pourcentage valide
Valide	موجود غير	2	20,0	20,0
	التطبيق جيد	8	80,0	100,0
	Total	10	100,0	100,0

البيانات تغيير عدم لضمان حماية وسائل او التشفير تقنيات استخدام				
		Fréquence	Pourcentage	Pourcentage valide
Valide	موجود غير	1	10,0	10,0
	التطبيق جيد	3	30,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

المعلومات تسريب بمخاطر الموظفين توعية				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق جيد	4	40,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

Audit Logs النظام داخل البيانات استخدام لتتبع اليات وجود				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	1	10,0	20,0
	فعال تطبيق	8	80,0	100,0
	Total	10	100,0	100,0

المعلومات تسريب بمخاطر الموظفين توعية				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق جيد	4	40,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

البيانات في التلاعب لمعالجة واضحة اليات وجود				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق جيد	4	40,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

البيانات في التلاعب لمعالجة واضحة اليات وجود				
		Fréquence	Pourcentage	Pourcentage valide
Valide	التطبيق جيد	4	40,0	40,0
	فعال تطبيق	6	60,0	100,0
	Total	10	100,0	100,0

قائمة الملاحق

الخدمة استمرارية على التأثير دون النظام دورية الصيانة أوقات تحديد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	1	10,0	10,0
	التطبيق جيد	5	50,0	60,0
	فعال تطبيق	4	40,0	100,0
Total	10	100,0	100,0	

Segregation of Duties . للحد التلاعب من المهام فصل				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	2	20,0	20,0
	التطبيق جيد	3	30,0	50,0
	فعال تطبيق	5	50,0	100,0
Total	10	100,0	100,0	

المخاطر الكبروني سجل على الاعتماد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	5	50,0	50,0
	فعال تطبيق	5	50,0	100,0
Total	10	100,0	100,0	

الازمات لادارة مختصة فرق تخصيص				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	2	20,0	30,0
	فعال تطبيق	7	70,0	100,0

مستمر بشكل للمستخدمين البيانات توفر ضمان				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	6	60,0	70,0
	فعال تطبيق	3	30,0	100,0
Total	10	100,0	100,0	

الاعطال لتفادي مستمر بشكل الأنظمة اداء مراقبة				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	4	40,0	40,0
	فعال تطبيق	6	60,0	100,0
Total	10	100,0	100,0	

دوري بشكل الاعمال استمرارية خطة تحديث				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	2	20,0	20,0
	التطبيق جيد	5	50,0	70,0
	فعال تطبيق	3	30,0	100,0
Total	10	100,0	100,0	

البيانات في عادية غير تغييرات حدوث عند تنبيه نظم وجود				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	موجود غير	1	10,0	10,0
	التطبيق متوسط	2	20,0	30,0
	التطبيق جيد	1	10,0	40,0
	فعال تطبيق	6	60,0	100,0
Total	10	100,0	100,0	

(BCP) الاعمال استمرارية خطة على الاعتماد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	5	50,0	50,0
	فعال تطبيق	5	50,0	100,0
Total	10	100,0	100,0	

دوري بشكل الاعمال استمرارية خطة تحديث				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	2	20,0	20,0
	التطبيق جيد	5	50,0	70,0
	فعال تطبيق	3	30,0	100,0
Total	10	100,0	100,0	

البنك داخل (DRP) الكوارث من تعافي خطة وجود				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	3	30,0	30,0
	فعال تطبيق	7	70,0	100,0
Total	10	100,0	100,0	

بها مصرح غير المباشرة التعديلات من البيانات قواعد حماية				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	2	20,0	20,0
	فعال تطبيق	8	80,0	100,0
Total	10	100,0	100,0	

دوري بشكل الاحتياطي النسخ أنظمة على الاعتماد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	1	10,0	10,0
	فعال تطبيق	9	90,0	100,0
Total	10	100,0	100,0	

النظام توقف حالة في بديلة تحتية بنية توفر				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق جيد	1	10,0	10,0
	التطبيق متوسط	1	10,0	20,0
	التطبيق جيد	2	20,0	40,0
	فعال تطبيق	6	60,0	100,0
Total	10	100,0	100,0	

الازمات مع للتعامل وواضحة مكتوبة إجراءات وجود				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	3	30,0	40,0
	فعال تطبيق	6	60,0	100,0
Total	10	100,0	100,0	

الازمات لادارة مختصة فرق تخصيص				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	التطبيق متوسط	1	10,0	10,0
	التطبيق جيد	2	20,0	30,0
	فعال تطبيق	7	70,0	100,0
Total	10	100,0	100,0	

