وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي – تبسة–

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم: علوم التسيير الرقم التسلسلي: ---------- / 2025

فرع: علوم التسيير

التخصص: إدارة أعمال

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي (ل م د)

موسومة بـ:

أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني في المؤسسات المالية

دراسة حالة: بنك الجزائر الخارجي BEA وكالة تبسة–46–

من إعداد الطالبين :

– إيمان زيطاري

– سمير دوالي

إشراف الدكتورة:

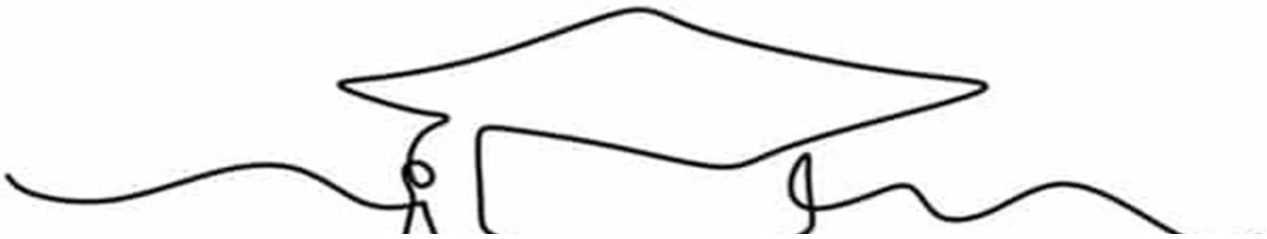
– هيبة الله أوريسي

أعضاء لجنة المناقشة:

الاسم واللقب	الرتبة العلمية	الصفة
أ.د. عمار براهمية	أستاذ التعليم العالي	رئيسا
د. هيبة الله أوريسي	أستاذ محاضر "ب"	مشرفا ومقررا
د. فاطمة الزهرة عايب	أستاذ محاضر "ب"	عضوا مناقشا

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم



شكر وعرفان

قال تعالى في كتابه الكريم:

" وَلَئِن شَكَرْتُمْ لَأَزِيدَنَّكُمْ" إبراهيم: (7)

فالحمد لله أولًا وأخرًا، ظاهرًا وباطنًا، على توفيقه وتيسيره لإتمام هذا البحث العلمي، سائلين المولى عز وجل أن يجعله عملًا خالصًا نافعا، وأن ينفع به قارئه ودارسه، والصلاة والسلام على خير خلق الله محمد بن عبد الله، وعلى آله وصحبه ومن تبعهم بإحسان إلى يوم الدين.

وبعد، لا يسعنا إلا أن نتقدم بأسمى عبارات الشكر والتقدير لمشرفتنا الفاضلة الأستاذة "**هيبة الله أوريسي**"، لما بذلته من جهد كبير، وتوجيهات سديدة، ومتابعة مستمرة كانت لها أبلغ الأثر في إنجاز هذا العمل، فجزاكِ الله خير الجزاء وبارك في علمكِ وعملكِ، وجعل ما قدمتِ في ميزان حسناتكِ.

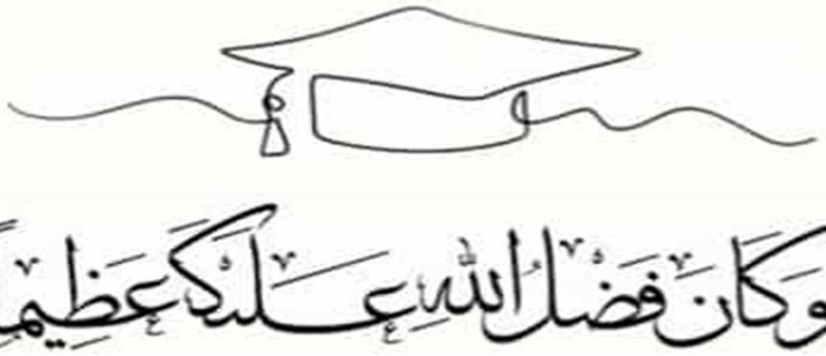
كما نعبر عن بالغ شكرنا وامتناننا **للأساتذة أعضاء لجنة المناقشة** على قبولهم مناقشة هذا العمل العلمي، وعلى ملاحظاتهم التي ستكون لنا نبراسًا للتطوير والتحسين.

ولا يفوتنا أن نتوجه بالشكر الجزيل **لموظفي بنك الجزائر الخارجي BEA وكالة تبسة –46–**، على تعاونهم الكريم، وحسن استقبالهم لنا، وما قدموه من تسهيلات ساهمت في جمع المادة العلمية لهذه الدراسة.

وأخيرًا، نتقدم بكل التقدير والعرفان لكل من علمنا حرفًا، وساهم في تشكيل معارفنا خلال مشوارنا الجامعي.

ومن شكر النعمة، نال دوامها وزيادتها، فشكرًا لكم جميعًا.

إهداء



"من قال أنا لها... نالها "

وقد كنتُ لها رغم الصعوبات، ورغم أن الطريق لم يكن سهلاً، لكنني سرتُ فيه بإصرار حتى بلغت المدى، وها أنا اليوم أهدي ثمرة تعبي وفخري إلى من كان لهم الفضل بعد الله:

إلى من كانت دعواتها زادي، وحبها سندي، إلى نبع الحنان وعين الرضا... **أمي الحبيبة**، حفظكِ الله وأطال في عمركِ، لكِ كلّ الامتنان؛

إلى من حملتُ اسمه بفخر واعتزاز، إلى قدوتي ومصدر عزيمتي الأولى، **أبي العزيز**، دمتَ فخرًا ودعماً لا ينضب؛

إلى من كانت نورًا في دربي، وسندًا في صغري، إلى من غابت عن الحياة لكنها باقية في قلبي وذكرياتي... **جدتي الغالية**، رحمكِ الله وجعل مثواكِ الجنة؛

إلى **إخوتي الأحبّة إسلام، إياد، لجين**، أنتم النبض الذي يسكن القلب، والكتف الذي لا يميل، والسند الذي لا يخيب، كنتم دومًا العون في ضعفي، والفرح في قوتي، ورفاق الدرب في كل حين، حفظكم الله لي؛

إلى من شاركتني كل خطوة من مشوار التخرج ...**إيمان**، شكراً لكِ على كل الدعم والتعاون خلال هذه الرحلة، فقد كان وجودك إلى جانبي قوة ودافعاً كبيراً لي؛

إلى القلب الطيب والروح النقية... **موسى** ، شكرًا لوجودك الدائم والداعم؛

إلى أصدقاء العمر، ومن جمعتني بهم أجمل اللحظات... **معز، محمد فضلاء، منذر، حسام، عبد الرحمن، سيف الدين، نوفل**، حفظكم الله ودام صداقتكم؛

إلى من آمنوا بي قبل أن أؤمن بنفسي، إلى من يفرحهم نجاحي كأنه إنجازهم ...**عائلتي الغالية**، شكرًا لقلوبكم النقية؛

وأخيرًا ...إلى نفسي التي لم تستسلم، التي واصلت وثابرت وآمنت ...شكرًا لي **أنا**.

سمير دوالي

إهداء

الحمد لله الذي بنعمته تتمّ الصالحات، وبتوفيقه تُدرك الغايات

ها أنا اليوم أقف على أعتاب التخرّج، أجني ثمار تعبٍ وسهرٍ وعملٍ متواصل، وقلبي يغمره الامتنان والعرفان...

إلى من غرست فيّ أولى بذور الحب والعطاء، إلى رمز الحنان والدفء، إلى **أمي الحبيبة** دمتِ لي سندًا ونبعًا لا ينضب، حفظكِ الله ورعاكِ؛

إلى من علّمني أن الطموح لا سقف له، إلى **والدي الغالي**، من لم يبخل يومًا بدعمه ومساندته جزاكَ الله عنّي خير الجزاء، وحفظك الله ورعاك؛

إلى من كانت الأخوّة معهن نعمة لا تقدّر بثمن، إلى رفيقات الروح، ورفيقات القلب قبل الدرب ... **آية، تقوى، رؤيا**، أهديكنّ هذا الإنجاز، فهو منكن وبكن، لأنكن كنتم دائمًا السبب في أن أواصل، وأحلم، وأصل؛

إلى من كان رفيق دربي في كل خطوة من مشوار التخرج... **سمير**، شكرًا لكِ على كل ما قدمته من دعم ومساندة، لقد كان وجودك بجانبي مصدر قوة، ودافعًا كبيرًا للاستمرار والوصول، ممتنة لكل لحظة شاركتني فيها هذه الرحلة؛

إلى **آية**، رفيقة القلب قبل الدرب ...كنتِ الحضن وقت الضيق، شكرًا لأنكِ كنتِ دائمًا قريبة، بحبك، بلطفك، وبصدقك؛

إلى كل **عائلتي**، أنتم الملجأ الآمن في كل محطات الحياة، في دعمكم وجدت القوة، وفي دعائكم كان العون؛

إلى **نفسي**، التي لم تعرف الاستسلام، التي قاومت، وجاهدت، ولم تضعف، التي آمنت بقدراتها، واستمرت رغم كل الصعاب ... شكراً لكِ على كل لحظة صبر، وكل نبضة عزيمة؛

وفي الأخير... إلى كل من يكن لي المحبة والاحترام.

إيمان زيطاري

فهرس المحتويات

فهرس المحتويات

فهرس المحتويات

فهرس الجداول

فهرس الجداول

فهرس الأشكال

فهرس الأشكال

فهرس الملاحق

فهرس الملاحق

مقدمة

مقدمة

أصبحت مؤسسات القرن الواحد والعشرين تعمل في بيئة رقمية متغيرة وسريعة التطور، حيث بات الاعتماد على التكنولوجيا من أبرز السمات المميزة لعصرنا الحالي، مما فرض على هذه المؤسسات، خصوصًا المؤسسات المالية، تحديات جديدة تتعلق بكيفية حماية معلوماتها وضمان أمن أنظمتها الرقمية. ومن بين أهم العوامل المؤثرة في مسارات العمل داخل هذه المؤسسات نجد القيادة المتبعة والسلوكيات الرقمية التي يتبناها الأفراد، سعياً لتحقيق أهداف المؤسسة والحفاظ على بقائها واستمراريتها في بيئة رقمية محفوفة بالمخاطر السيبرانية.

لقد أثبت الواقع أن النمط التقليدي للقيادة، المعتمد على المركزية والانغلاق المعلوماتي، لم يعد مجدياً في ظل التحول الرقمي المتسارع، بل أصبح عائقاً أمام التفاعل السليم مع المتغيرات الرقمية وتحديات الأمن السيبراني. الأمر الذي دفع المؤسسات الحديثة إلى تبني أنماط قيادية جديدة تتماشى مع هذه التحولات، من أبرزها "القيادة الرقمية" التي تقوم على تسخير أدوات التكنولوجيا في تسيير الموارد البشرية وتعزيز التفاعل الإيجابي مع البيئة الرقمية، خاصة عندما يتعلق الأمر بترسيخ ثقافة الأمن السيبراني كعنصر أساسي في نجاح المؤسسات وحمايتها.

ومع تزايد اعتماد المؤسسات على الأنظمة الرقمية، أصبح سلوك الأمن السيبراني أحد الركائز الأساسية التي لا غنى عنها لضمان استقرار العمليات وحماية الأصول الرقمية. فرغم أن هذا السلوك يُعد في ظاهره التزاماً وظيفياً، إلا أنه في عمقه يُمثل توجهاً طوعياً ووعياً ذاتياً من الموظفين نحو حماية مؤسساتهم من الأخطار الرقمية. ويُعد هذا السلوك امتداداً لثقافة المؤسسة ومرآة لمدى فاعلية القيادة الرقمية في التأثير على تصرفات الأفراد، خاصة في ظل تعقيد التهديدات الإلكترونية وتنوعها، مما يستدعي تعزيز هذا السلوك باستمرار ومعرفة العوامل المؤثرة فيه.

أولا: إشكالية الدراسة

في ظل التوجه نحو الرقمنة، سعت المؤسسات المالية الجزائرية إلى تبني أنماط قيادية رقمية تساهم في تعزيز ثقافة الأمن السيبراني، بالنظر إلى أهميته في حماية البيانات وضمان استمرارية النشاط المالي. وفي هذا السياق، يعمل بنك الجزائر الخارجي على تفعيل القيادة الرقمية في إدارة فروعه، ومن بينها الوكالة محل الدراسة بولاية تبسة، من خلال التأثير في سلوكيات الأفراد نحو مزيد من الالتزام الواعي بالممارسات السيبرانية.

وعليه، تتمثل إشكالية الرئيسية للدراسة في التساؤل الآتي:

ما مدى تأثير القيادة الرقمية على تعزيز سلوك الأمن السيبراني لدى الموظفين بينك الجزائر الخارجي BEA وكالة تبسة46؟

وللإجابة على هذه الإشكالية تطرح الأسئلة الفرعية التالية:

- ما الأبعاد التي تتجلى من خلالها القيادة الرقمية في إدارة المخاطر السيبرانية في بنك الجزائر الخارجي؟
- ما مدى وعي موظفو بنك الجزائر الخارجي بمفاهيم وممارسات الأمن السيبراني؟
- ما دور الممارسات القيادية الرقمية في ترسيخ ثقافة الأمن السيبراني داخل بنك الجزائر الخارجي؟
- ما نوع السلوكيات السيبرانية التي يتبناها الموظفون في بنك الجزائر الخارجي نتيجة لتوجيهات القيادة الرقمية؟

ثانيا: فرضيات الدراسة

لمعالجة إشكالية الدراسة وللإجابة على التساؤلات الفرعية، تم اعتماد الفرضيتين الرئيسيتين الآتيتين:

1-الفرضية الرئيسية الأولى

تتضمن الفرضية الرئيسية الأولى على:

-**الفرضية الصفرية H0**: لا يوجد أثر ذو دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني لدى موظفي بنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1**: يوجد أثر ذو دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني لدى موظفي بنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

وتنقسم إلى الفرضيات الفرعية التالية:

1-1-الفرضية الفرعية الأولى: تتمثل في:

-**الفرضية الصفرية H0**: لا يوجد أثر ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1**: يوجد أثر ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

1-2-الفرضية الفرعية الثانية: تكمن في:

-**الفرضية الصفرية H0**: لا يوجد أثر ذو دلالة إحصائية للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1**: يوجد أثر ذو دلالة إحصائية للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

1-3-الفرضية الفرعية الثالثة: تتمحور حول:

-**الفرضية الصفرية H0:** لا يوجد أثر ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:** يوجد أثر ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

1-4-الفرضية الفرعية الرابعة: تتمثل في:

-**الفرضية الصفرية H0:** لا يوجد أثر ذو دلالة إحصائية للمشاركة والتعاون على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:** يوجد أثر ذو دلالة إحصائية للمشاركة والتعاون على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

2-الفرضية الرئيسية الثانية

تنقسم الفرضية الرئيسية الثانية إلى:

-**الفرضية الصفرية H0:** لا توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى للخصائص الشخصية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية) ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:** توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى للخصائص الشخصية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

وتنقسم إلى الفرضيات الفرعية التالية:

2-1-الفرضية الفرعية الأولى: تكمن في:

-**الفرضية الصفرية H0:** لا توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى لمتغير المستوى العلمي،ببنك الجزائر الخارجي BEA-وكالة تبسة 46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:**توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى لمتغير المستوى العلمي،ببنك الجزائر الخارجي BEA-وكالة تبسة 46، عند مستوى الدلالة ($\propto \leq 0.05$).

2-2-الفرضية الفرعية الثانية: تتمحور في:

-**الفرضية الصفرية H0:** لا توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تعزى لمتغير المركز الوظيفي،ببنك الجزائر الخارجي BEA-وكالة تبسة 46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:**توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى لمتغير المركز الوظيفي،ببنك الجزائر الخارجي BEA-وكالة تبسة 46، عند مستوى الدلالة ($\propto \leq 0.05$).

2-3-الفرضية الفرعية الثالثة: تتمثل في:

-**الفرضية الصفرية H0:** لا توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزىلمتغير الخبرة المهنية،ببنك الجزائر الخارجي BEA-وكالة تبسة46، عند مستوى الدلالة ($\propto \leq 0.05$).

-**الفرضية البديلة H1:**توجد فروق ذات دلالة إحصائية في إدراك الموظفين لتأثير القيادة الرقمية على سلوك الأمن السيبراني تُعزى لمتغير الخبرة المهنية،ببنك الجزائر الخارجي BEA-وكالة تبسة 46، عند مستوى الدلالة ($\propto \leq 0.05$).

ثالثا: أهمية الدراسة

تكتسب هذه الدراسة أهمية من زاويتين نظرية وتطبيقية، على النحو التالي:

1-الأهمية النظرية:

تنبع الأهمية النظرية من تناول موضوعين حديثين ومترابطين، هما "القيادة الرقمية" و"سلوك الأمن السيبراني"، وهما من المفاهيم الإدارية والتقنية المعاصرة التي فرضتها التحولات الرقمية السريعة، خاصة في بيئات العمل الحساسة مثل: المؤسسات المالية،وتتجلى أهمية الدراسة من خلال:

- التوجه المتزايد في الفكر الإداري المعاصر نحو استكشاف القيادة الرقمية كأح د الأنماط القيادية المتماشية مع متطلبات التحول الرقمي، مما يجعلها بحاجة إلى مزيد من التأطير والدراسة خاصة في السياق المالي الجزائري؛
- إبراز سلوك الأمن السيبراني كمفهوم أمني مستحدث يمثل دعامة أساسية لحماية البيانات والأنظمة في المؤسسات المالية؛
- الربط بين القيادة الرقمية وسلوك الأمن السيبراني يعتبر إسهاماً علميا جديداً، نظراً لندرة الدراسات التي عالجت العلاقة بين المتغيرين داخل البيئة الجزائرية، وبشكل خاص في القطاع البنكي.

2-الأهمية التطبيقية:

تتجلى الأهمية التطبيقية للدراسة في سعيها إلى تقديم معطيات علمية وميدانية يمكن أن تساعد مسؤولي بنك الجزائر الخارجي-وكالة تبسة 46-على فهم الدور الذي تلعبه القيادة الرقمية في تعزيز السلوكيات السيبرانية السليمة لدى الموظفين، وذلك من خلال:

- تقديم تصور علمي لواقع القيادة الرقمية داخل الوكالة؛
- تحديد مستوى تبني سلوك الأمن السيبراني لدى الموظفين، والعوامل المؤثرة فيه؛
- تقديم توصيات عملية تدعم ثقافة الأمن السيبراني في المؤسسات المالية الجزائرية عبر نماذج قيادية ملائمة للبيئة الرقمية، بما يسهم في الوقاية من التهديدات السيبرانية المحتملة.