قائمة الملاحق

دوري بشكل المخاطر تقييم			
	Fréquence	Pourcentage	Pourcentage valide
Valide			
التطبيق متوسط	1	10,0	10,0
التطبيق جيد	4	40,0	40,0
فعال تطبيق	5	50,0	50,0
Total	10	100,0	100,0

وفعالية بسرعة للالزمات الاستجابة				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide				
التطبيق متوسط	2	20,0	20,0	20,0
التطبيق جيد	5	50,0	50,0	70,0
فعال تطبيق	3	30,0	30,0	100,0
Total	10	100,0	100,0	

دقيق بشكل (RTO) استرجاع زمن تحديد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide				
التطبيق متوسط	2	20,0	20,0	20,0
التطبيق جيد	2	20,0	20,0	40,0
فعال تطبيق	6	60,0	60,0	100,0
Total	10	100,0	100,0	

استمرارية الاعمال بإدارة الخاص ISO 22301 معيار على البنك اعتماد				
	Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide				
موجود غير	2	20,0	20,0	20,0
التطبيق ضعيف	1	10,0	10,0	40,0
التطبيق متوسط	1	10,0	10,0	50,0
التطبيق جيد	2	20,0	20,0	70,0
فعال تطبيق	3	30,0	30,0	100,0
Total	10	100,0	100,0	

Statistiques descriptives			
	N	Moyenne	Ecart type
الا النسخ أنظمة على الاعتماد دوري بشكل احتياطي	10	4,90	,316
حدوث بسرعة البيانات استرجاع اعطال	10	4,60	,516
مستمر بشكل الأنظمة أداء مراقبة الاعطال لتفادي	10	4,60	,516
حالة في بديلة تحتية بنية توفر النظام توقف	10	4,30	1,059
للنظام دورية الصيانة أوقات تحديد الخدمة استمرارية على التأثير دون	10	4,20	,919

Statistiques descriptives			
	N	Moyenne	Ecart type
الا النسخ أنظمة على الاعتماد دوري بشكل احتياطي	10	4,90	,316
دوري بشكل المرور كلمات تغيير الأمنية المعايير وفق	10	4,80	,422
واضحة سياسات على الاعتماد الى الوصول صلاحيات لتحديد المعلومات	10	4,80	,422
التعديلات من البيانات قواعد حماية بها مصرح غير المباشرة	10	4,80	,422
البيانات استخدام لتتبع اليات وجود Audit Logs) النظام داخل	10	4,70	,675
الهوية من التحقق تقنيات استخدام Authentication) النظام لحماية	10	4,70	,675
حدوث بسرعة البيانات استرجاع اعطال	10	4,60	,516
مستمر بشكل الأنظمة أداء مراقبة الاعطال لتفادي	10	4,60	,516
التلا لمعالجة واضحة اليات وجود البيانات في عب	10	4,60	,516
وخلوها البيانات سلامة من التأكد النظام إلى إدخالها قبل الأخطاء من الحفظ أو للمعالجة	10	4,60	,516
تسريب بمخاطر الموظفين توعية المعلومات	10	4,60	,516
حالة في بديلة تحتية بنية توفر النظام توقف	10	4,30	1,059

قائمة الملاحق

لحد التلاعب من المهام فصل Segregation of Duties .	10	4,30	,823
وسائل أو التشفير تقنيات استخدام البيانات تغيير عدم لضمان حماية	10	4,30	1,252
للنظام دورية الصيانة أوقات تحديد الخدمة استمرارية على التأثير دون	10	4,20	,919
للمستخدمين البيانات توفر ضمان مستمر بشكل	10	4,20	,632
حدوث عند تنبيه نظم وجود البيانات في عادية غير تغييرات	10	4,10	1,370
المعلومات الى الوصول تقييد الوظيفة طبيعة حسب الحساسية	10	4,00	1,633
N valide (liste)	10		

Corrélations			
		الاعمال استمرارية البنوك في	نظام امن مستوى البنوك في المعلومات
في المعلومات نظام امن مستوى البنوك	Corrélation de Pearson	1	,293
	Sig. (bilatérale)		,411
	N	10	10
البنوك في الاعمال استمرارية	Corrélation de Pearson	,293	1
	Sig. (bilatérale)	,411	
	N	10	10