رابعا: أهداف الدراسة

يهدف هذا البحث إلى تحقيق مجموعة من الأهداف، يمكن تصنيفها إلى رئيسية وفرعية كما يلي:

1-الهدف الرئيسي:

التعرف على واقع ممارسة القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني داخل بنك الجزائر الخارجي-وكالة تبسة.46

2-الأهداف الثانوية:

- ✓ إبراز مدى تأثير القيادة الرقمية على تعزيز سلوك الأمن السيبراني لدى موظفي بنك الجزائر الخارجي؛
- ✓ تحديد مفاهيم القيادة الرقمية وأبعادها ضمن السياق المؤسساتي المالي؛
- ✓ توضيح مفاهيم الأمن السيبراني وسلوكياته ومتطلبات تطبيقه داخل المؤسسة المالية؛
- ✓ تقديم نتائج وتوصيات قابلة للتطبيق لتحسين ممارسات القيادة الرقمية والأمن السيبراني في المؤسسات المالية

خامسا: دوافع اختيار الموضوع

يعزى اختيار الباحث لموضوع الدراسة إلى مجموعة من الدوافع، أبرزها:

- ✓ الرغبة في التعمق في موضوع حديث وحيوي يجمع بين القيادة الرقمية والأمن السيبراني؛
- ✓ ارتباط الموضوع بشكل مباشر بتخصص الباحث الأكاديمي؛
- ✓ قلة الدراسات والبحوث التي تناولت العلاقة بين القيادة الرقمية وسلوك الأمن السيبراني في البيئة المالية الجزائرية، مما يبرز الحاجة إلى إثراء هذا المجال العلمي؛

- ✓ الأهمية البالغة التي يكتسبها موضوع الأمن السيبراني في ظل تصاعد التهديدات الرقمية، والحاجة إلى تفعيل دور القيادة الرقمية في مواجهتها داخل المؤسسات المالية.

سادسا: حدود الدراسة

سعياً لفهم إشكالية الدراسة بشكل شامل، تم تحديد نطاقها وفق ما يلي:

1-الحدود الموضوعية:

تنصب الدراسة على تحليل أثر القيادة الرقمية، بأبعادها الأربعة (الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون)، بوصفها متغيرًا مستقلًا، على سلوك الأمن السيبراني بوصفه متغيرًا تابعًا، في بيئة العمل البنكية.

2-الحدود المكانية:

اقتصرت الدراسة الميدانية على بنك الجزائر الخارجي – وكالة تبسة 46، باعتباره نموذجًا للمؤسسات المالية موضوع الدراسة.

3-الحدود الزمانية:

تمت الدراسة خلال الفترة الممتدة من 16 مارس 2025 إلى 17 أفريل 2025، وهي الفترة التي جُمعت فيها البيانات وتم خلالها تحليل واقع القيادة الرقمية وسلوك الأمن السيبراني في الوكالة.

سابعا: منهج الدراسة

للإجابة على تساؤلات الدراسة واختبار فرضياتها، تم الاعتماد على ما يلي:

- ✓ **في الجانب النظري:** تم استخدام المنهج الوصفي، من خلال استعراض وتحليل الأدبيات والمراجع النظرية ذات الصلة بمفهومي القيادة الرقمية وسلوك الأمن السيبراني، مع التركيز على تحديد أبعاد العلاقة بين المتغيرين.
- ✓ **في الجانب التطبيقي:** تم اعتماد منهج دراسة الحالة مستعينين بالمنهج التحليلي، عبر تحليل البيانات المستخلصة من الاستبيان الموجه إلى موظفي بنك الجزائر الخارجي – وكالة تبسة 46، بهدف تشخيص واقع القيادة الرقمية وتأثيرها في السلوكيات السيبرانية داخل المؤسسة، ومقارنة ذلك بنتائج الجانب النظري.

ثامنا: هيكل الدراسة

تماشيًا مع أهداف الدراسة وفرضياتها، تم تنظيم محتواها وفق الهيكل التالي:

- ✓ **الفصل الأول بعنوان التأصيل النظري للقيادة الرقمية وسلوك الأمن السيبراني،** حيث يتناول هذا الفصل المفاهيم النظرية الأساسية المتعلقة بالقيادة الرقمية وسلوك الأمن السيبراني في المؤسسات

المالية، بما في ذلك الأبعاد، الخصائص، والدوافع، مع التطرق إلى تحديات التحول الرقمي، بالإضافة إلى عرض مفهوم الأمن السيبراني، عناصره، أبعاده، وآليات تطبيقه. كما يتضمن هذا الفصل استعراضًا لأبرز الدراسات السابقة ذات الصلة.

- ✓ **الفصل الثاني بعنوان الدراسة الميدانية في المؤسسة المالية** ، حيث يُخصص هذا الفصل لبنك الجزائر الخارجي وكالة تبسة –46–، ويشمل عرض تصميم الدراسة، أدوات جمع البيانات، والمنهجية الإحصائية المعتمدة، إلى جانب تحليل بيانات الاستبيان، وصف خصائص العينة، واختبار الفرضيات المقترحة.

تاسعا:صعوبات البحث

واجهت الدراسة مجموعة من التحديات، يمكن تلخيص أبرزها فيما يلي:

- ✓ ندرة المراجع الأكاديمية المتخصصة في موضوع القيادة الرقمية وسلوك الأمن السيبراني في المؤسسات المالية؛
- ✓ ضعف التفاعل من قبل بعض موظفي البنك أثناء مرحلة جمع البيانات، نتيجة للتحفظ أو ضيق الوقت، ما تطلب بذل جهود إضافية لضمان تمثيل مناسب للعينة.

الفصل الأول: التأصيل النظري للقيادة الرقمية وسلوك الأمن السيبراني

تمهيد:

تُعدّ القيادة الرقمية من بين أهم العوامل المؤثرة على سلوك الأمن السيبراني في المؤسسات المالية، حيث أصبحت هذه المؤسسات تواجه تحديات متزايدة تتعلق بأمن المعلومات وحماية البيانات، وذلك نتيجة لتطور الهجمات السيبرانية، والتغيرات التكنولوجية المتسارعة، بالإضافة إلى العوامل التنظيمية والتشريعية. هذه التحديات قد تؤثر على استقرار المؤسسة وسمعتها، مما يستدعي تبنّي نهج قيادي رقمي قادر على تعزيز الوعي السيبراني، وتطوير استراتيجيات استباقية للتصدي للمخاطر المحتملة . في هذا السياق، يُصبح دور القائد الرقمي محوريًا في توجيه المؤسسة نحو تبنّي سياسات أمنية قوية، وتعزيز ثقافة الأمن السيبراني بين الموظفين، مما يسهم في تقليل احتمالات الاختراقات وتقوية أنظمة الحماية. كما يمكن للقائد الرقمي استثمار التحديات الأمنية وتحويلها إلى فرص لتعزيز البنية التحتية الرقمية، وتحقيق التوازن بين الابتكار وحماية البيانات.

من خلال هذا الفصل، سيتم التطرق على تأثير القيادة الرقمية لتعزيز سلوك الأمن السيبراني داخل المؤسسات، وذلك من خلال مبحثين المتمثلين فيمايلي:

- **المبحث الأول: مدخل نظري إلى القيادة الرقمية والأمن السيبراني؛**
- **المبحث الثاني: الدراسات السابقة.**

المبحث الأول: مدخل نظري إلى القيادة الرقمية والأمن السيبراني

أصبحت القيادة الرقمية من المواضيع الحديثة ذات الأهمية الكبيرة في الإدارة والتكنولوجيا، نظرًا لدورها المحوري في تعزيز الحماية السيبرانية داخل المؤسسات المالية، فهي تساهم في توجيه السياسات الأمنية، ورفع الوعي بالمخاطر الإلكترونية، مما يساعد في ضمان استمرارية المؤسسة في بيئة رقمية مليئة بالتحديات الأمنية. ومع تصاعد الهجمات السيبرانية، أصبح من الضروري تبنّي قيادة رقمية فعالة لتعزيز سلوك الأمن السيبراني، من خلال تطوير استراتيجيات متقدمة واعتماد أحدث وسائل الحماية.

وعليه، فإن نجاح المؤسسات في مواجهة التهديدات الرقمية يعتمد على قيادة واعية تضع الأمن السيبراني ضمن أولوياتها، لذا سيتم التطرق في هذا المبحث إلى المطالب التالية:

المطلب الأول: القيادة الرقمية؛

المطلب الثاني: الأمن السيبراني؛

المطلب الثالث: العلاقة بين القيادة الرقمية والأمن السيبراني.

المطلب الأول: القيادة الرقمية

تُعدّ القيادة الرقمية من الأساليب القيادية الحديثة التي تعتمدها المؤسسات، نظرًا لدورها في تعزيز كفاءة العمل وتطوير الأداء من خلال تبنّي التكنولوجيا والاستراتيجيات الرقمية. فهي تُمكّن القائد من إدارة المؤسسة بفعالية في بيئة رقمية تعتمد على الابتكار والتواصل الفعّال، مما يسهم في تحسين الإنتاجية وتعزيز التكيف مع التحولات التكنولوجية المتسارعة.

أولا: مفاهيم عامة حول القيادة الرقمية

قبل الخوض في مفهوم القيادة الرقمية، من الضروري أولاً فهم معنى القيادة، والتعرف على دور القائد والتمييز بينه وبين المدير، ثم الانتقال إلى تعريف القيادة الرقمية بشكل شامل.

1-تعريف القيادة والقائد:

1-1-تعريف القيادة (Leadership):

بسبب الاهتمام الواسع الذي أولاه العلماء والباحثين لدراسة موضوع القيادة، برزت اختلافات في تحديد مفهوم موحد لها، لذا سيتم عرض بعض التعريفات التي تتميز بالتفصيل والدقة.

تعرف القيادة لغةً بأنها: "نقيض السّوق، ويقود الدابة من أمامها ويسوقها من خلفها". [1]يظهر التعريف أن القيادة تعني التوجيه من الأمام، بينما السّوق يعتمد على الدفع، مما يؤكد دور القائد في الإرشاد والتأثير.

وفي كل من اللغة اليونانية واللاتينية، يُشتق مصطلح (Leadership) من فعل يعني "يفعل أو يقوم بمهمة ما"، كما أشار آرندت (Arndt). حيث يتوافق الفعل اليوناني (Archie) ، الذي يعني يبدأ أو يقود أو يحكم، مع الفعل اللاتيني(Arguer) ، الذي يحمل معنى التحريك أو القيادة.[2]

أما اصطلاحا فقد عرفها (والتر ف أولمر، الابن Walter F Ulmer , Jr) على أنها: " نشاط – أو عملية تأثير – يتمكن فيها الشخص من كسب ثقة الآخرين والتزامهم ويستطيع أن يدفع الجماعة إلى تحقيق مهمة أو مجموعة من المهام دون أن يعتمد في ذلك على منصب أو سلطة رسمية". [3]يشير هذا التعريف إلى أن القيادة عملية تأثير وإقناع، حيث يكسب القائد ثقة الآخرين ويلهمهم لتحقيق الأهداف دون الحاجة إلى سلطة رسمية.

---

[1]–عفاف بن فهم حسن العتيبي، **"دور القيادة في الحد من الجرائم المعلوماتية"** ، مجلة الدراسات الجامعية للبحوث الشاملة، العدد 05، المجلد 01، 2022، ص 3230.

[2]– بلال خلف السكارنة، **القيادة الإدارية الفعالة**، ط2، دار الميسرة للنشر والتوزيع، عمان، الأردن، 2014، ص ص. 95-96

[3]–فيليب سالدر، ترجمة هدى فؤاد، **القيادة**، ط1، مجموعة النيل العربي، القاهرة، مصر، 2008، ص. 18

بينما عرفها كان (kahn) على أنها: "هي نوع من القدرة أو المهارة في التأثير على المرؤوسين بحيث يرغبون في أداء وإنجاز ما يحدده القائد". [1] يظهر هذا التعريف أن الباحث يرى القيادة كمهارة تستخدم للتأثير على الأفراد وتحفيزهم.

كما عرفها فيلدر (Fred.Fiedler) على أنها: " تعني الجهود المبذولة للتأثير أو تغيير سلوك الناس من أجل الوصول إلى أهداف المؤسسة والأفراد معا". [2] يشير هذا التعريف إلى أن القيادة هي عملية تأثير تهدف إلى توجيه سلوك الأفراد لتحقيق أهداف المؤسسة وأهدافهم الشخصية معاً.

وعندما يتم ممارسة القيادة على مستوى الإدارات، فإن ذلك يعرف بالقيادة الإدارية، والتي تعني: "النشاط الذي يمارسه القائد الإداري في مجال اتخاذ القرار وإصداره، وإصدار الأوامر والإشراف الإداري على الآخرين باستخدام السلطة الرسمية وعن طريق التأثير والاستمالة بقصد تحقيق هدف معين". [3] وعليه، فإن القيادة الإدارية تتمثل في اتخاذ القرارات وتوجيه الأفراد من خلال السلطة الرسمية والتأثير، بهدف تحقيق الأهداف المحدد.

مما سبق ذكره يمكن القول أن القيادة تعدّ عملية تأثير تهدف إلى توجيه الأفراد وتحفيزهم لتحقيق الأهداف المشتركة، سواء على المستوى الفردي أو التنظيمي، حيث أنها تعتمد على الإقناع والثقة والتفاعل المستمر، ولا تقتصر على السلطة الرسمية، أما القيادة الإدارية فتعني اتخاذ القرارات ومتابعة تنفيذها من قبل القائد الإداري، مستندًا إلى سلطته الرسمية لتحقيق أهداف محددة.

1-2-تعريف القائد (Leader):

يصبح الشخص قائدا متى اعتقد الناس أنه يستطيع إشباع رغباتهم، ومتى أدرك هو دوافعهم واستجاب لها، ومن هنا تفشل محاولات التأثير من الشخص على الأتباع إذا لم تتصل باحتياجاتهم وتطلعاتهم.[4]

حيث يعرف القائد بأنه:" ذلك الشخص المتأثر باحتياجات الجماعة، والمعبر عن رغبات أعضائها، ومن ثم فهو يركز الاهتمام، ويطلق طاقات أعضاء الجماعة في الاتجاه المطلوب".[5]

---

[1]-التجاني دوح، "**سلوكيات القيادة التحويلية وأثرها على الإبداع التنظيمي** -دراسة حالة – جامعة غرداية"، أطروحة دكتوراه، جامعة غرداية، 2020، ص. 04

[2]-عبد اللطيف صيتي، " **دور أنماط القيادة الإدارية في تدعيم سلوك المواطنة التنظيمية في الجامعات الجزائرية** – دراسة ميدانية على عينة من جامعات قسنطينة، ورقلة، تلمسان –"، أطروحة دكتوراه، جامعة قاصي مرباح، ورقلة، 2021، ص. 05

[3]-بطرس حلاق، **القيادة الإدارية**، منشورات الجامعة الافتراضية السورية،سوريا، 2020، ص. 15

[4]-عبد الله بن عبد الغني الطجم، طلق بن عوض الله السواط، **السلوك التنظيمي**، ط4، دار حافظ للنشر والتوزيع، المملكة العربية السعودية، 2003، ص. 184

[5]-سالم حمد دحبج، "**دور الأتمته في تحسين قيادة المؤسسات الاجتماعية**"، رسالة ماجستير، جامعة قطر، 2023، ص. 42

يبرز هذا التعريف دور القائد في فهم احتياجات الجماعة والتعبير عن رغباتهم، مما يساعد على توجيه طاقاتهم نحو الأهداف المطلوبة.

كما يعرف بأنه: "الشخص الذي يستخدم فنون القيادة للتأثير على سلوك الآخرين، ويمتلك مجموعة من المهارات والقدرات التي اكتسبها خلال العمل والممارسة، وصقلها عن طريق التجارب والتدريب ".[1]وعليه فإن القائد يؤثر على الآخرين من خلال مهاراته وخبراته المكتسبة، والتي تتطور بالممارسة والتدريب.

مما سبق يتضح أن القائد هو شخص يؤثر في الآخرين من خلال فهم احتياجاتهم وتوجيه طاقاتهم، مستندًا إلى مهاراته وخبراته المكتسبة التي تتطور بالممارسة والتدريب.

1-3-الفرق بين القائد والمدير:

قبل التطرق للاختلاف بين القائد والمدير يجب معرفة الفرق بين القيادة والإدارة حيث أنهما مترابطتان لكنهما ليسا متطابقين، فالإدارة تشمل وظائف التخطيط والتنظيم والتوجيه والرقابة، بينما تُعد القيادة جزءًا منها، حيث تركز على التأثير وتحفيز الأفراد لتحقيق الأهداف. وليس كل مدير قائدًا بالضرورة، إذ تتطلب القيادة مهارات إضافية لا يوفرها المنصب الإداري وحده، مما يجعل تنمية القادة داخل الالمؤسسات أمرًا ضروريًا. وتتمحور القيادة حول التغيير والتحفيز والتأثير، بينما تهدف الإدارة إلى تحقيق الاستقرار والنتائج المنتظمة. لذا، فإن الجمع بينهما يحقق الفعالية التنظيمية ويساعد المؤسسات على التكيف مع بيئتها المتغيرة[2].

ويبرز الجدول التالي أبرز الفروقات بين القائد والمدير:

[1]-**المرجع السابق.**

[2]-بشير العلاق، **القيادة الإدارية**، دار اليازوري العلمية للنشر والتوزيع،عمان، الأردن، 2009، ص.24.

جدول رقم (01): الاختلاف بين القائد والمدير

المدير	القائد
- يصدر الأوامر ويقرر؛ - يعتمد على السلطات الممنوحة يهتم بحل المشكلات؛ - متخصص في أداء عمله؛ - يلتزم بتنفيذ التعليمات؛ - الحرص على أن تكون هناك فجوة بينه وبين المرؤوسين؛ - لا يميل إلى التجدد والابتكار؛ - يكون مفروضا على الجماعة؛ - يهتم بتحقيق الأهداف الرسمية؛ - المهارات الإدارية أولا؛ – الاتصالات باتجاه واحد من الأعلى إلى الأسفل.	- يدرب وينصح؛ - يعتمد على الثقة بالنفس والمرؤوسين؛ - يفجر الحماسة في المرؤوسين؛ - يتكلم بالصيغة الجماعية (نحن)؛ - يبحث عن حلول للمشكلات؛ - يستشير ويطلب النصيحة؛ - يفجر العمل الجماعي؛ - يركز على التجديد والابتكار؛ - صلاحياته مستمده من الجماعة؛ - يهتم ببناء العلاقات مع المرؤوسين؛ - سلطة التأثير في الآخرين؛ - الاتصالات من الأعلى إلى الأسفل أو بالعكس.