Statistiques descriptives			
	N	Moyenne	Ecart type
الكوارث من تعافي خطة وجود البنك داخل (DRP)	10	4,70	,483
الا لإدارة مختصة فرق تخصيص زومات	10	4,60	,699
وواضحة مكتوبة إجراءات وجود الازمات مع للتعامل	10	4,50	,707
الالكتروني سجل على الاعتماد للمخاطر	10	4,50	,527
الا استمرارية خطة على الاعتماد عمال (BCP)	10	4,50	,527
دوري بشكل المخاطر تقييم (RTO) استرجاع زمن تحديد	10	4,40	,699
دقيق بشكل	10	4,40	,843
وفعالية بسرعة للازمات الاستجابة	10	4,10	,738
الاعمال استمرارية خطة تحديث دوري بشكل	10	4,10	,738
22301 معيار على البنك اعتماد استمرارية الا بإدارة الخاص ISO عمال	10	3,10	1,729
N valide (liste)	10		

Corrélations				
		سرية المعلومات	سلامة المعلومات	المعلومات توافر
المعلومات سرية	Corrélation de Pearson	1	,655	,179
	Sig. (bilatérale)		,040	,621
	N	10	10	10
المعلومات سلامة	Corrélation de Pearson	,655	1	,675
	Sig. (bilatérale)	,040		,032
	N	10	10	10
المعلومات توافر	Corrélation de Pearson	,179	,675	1
	Sig. (bilatérale)	,621	,032	
	N	10	10	10
في الاعمال استمرارية البنوك	Corrélation de Pearson	,040	,274	,401
	Sig. (bilatérale)	,913	,443	,251
	N	10	10	10

Tests de normalité						
	البنك نوع	Kolmogorov-Smirnov ^a			Shapiro-Wilk	
		Statistiques	ddl	Sig.	Statistiques	ddl
المعلومات نظام امن مستوى البنوك في	عمومي	,183	5	,200	,935	5
	خاص	,328	3		,871	3
	مختلط	,260	2			
البنوك في الاعمال استمرارية	عمومي	,275	5	,200	,879	5
	خاص	,304	3		,907	3
	مختلط	,260	2			

Tests de normalité ^{a,d}					
	حجم المؤسسة	Kolmogorov-Smirnov ^a			Shapiro-Wilk
		Statistiques	ddl	Sig.	Statistiques
المعلومات نظام امن مستوى البنوك في	كبير	,190	6	,200	,953
	صغير	,253	3		,964
في الاعمال استمرارية البنوك	كبير	,360	6	,014	,770
	صغير	,385	3		,750

قائمة الملاحق

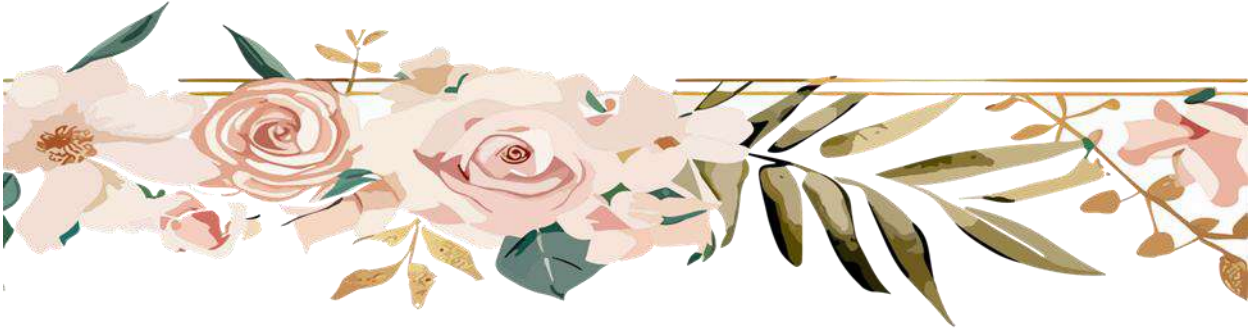
البنك نوع		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	عمومي	5	50,0	50,0	50,0
	خاص	3	30,0	30,0	80,0
	مختلط	2	20,0	20,0	100,0
	Total	10	100,0	100,0	

ANOVA					
البنوك في المعلومات نظام امن مستوى					
	Somme des carrés	ddl	Carré moyen	F	Sig.
Intergruppes	,034	2	,017	,146	,867
Intragruppes	,809	7	,116		
Total	,842	9			

Récapitulatif du test Kruskal-Wallis pour échantillons indépendants	
N total	10
Statistiques de test	2,027 ^{a,b}
Degré de liberté	2
Sig. asymptotique (test bilatéral)	,363