المصدر: بطرس حلاق، **القيادة الإدارية**، سوريا، منشورات الجامعة الافتراضية السورية، 2020، ص. 97

يوضح الجدول رقم (01) أن المدير يتسم بالصرامة والجدية في عمله، حيث يعتمد على السلطة المخولة له لإصدار التعليمات التي يجب على الموظفين تنفيذها ضمن إطار قانوني محدد. في المقابل، يسعى القائد إلى بناء علاقات قوية مع موظفيه، ويشاركهم في مناقشة الحلول للمشكلات. ورغم اختلاف أسلوب كل منهما في تنفيذ العمل والتعامل مع الموظفين، فإن كلاهما يسعى لتحقيق أهداف المؤسسة.

2-مفهوم القيادة الرقمية:

عند دراسة الأدبيات البحثية في مختلف المجالات، يتضح أن مفهوم القيادة الرقمية لا يزال غير واضح تماماً، ولا يوجد اتفاق عام على تعريف موحد له، ومع ذلك، سيتم تناول في هذه الدراسة مجموعة من التعريفات بهدف توضيح هذا المفهوم بشكل أكثر شمولاً.

2-1-تعريف القيادة الرقمية :

بعد توضيح تعريف القيادة بشكل عام، يمكن الآن التطرق إلى تعريف القيادة الرقمية. لكن قبل ذلك، من المهم الإشارة إلى مصطلح الرقمي (Digital) والذي يعرف في قاموس كامبريدج بأنه: "تسجيل أو تخزين المعلومات كسلسلة من الأرقام بين 1 و 0،لإظهار أن الإشارة موجودة أو غائبة"، أو "كل ما هو مرتبط

بالإشارات الرقمية وتكنولوجيا الكمبيوتر"، أو "إظهار المعلومات على شكل صورة إلكترونية"، أو "استخدام نظام بواسطة الكمبيوتر والأجهزة الإلكترونية الأخرى، حيث يتم إرسال المعلومات واستلامها في شكل إلكتروني كسلسلة من الأرقام 1 و 0".[1] وعليه مصطلح الرقمي (Digital) يشير إلى تخزين المعلومات ومعالجتها باستخدام الأرقام الثنائية (1 و 0)، وهو مفهوم يرتبط بتكنولوجيا الكمبيوتر والأنظمة الإلكترونية، حيث يتم إرسال واستقبال البيانات إلكترونيًا.

تعرف القيادة الرقمية بأنها: " قدرة القائد على استخدام التكنولوجيا الرقمية لممارسة التأثير والتوجيه على أعضاء الفريق حتى يمكن تحقيق أهداف الشركة".[2] أي أنها قدرة القائد على استخدام التكنولوجيا الرقمية للتأثير و التوجيه بغية تحقيق الأهداف المرجوة.

كما أشار روجرز (Rogers) أن القيادة الرقمية تشير إلى: "ممارسات وسلوكيات القائد من خلال استخدام الأدوات الرقمية كوسائل التواصل الاجتماعي والتواصل عبر تطبيقات الويب مثل برنامج zoom، المؤتمرات، الفيديوات، وغيرها من الأدوات الرقمية التي تتطور كل يوم، والقيادة الرقمية لا تعني أن يكون القائد خبيرا في استخدام أدوات وتطبيقات التكنولوجيا وصيانتها وحل مشكلاتها بل الكيفية التي يكون مطلعا على آخر تقنيات التكنولوجيا ليستطيع توجيه والتأثير على العاملين بما يعود بالمنفعة على تحقيق أهداف المؤسسة بفاعلية".[3] أي أنها ممارسات وسلوكيات القائد في استخدام الأدوات الرقمية للتواصل والتأثير على العاملين بفعالية.

كما تعرف أيضا على أنها: "عملية تأثير اجتماعي بواسطة تكنولوجيا المعلومات والاتصالات لإحداث تغيير في المواقف، والمشاعر، والتفكير، والسلوك، والأداء مع الأفراد، الجماعات، والالمؤسسات".[4] وهنا يقصد بها عملية تأثير اجتماعي عبر تكنولوجيا المعلومات لإحداث تغيير في السلوك والأداء داخل المؤسسات.

---

[1]–مها فهد الشمراني، "**أثر القيادة الرقمية على تحقيق التميز المؤسسي**"، المجلة العربية للنشر العلمي، العدد 58، المجلد 06، 2023، ص. 504

[2]-Fetty poerwita sary**, digital leadership and organizational communication toward millennial Employees in A telecommunication company,** corporate governance and organizational behavior review**,** vol: 06, N°:04, university of Telkom, 2022, P.160

[3]–أميرة هاتف حداوي، وآخرون، "**القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في المنظمات**"، مجلة العلوم الإنسانية والطبيعية، العدد 01، المجلد 05، 2024، ص. 686

[4]–جمال زمورة، ليلى بن عيسى، "**دور القيادة الرقمية في نجاح التحول الرقمي للخدمات العمومية في الجزائر**"، مجلة الاقتصاديات المالية البنكية وإدارة الأعمال، العدد 02، المجلد 11، 2022، ص. 302

وتعرف أيضا بأنها: القدرة على توجيه المؤسسات نحو التحول الرقمي من خلال تبني التكنولوجيا وتطوير استراتيجيات رقمية فعالة، بهدف تعزيز النمو والابتكار، مع مراعاة التحديات مثل نقص المهارات والقيود المالية واختلاف مستويات نضج الدول في استخدام التطبيقات الرقمية.[1]

ويمكن الإشارة إلى تعريف القائد الرقمي بأنه شخص مبتكر ومرن يمتلك مهارات وخبرات متنوعة تمكنه من قيادة التحول الرقمي بفعالية، حيث أنه يتميز بالانفتاح على الأفكار الجديدة، التعلم المستمر، والتكيف مع التغيرات، مع رؤية واضحة لتحقيق الأهداف المرجوة.[2]

من خلال ما سبق يمكن القول القيادة الرقمية هي نهج قيادي معاصر يعتمد على استخدام التكنولوجيا الرقمية للتأثير والتوجيه، حيث يوظف القائد الأدوات الرقمية الحديثة مثل وسائل التواصل الاجتماعي، وتطبيقات الاجتماعات الافتراضية، وأنظمة المعلومات، لتعزيز التواصل، وتحسين الأداء، ودعم التحول الرقمي في المؤسسات.

2-2 خصائص القيادة الرقمية:

تبرز خصائص القيادة الرقمية فيما يلي:[3]

- **قيادة رقمية:** تتميز بالمرونة وعدم التقيد بمكان أو زمان محدد، مما يتيح للقائد والعاملين إمكانية التواصل بحرية دون أي قيود؛
- **قيادة إنسانية:** لا تعتمد على التكنولوجيا فقط، بل تركز على بناء علاقات مفتوحة وتواصل فعّال بين جميع المستويات الإدارية؛
- **قيادة إبداعية:** تتطلب امتلاك القائد لمهارات ابتكارية تمكّنه من التفكير خارج الصندوق وإيجاد حلول مبتكرة لمواجهة التحديات المرتبطة بالتطور التكنولوجي؛
- **قيادة تقنية:** يتطلب هذا النوع من القيادة الإلمام بالأدوات الرقمية والقدرة على تحليل البيانات واتخاذ قرارات مستندة إلى المعلومات الفورية والدقيقة، مما يساعد في تسريع العمليات واتخاذ قرارات أكثر دقة وفعالية.

وعليه يمكن القول أن القيادة الرقمية تساهم في تحسين بيئة العمل، دعم التحول الرقمي، وتعزيز كفاءة المؤسسات في مجالات مختلفة.

---

[1]-Ahmed Bounfour ,**digital futures, digital transformation**, Springer international publishing, edition 01, switzerland, 2016, P:20

[2]-سيرين عزيز حسن حسني الجيوسي، "**القيادة الرقمية وعلاقتها بالاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية**"، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2024، ص. 17

[3]-أسماء عوض نهار الجريان، "**القيادة الرقمية وعلاقتها بالأداء الوظيفي في المدارس الحكومية** "، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2024، ص ص. 19- 20

2-3-أهمية ودوافع القيادة الرقمية:

تُعتبر القيادة الرقمية ذات أهمية باللغة في مختلف المؤسسات، حيث يهدف هذا النمط من القيادة إلى تحقيق مجموعة من الأهداف، والتي سيتم تناولها فيما يلي:

2-3-1-أهمية القيادة الرقمية:

تتمثل أهمية القيادة الرقمية في النقاط التالية:[1]

- تسهيل العمل الإداري من خلال دعم الموظفين وتبسيط الإجراءات التنظيمية؛
- تعزيز الشفافية والمشاركة في صنع القرار، مما يقلل من التعقيدات الإدارية؛
- تمكين الإدارات والقيادات من التخطيط بفعالية لتحقيق أهداف المؤسسة بكفاءة؛
- تحسين جودة الأداء وفق المعايير الفنية والتقنية الحديثة، بما يواكب التطورات التكنولوجية؛
- تبسيط إدارة المعلومات المختلفة وجعلها أكثر سهولة ووضوحًا؛
- تسريع تدفق المعلومات والمعاملات بين المستويات الإدارية المختلفة؛
- تعزيز سبل التواصل والتعاون مع المؤسسات الأخرى بشكل أكثر فاعلية؛
- الإسهام في بناء مجتمع رقمي متطور يتماشى مع متطلبات العصر.

من خلال ما سبق يمكن القول أن القيادة الرقمية تعزز الكفاءة والشفافية والتواصل، مما يرفع جودة الأداء ويدعم التحول الرقمي للمؤسسات والمجتمع.

2-3-2-دوافع القيادة الرقمية:

تتعدد الدوافع وراء تبني القيادة الرقمية في المؤسسات، حيث تشمل ما يلي: [2]

- **رفع كفاءة العمل المؤسسي:** يعتمد القائد الرقمي على التكنولوجيا الحديثة، مثل الأتمتة والإدارة الذكية للمعلومات، لتحسين الإنتاجية وتقليل الأخطاء والتكاليف التشغيلية؛
- **تقديم خدمات متطورة :** تهدف القيادة الرقمية إلى تحسين تجربة المواطنين والمستفيدين عبر توفير خدمات إلكترونية سهلة وسريعة، مما يوفر الوقت ويرفع جودة الخدمات؛
- **تعزيز الشفافية والمساءلة:** توفر القيادة الرقمية إمكانية الوصول إلى المعلومات، مما يسهم في متابعة القرارات والسياسات، إضافةً إلى تحسين آليات تقييم أداء العاملين؛

---

[1]-مها فهد الشمراني، **مرجع سابق**، ص ص. 504- 505

[2]-منى عبد عليّ المهنّديّ، "**دور القيادة العليا في تبني حالة التغيير وتضمين إستراتيجية التحول الرقميّ** دراسة حالة: الهيئة العامة لشؤون القاصرين بدولة قطر"، رسالة ماجستير ،جامعة قطر، 2023، ص. 23

- **تفعيل المشاركة المجتمعية:** تتيح القيادة الرقمية استخدام التكنولوجيا لتعزيز مشاركة المواطنين في صنع القرار عبر منصات التواصل الاجتماعي، الاستطلاعات الإلكترونية، والمنصات الرقمية التفاعلية.

يمكن القول من خلال ما سبق أن دوافع القيادة الرقمية تتمثل في تحسين كفاءة العمل، وتقديم خدمات متطورة، وتعزيز الشفافية، ودعم المشاركة المجتمعية، مما يساهم في تطوير المؤسسات وتحقيق أهداف بفعالية.

2-4-أهداف القيادة الرقمية:

توفر القيادة الرقمية العديد من المزايا التي تؤثر إيجابيًا على بيئة العمل، ومنها:[1]

- ✓ التحول من العمل اليدوي إلى الأساليب التقنية الحديثة؛
- ✓ زيادة الاعتماد على الموارد الرقمية في تنفيذ المهام وتحسين الأداء؛
- ✓ تحسين إدارة البيانات والمعلومات الرقمية من خلال جمعها وتنظيمها وحفظها واسترجاعها بسهولة؛
- ✓ تعزيز وتوسيع نطاق علاقات العمل داخل المؤسسة وخارجها؛
- ✓ تطوير بيئة العمل وتحسين الأدوات والمعدات المستخدمة في الأداء الوظيفي؛
- ✓ توسيع تأثير القادة المشرفين، مما يمنحهم قدرة أكبر على الإدارة والتوجيه.

يمكن القول أن حوصلة القيادة الرقمية تتمثل في تحسين كفاءة الأداء، وتعزيز استخدام التكنولوجيا في إنجاز المهام، وتطوير بيئة العمل، وتوسيع نطاق العلاقات المهنية، مما يسهم في تحقيق إدارة أكثر فعالية وتأثيرًا.

2-5-الفرق بين القيادة الرقمية، القيادة التكنولوجية، والقيادة الإلكترونية:

مع تطور التكنولوجيا، برزت مفاهيم قيادية حديثة تعتمد على التقنية لتطوير بيئة العمل، يوضح الجدول الموالي توضيح الفرق بين القيادة الرقمية، القيادة التكنولوجية، والقيادة الإلكترونية مع إبراز نقاط التوافق بينهم:[2]

[1]-عفاف بن فهم حسن العتيبي، **مرجع سابق**، ص. 3237

[2]-سيرين عزيز حسن حسني الجيوسي، **مرجع سابق**، ص ص. 13- 15

الجدول رقم (02): الاختلاف بين القيادة الرقمية، القيادة التكنولوجية، والقيادة الإلكترونية

العنصر	القيادة الرقمية	القيادة التكنولوجية	القيادة الإلكترونية	التوافقات المشتركة
التعريف	نهج قيادي يعتمد على التقنيات الرقمية لتعزيز الكفاءة، الشفافية، والتواصل داخل المؤسسات.	استثمار التكنولوجيا لتسهيل العمليات الإدارية وتحسين الأداء المؤسسي.	دمج الاتصال التقليدي والإلكتروني لتعزيز التأثير الاجتماعي عن بعد.	جميعها تعتمد على التكنولوجيا الحديثة في تطوير العمل المؤسسي.
المجالات المرتبطة	الابتكار في الإدارة، التحول الرقمي، القيادة المرنة والتطوير المستمر.	التعلم والتدريس، الإنتاجية والممارسة المهنية، القضايا القانونية والأخلاقية.	الاستباقية، الحلول الإبداعية التقنية، الدافعية التقنية.	تهدف جميعها إلى تطوير بيئة العمل وتسهيل الإدارة من خلال التكنولوجيا.
الكفايات المطلوبة	التفكير الابتكاري، التكيف مع التغيرات الرقمية، رؤية واضحة نحو التحول الرقمي.	التخطيط الإنتاجية، التقييم والتقويم، فهم القضايا القانونية والاجتماعية.	مهارات الاتصال الفّعال، القدرة على تشكيل الفرق وتعزيز التعاون، النزاهة والشفافية في الإدارة.	تتطلب جميعها امتلاك القائد لمهارات تقنية، إدارية، واتصالية فعّالة.
الهدف الرئيسي	تحقيق التحول الرقمي ورفع كفاءة المؤسسات باستخدام التكنولوجيا.	تحسين الأداء المؤسسي عبر استثمار التكنولوجيا بطرق مبتكرة.	تعزيز الاتصال الإلكتروني داخل المؤسسات وزيادة التفاعل الرقمي بين الأفراد.	تهدف جميعها إلى تحسين الأداء المؤسسي من خلال التكنولوجيا والابتكار.

المصدر: من إعداد الطالبين بالاعتماد على دراسة سيرين عزيز حسن حسني الجيوسي، "**القيادة الرقمية وعلاقتها بالاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية**"،رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2024.

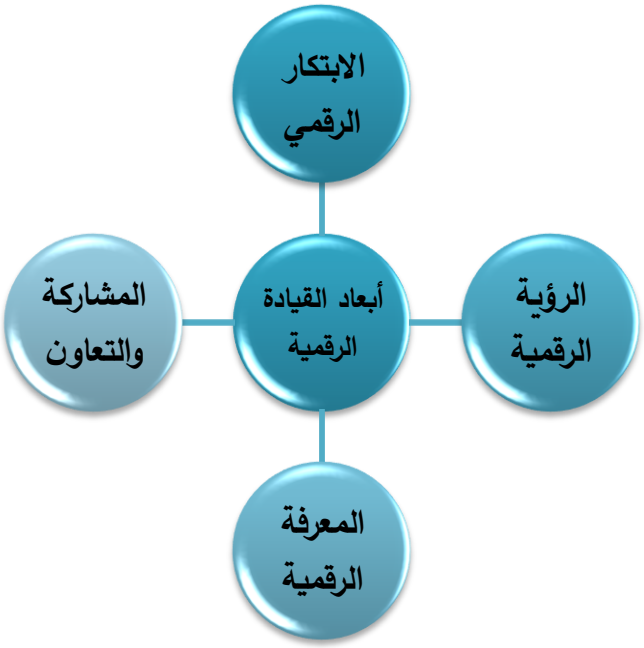
ثانيا: أبعاد ومراحل تطبيق القيادة الرقمية

ترتكز القيادة الرقمية على أبعاد متعددة وتمر بمراحل مترابطة تهدف إلى تحسين كفاءة القادة الرقميين. ويتطلب ذلك استيفاء شروط معينة لتطبيقها بفعالية في المؤسسات، وهو ما سيتم عرضه في هذا الفرع.

1-أبعاد القيادة الرقمية:

تكمن أبعاد القيادة الرقمية في الشكل الموالي:

الشكل رقم (01): أبعاد القيادة الرقمية



المصدر: من إعداد الطالبين بالاعتماد على دراسة أميرة هاتف حداوي، وآخرون، "**القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في الالمؤسسات**"، مجلة العلوم الإنسانية والطبيعية، العدد 01، المجلد 05، 2024، ص ص.687 – 688

يتضح من الشكل أعلاه أن القيادة الرقمية لها أربعة أبعاد والمتمثلة فيما يلي:

1-1-بعد الابتكار الرقمي:

من خلال هذا البعد يجب أن يتمتع القائد الفعّال بقدرة عالية على التكيف مع المتغيرات السريعة التي يشهدها العالم الرقمي، وذلك من خلال التجديد والإبداع وتبنّي الابتكار كركيزة أساسية في استراتيجياته القيادية. حيث يتطلب ذلك تطوير مهارات التفكير الإبداعي ولاستباقي، إلى جانب اعتماد مقومات الابتكار الرقمي، مثل المرونة في التعامل مع التغيرات التقنية، الحساسية تجاه الاتجاهات الرقمية الجديدة، والطاقة في تنفيذ التحولات الرقمية بفعالية.[1]

1-2-بعد الرؤية الرقمية:

الرؤية الرقمية تعني استشراف المستقبل والتخطيط له بوضوح، مما يمكّن القادة الرقميين من توجيه التحول الرقمي بفعالية عبر استراتيجيات مدروسة. حيث تعتمد هذه الرؤية على التفكير التصميمي والابتكار

[1]-Mubarak Mohsen Al- Faris, Merei Hassan Hamad Bani Khaled, " **Impact of Digital Leadership on Kuwaiti Hospitals' Employees' Performance"**, Journal of Economic, Administrative and Legal Sciences **,** Issue 19, volume 06, 2022, P . 135

لتوظيف الذكاء الاصطناعي والتقنيات الرقمية في تحسين العمليات وتعزيز التنافسية . لذا يتطلب التحول الرقمي إعادة هيكلة المؤسسات وتحديد الأهداف بوضوح، مع إشراك العملاء والموظفين والمستثمرين في صياغة رؤية متكاملة. وتعدّ الرؤية الرقمية الملهمة أساس نجاح التحول الرقمي، حيث تتجاوز مجرد تبني التكنولوجيا إلى تحسين تجربة العملاء وتطوير نماذج الأعمال، مما يستلزم مشاركة جميع مستويات المؤسسة لضمان تحقيقها بفعالية[1].