الفهرس



الفهرس

الصفحة	العنوان
I	الإهداء
III	الشكر والتقدير
IV	ملخص الدراسة
VI	قائمة المحتويات
VIII	قائمة الجداول
IX	قائمة الاشكال
XIII	قائمة الملاحق
XIV	قائمة المختصرات
١	المقدمة
1	الفصل الأول: الأدبيات النظرية لأمن نظام المعلومات وإدارة استمرارية الأعمال
3	المبحث الأول: ماهية أمن نظام المعلومات
3	المطلب الأول: مفهوم أمن نظام المعلومات
3	أولاً: مفهوم أمن نظام المعلومات
5	ثانياً: أهداف أمن نظام المعلومات

قائمة الفهرس

7	ثالثًا: مكونات أمن نظام المعلومات
11	المطلب الثاني: أساسيات أمن نظام المعلومات
11	أولًا: متطلبات أمن نظم المعلومات
13	ثانيًا: استراتيجية أمن نظم المعلومات
17	ثالثًا: معايير أمن نظم المعلومات
17	المطلب الثالث: المخاطر التي تواجه أمن نظام المعلومات والتدابير المتخذة
17	أولًا: المخاطر التي تهدد أمن نظم المعلومات
19	ثانيًا: التدابير المتخذة لضمان أمن نظم المعلومات ووسائل الحماية
20	المبحث الثاني: ماهية إدارة استمرارية الأعمال
21	المطلب الأول: مفهوم إدارة استمرارية الأعمال
21	أولًا: مفهوم إدارة استمرارية الأعمال
22	ثانيًا: أهمية إدارة استمرارية الأعمال
23	ثالثًا: متطلبات إدارة استمرارية الأعمال
27	لمطلب الثاني: معايير نظام إدارة استمرارية الأعمال وفق ISO 22301
27	أولًا: مفهوم معيار ISO 22301

قائمة الفهرس

32	ثانيًا: مجال تطبيق إدارة استمرارية الاعمال
33	المطلب الثالث: العلاقة بين أمن نظام المعلومات وإدارة استمرارية الأعمال
34	أولًا: العلاقة التكاملية بين أمن نظام المعلومات وإدارة استمرارية الأعمال
36	المبحث الثالث: الدراسات السابقة المتعلقة بأمن نظام المعلومات وإدارة استمرارية الأعمال
36	أولًا: دراسات السابقة باللغة العربية
41	ثانيا : دراسات السابقة باللغة الاجنبية
50	المطلب الثاني: أبعاد أمن نظام المعلومات وإدارة استمرارية الأعمال
50	اولا : ابعاد امن نظام المعلومات
52	ثانيا: ابعاد ادارة استمرارية الاعمال
54	المطلب الثالث: مقارنة بين الدراسات السابقة والدراسة الحالية
57	اولا: اوجه التشابه بين دراسات الحالية وسابقة
57	ثانيا : اوجه الاختلاف بين دراسات سابقة وحالية
60	ثالثا: اسهامات الدراسة السابقة في الدراسة الحالية
61	خلاصة الفصل الأول
61	الفصل الثاني: الدراسة الميدانية لمساهمة أمن نظام المعلومات في دعم إدارة استمرارية الأعمال بالبنوك الجزائرية بورقلة

قائمة الفهرس

64	المبحث الأول: الطريقة والأدوات المستخدمة في الدراسة الميدانية
64	المطلب الأول: الطريقة المعتمدة في الدراسة
64	اولا: منهج الدراسة
65	ثانيا: ادوات جمع البيانات
66	ثالثا : لمحة عامة حول البنوك
77	رابعا : مجتمع وعينة الدراسة
85	المطلب الثاني: تقديم أداة الدراسة
86	اولا: معلومات عامة
88	ثانيا : مقياس الدراسة
90	المطلب الثالث: الأدوات الإحصائية المستخدمة
92	المبحث الثاني: عرض ومناقشة النتائج
92	المطلب الأول: عرض وتحليل نتائج محاور الدراسة
92	اولا : متغير أمن نظام المعلومات
126	ثانيا : متغير إدارة استثمارية الاعمال
	ثالثا : عرض وتحليل المؤشرات الاحصائية لأجمالي متغيرات الدراسة
153	المطلب الثاني: عرض وتحليل نتائج اختبار فرضيات الدراسة

قائمة الفهرس

161	المطلب الثالث: مناقشة نتائج الدراسة
161	اولا: واقع متغيرات الدراسة
165	ثانيا : مناقشة النتائج المتعلقة بالعلاقة بين متغيري الدراسة والفروق حسب خصائص البنوك
171	خلاصة الفصل الثاني
173	الخاتمة
177	قائمة المراجع
182	الملاحق
204	الفهرس

الْحَمْدُ لِلَّهِ