1-3-بعد المعرفة الرقمية:

المعرفة الرقمية أصبحت جزءًا أساسيًا في المؤسسات الحديثة، حيث تؤثر الابتكارات التكنولوجية بشكل مباشر على عمليات الإدارة، مما يمنح المؤسسات الرقمية مرونة أكبر في اتخاذ القرارات مقارنة بتلك التي لم تعتمد الرقمنة بعد. حيث تُعد إدارة المعرفة الرقمية محورًا رئيسيًا لبناء ميزة تنافسية، إذ تعتمد على تطوير الابتكارات التكنولوجية وربطها بالتحديات الإدارية. وتشمل القدرة على جمع البيانات إلكترونيًا من مصادر متعددة داخل المؤسسة، ومعالجتها وتحليلها لربطها بالأداء والأنشطة التي ينفذها الموظفون. كما تسهم في تحسين العمليات وتبسيطها، مما يعزز من كفاءة المؤسسة وقدرتها على الاستجابة للتغيرات بمرونة أكبر.[2]

1-4-بعد المشاركة والتعاون:

تشير هذه العملية إلى الاستفادة من المعرفة الجماعية من خلال تبادل الخبرات بطريقة غير هرمية، مما يتيح مشاركة أوسع للموظفين. يمكن تحقيق ذلك عبر ورش عمل حضورية أو افتراضية من خلال منصات إلكترونية، حيث تتاح لكل فرد فرصة لطرح أفكاره والمساهمة في عملية صنع القرار[3].

من خلال ما سبق يمكن القول أن القيادة الرقمية الفعالة تتطلب التكيف مع التغيرات السريعة عبر الابتكار الرقمي، واستشراف المستقبل من خلال الرؤية الرقمية، إلى جانب توظيف المعرفة الرقمية لتعزيز المرونة واتخاذ القرارات الذكية، كما يعد بعد المشاركة والتعاون عاملاً أساسياً في تبادل المعرفة ودعم عملية صنع القرار داخل المؤسسات.

2-مراحل تطبيق القيادة الرقمية:

---

[1]-أميرة هاتف حداوي وآخرون، **مرجع سابق**، ص ص. 687-688

[2]-**المرجع السابق**، ص. 688

[3]-**المرجع السابق**،

تمر القيادة الرقمية بعدة مراحل مترابطة هدفت إلى تعزيز الفاعلية الإدارية للقادة الرقميين وتحقيق التحول الرقمي داخل المؤسسات، وتشمل ما يلي:[1]

2-1-مرحلة التوثيق الإداري:

تتضمن تنظيم الهيكل الإداري والإجراءات الوظيفية، وتوثيق المهام، الصلاحيات، والخدمات المقدمة، مما يساهم في تحسين الأداء واتخاذ قرارات مستنيرة بناء على البيانات المتاحة؛

2-2-مرحلة التطوير القيادي:

تهدف إلى إعادة هندسة العمليات داخل المؤسسة وفق رؤية تقنية حديثة، مما يعزز الابتكار ويخلق بيئة قيادية أكثر كفاءة ومرونة؛

2-3-مرحلة التطوير التقني:

تركز على تحسين البنية التحتية الرقمية، وتعزيز استخدام البرمجيات الحديثة والأجهزة المتطورة، وتأهيل الموارد البشرية لضمان تنفيذ العمليات بفاعلية.

يتضح من خلال ما سبق، أن القيادة الرقمية ليست مجرد عملية عشوائية، بل هي نهج مخطط ومتتابع يهدف إلى تحسين الأداء القيادي والإداري، مما يعزز من قدرة المؤسسات على التكيف مع المتغيرات الرقمية.

ثالثا: متطلبات ومهارات القيادة الرقمية

تعتمد القيادة الرقمية على مجموعة من المتطلبات والمهارات التي تعزز كفاءة القادة في بيئة عمل متسارعة التطور. ويتطلب نجاحها تحقيق تكامل فعّال بين التكنولوجيا والقيادة، مما يساهم في تحسين الأداء المؤسسي ودعم التحول الرقمي، وهو ما سيتم التطرق إليه في هذا الفرع.

1-متطلبات تطبيق القيادة الرقمية:

يتطلب تطبيق القيادة الرقمية توفير مجموعة من المتطلبات الأساسية، ومنها ما يلي:[2]

- **البنية التحتية الرقمية:** تشمل شبكات الاتصالات، قواعد البيانات، الاتصال المستمر بالإنترنت، والأجهزة الرقمية اللازمة لضمان تواصل فعال؛
- **مزودو خدمات الإنترنت:** ضرورة توفير الإنترنت بأسعار مناسبة لضمان استمرارية الاتصال؛

[1]-حنان البدري كمال، حنان عبد الستار محمود، **"القيادة الرقمية كمدخل لتعزيز المرونة التنظيمية لدى القيادات الأكاديمية بجامعة أسوان"** ، المجلة التربوية كلية التربية، العدد 100، المجلد 01، 2022، ص. 170

[2]-أماني جبريل بصيلي، " **واقع تطبيق القيادة الرقمية بمدارس التعليم العام بمنطقة أبها الحضرية من وجهة نظر القيادات التربوية"** ، مجلة العلوم التربوية والنفسية، العدد 42، المجلد 6، 2022، ص ص. 28- 29

- **التدريب وبناء القدرات:** يشمل تأهيل الموظفين لاستخدام التقنيات الحديثة وإدارة الشبكات والبيانات بكفاءة؛
- **التمويل الكافي:** يضمن إجراء الصيانة الدورية وتمويل البرامج التدريبية لتعزيز جاهزية المؤسسة الرقمية؛
- **الإدارة المؤسسية:** توفير جهة مسؤولة عن تنفيذ القيادة الرقمية، وتهيئة البيئة المناسبة، والإشراف على عمليات التطبيق والتقييم؛
- **الأمن السيبراني:** حماية المعلومات الوطنية والشخصية، وضمان سرية البيانات ضد التهديدات الإلكترونية.

وعليه، يمكن القول أن هذه المتطلباتتُعد ركيزة أساسية لنجاح القيادة الرقمية، حيث تضمن تكامل التكنولوجيا مع العمليات المؤسسية، مما يسهم في تعزيز الكفاءة، وتحقيق التحول الرقمي الأمن والمستدام.

2-مهارات القيادة الرقمية:

تكمن أبرز المهارات المطلوبة للقادة الرقميين فيما يلي:[1]

- **إجادة استخدام التكنولوجيا الرقمية:** يشمل ذلك تكنولوجيا المعلومات والاتصالات، الأدوات الرقمية، البرمجيات، المنصات، والأنظمة السيبرانية؛
- **التواصل الفعّال والتفاعل المؤسسي:** يتطلب بناء علاقات قوية داخل المؤسسة، وتعزيز الاتصال بين المستويات الإدارية لضمان تحقيق الأهداف التنظيمية؛
- **التعلم المستمر وتطوير المعرفة:** يتطلب الواقع الاقتصادي والاجتماعي المتغير تحديثًا مستمرًا للمهارات، وتطوير الكفاءات عبر نهج متعدد التخصصات؛
- **المرونة والاستجابة السريعة:** يفرض التغيير المتسارع تبنّي حلول ديناميكية وغير تقليدية، والقدرة على التكيف مع المستجدات؛
- **تنفيذ حلول إبداعية ومبتكرة:** يشمل ذلك تطوير أساليب وتقنيات جديدة مع تحمل مستوى معتدل من المخاطر لتعزيز النمو والابتكار.

من خلال ما سبق يمكن القول أن هذه المهارات تمثل الأساس لنجاح القادة الرقميين في بيئة عمل تتسم بالتطور المستمر، حيث تمكن المؤسسات من مواكبة التحولات الرقمية بفعالية.

[1]-عفاف بن فهم حسن العتيبي، **مرجع سابق**، ص. 3236

رابعا: تحديات التحول إلى القيادة الرقمية:

تواجه القيادة الرقمية تحديات تتعلق بالبنية التحتية، والتكيف مع التغيرات، وتعزيز ثقافة الابتكار، حيث يتطلب نجاحها التغلب على هذه العقبات لضمان تحول رقمي فعّال، وهو ما سيتم استعراضه في هذا الفرع.

1-تحديات التحول نحو القيادة الرقمية:

تواجه عملية التحول إلى نمط القيادة الرقمي العديد من التحديات، لعل أبرزها ما يلي:

1-1-نقص القيادات المؤهلة للتحول الرقمي:

يتطلب التحول الرقمي قيادة تمتلك رؤية واضحة، ومهارات تقنية متقدمة، وقدرة على إدارة التغيير بفعالية. في العديد من المؤسسات، يواجه القادة صعوبة في التعامل مع التقنيات الحديثة أو وضع استراتيجيات فعالة للتحول الرقمي، مما يعيق تنفيذ المشاريع الرقمية بكفاءة؛[1]

1-2-مقاومة الموظفين للتغيير:

يعد التغيير الرقمي تحديًا للعديد من الموظفين الذين قد يشعرون بعدم الأمان الوظيفي أو يجدون صعوبة في التكيف مع الأدوات والتقنيات الجديدة. غياب ثقافة الابتكار والتدريب المناسب يؤدي إلى مقاومة التحول الرقمي، مما يستلزم توعية الموظفين بأهمية التغيير وتقديم برامج تدريبية لدعمهم في هذه المرحلة؛[2]

1-3غياب إستراتيجية شاملة للتحول الرقمي:

تعتمد القيادة الرقمية على رؤية وإستراتيجية واضحة تحدد الأهداف والخطوات التنفيذية بوضوح. عدم وجود خطة إستراتيجية متكاملة يؤدي إلى التخبط في تنفيذ مشاريع التحول الرقمي، مما يقلل من فاعليتها وقدرتها على تحقيق النتائج المرجوة؛[3]

1-4-ضعف الدعم المالي وعدم تعاون الشركاء:

يتطلب التحول الرقمي استثمارات كبيرة في البنية التحتية، والتقنيات الحديثة، وتدريب الموظفين، حيث غياب الميزانية الكافية أو عدم تعاون الشركاء والموردين في توفير الحلول الرقمية المناسبة قد يؤخر تنفيذ التحول الرقمي، مما يعطل تطور المؤسسة ويحدّ من تنافسيتها.[4]

---

[1]-**المرجع السابق**، ص. 3237

[2]-**المرجع السابق**.

[3]-أماني جبريل بصيلي، **مرجع سابق**، ص. 29

[4]-**المرجع السابق**.

يمكن القول أن التحول إلى القيادة الرقمية يتطلب تجاوز هذه التحديات من خلال تطوير الكفاءات القيادية، وتحفيز الموظفين على التكيف، ووضع استراتيجيات رقمية واضحة، إلى جانب توفير الموارد المالية والدعم اللازم لضمان نجاح العملية الرقمية.

خلاصة القول تعد ا لقيادة الرقمية نمط حديث لا يرتبط بمكان أو زمان محدد، حيث تعتمد على استخدام الأجهزة الرقمية والتقنيات الحديثة لتعزيز كفاءة الإدارة واتخاذ القرارات. وقد دفعت مجموعة من العوامل المؤسسات إلى تبني هذا التحول لما له من أهمية كبيرة في تحسين الأداء وتحقيق أهداف إستراتيجية، حيث تقوم القيادة الرقمية على مجموعة من المفاهيم والأبعاد المتعددة، وتمر بمراحل متكاملة، وتتطلب توفر متطلبات معينة لضمان نجاحها والتغلب على التحديات التي تواجهها، ومن بين الجوانب التي تتأثر بالقيادة الرقمية الأمن السيبراني، حيث يساهم التحول الرقمي في رفع مستوى الوعي الأمني، وتبني ممارسات وقائية، وتعزيز القدرة على التصدي للمخاطر السيبرانية داخل المؤسسات، ومن خلال المطلب الموالي سيتم التطرق إلى عموميات حول الأمن السيبراني.

المطلب الثاني: الأمن السيبراني

أدى التقدم التكنولوجي والتطور الهائل في مجالات الإعلام والمعلومات والاتصالات إلى ظهور مفاهيم جديدة، من أبرزها الأمن السيبراني. وقد ازدادت أهمية هذا المفهوم بشكل ملحوظ، حيث أصبح يُنظر إليه كسلاح استراتيجي تسعى الدول والحكومات إلى تطويره واعتماده لحماية نفسها من الهجمات الإلكترونية والاختراقات. ويأتي هذا الاهتمام نتيجة الإدراك المتزايد لحجم المخاطر والتحديات المرتبطة بالأمن السيبراني، والتي تمتد آثارها إلى الدول ومؤسساتها وأفرادها. لذا، أصبح من الضروري تبني إستراتيجية واضحة لتعزيز الأمن السيبراني بجميع أبعاده.

أولا: مفاهيم أساسية متعلقة بالأمن السيبراني

يعد الأمن السيبراني من المفاهيم التي نالت اهتمام الباحثين والمتخصصين، لدوره الأساسي في حماية الأنظمة والمعلومات من التهديدات الرقمية، وتعزيز أمن المؤسسات والأفراد . حيث سيتم التطرق من خلال هذا الفرع إلى نشأة وتعريف الأمن السيبراني، أهميته، وأهدافه، وكذا الإشارة إلى مفاهيم مرتبطة به.

1-تعريف ونشأة الأمن السيبراني:

1-1-تعريف الأمن السيبراني:

قبل تعريف الأمن السيبراني، سيتم أولا توضيح معنى الأمن، والسبرانية من الناحيتين اللغوية والاصطلاحية، كما يلي:

- **الأمن لغةً:**تدل كلمة "أمن" في اللغة العربية على الطمأنينة وزوال الخوف، وتستخدم بضد الخوف، والخيانة، والكفر، والتكذيب، فإذا انتفت هذه المعاني تحقق الأمن في الدنيا والآخرة،[1] كما قال تعالى: "**الذين آمنوا ولم يلبسوا إيمانهم بظلم أولئك لهم الأمن وهم مهتدون**" **(الأنعام: 82).**
- **الأمن اصطلاحاً:** يمكن تعريفه بأنه:"طمأنينة النفس التي تزيل عن الإنسان الخوف على نفسه ودينه وعرضه وعقله، وماله في أحوال معاشه ومعاده".[2] يعبر الأمن اصطلاحاً عن الشعور بالطمأنينة وزوال الخوف في مختلف جوانب حياة الإنسان.
- **السيبرانية لغةً:** تعرف على أنها: "مأخوذة من كلمة (سيبر Cyber) وتعني صفة ألي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني (فضاء الإنترنت) ، وهي كلمة مشتقة من الكلمة اليونانية (Kybernetes) التي وردت بداية في مؤلفات الخيال العلمي، وكان

[1]-مها بنت غزاي عبد الله العتيبي، **"تطبيقات قاعدة "الضرر يزال" في مجال الأمن السيبراني"**، مجلة الإبراهيمي للآداب والعلوم الإنسانية، جامعة برج بوعريريج، العدد 02، المجلد 05، 2023، ص. 139

[2]-**المرجع السابق**، ص. 140

يقصد بها قيادة ربان السفينة". [1] وعليه يشير مصطلح (سيبر Cyber) إلى كل ما يتعلق بتكنولوجيا المعلومات والفضاء الإلكتروني، وهو مشتق من كلمة يونانية تعني القيادة والتحكم.

- **السيبرانية اصطلاحاً:** "تطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية وشبكة الانترنت، والفضاء السيبراني (Cyberspace) يعني الفضاء الإلكتروني، ويعني كل ما يتعلق بشبكات الحاسوب والإنترنت، والتطبيقات المختلفة (كالواتس آب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم".[2] يشير مصطلح "سيبراني" إلى كل ما يتعلق بالشبكات الإلكترونية وتطبيقاتها وخدماتها.
- **الأمن السيبراني:**

يعرف حسب المعهد الوطني للمعايير والتقنية الأمريكية على أنه:" الحماية من الأضرار واستعادة أنظمة الحاسب وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية والاتصالات الإلكترونية، بما في ذلك المعلومات الواردة فيها؛ لضمان توافرها وسلامتها والمصادقة والسرية وعدم الانتهاك". [3] وعليه يعرف الأمن السيبراني على أنه حماية أنظمة الحاسب والاتصالات لضمان سلامتها وسريتها وتوافرها ومنع أي انتهاك لها.

وقد عرفه أيضا المشرع الجزائري في نص المادة 2 من المرسوم التنفيذي رقم 05.20 المؤرخ في 25 يوليو 2020 المتعلق بالأمن السيبراني على أنه: " مجموعة من التدابير والإجراءات ومفاهيم الأمن وطرق إدارة المخاطر والأعمال والتكوينات وأفضل الممارسات والتكنولوجيات التي تسمح لنظام معلومات أن يقام أحداثا مرتبطة بالفضاء السيبراني، من شأنها أن تمس بتوافر وسلامة وسرية المعطيات المخزنة أو المعالجة أو المرسلة، من خدمات ذات الصلة التي يقدمها هذا النظام أو تسمح بالولوج إليه". [4] يمكن القول حسب هذه المادة أعاله أن المشرع الجزائري يعرف الأمن السيبراني بأنه مجموعة تدابير وإجراءات لحماية نظم المعلومات من التهديدات التي تمس بتوافرها وسلامتها وسريتها.

كما يعرف على أنه:" حماية الشبكات وأنظمة المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من عتاد وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو دخول أو استخدام

---

[1]–إدريس عطية، "**مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري**"، العدد 01، المجلد 01، 2019، ص. 103

[2]–فايزة أحمد الحسيني مجاهد،" **الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية**"، مجلة بحث وتربية المعهد الوطني للبحث في التربية، العدد 02، المجلد 13، 2023، ص. 59

[3]–مها بنت غزاي عبد الله العتيبي، **مرجع سابق**، ص. 141

[4]–المرسوم التنفيذي رقم 05/20، **الجريدة الرسمية للجمهورية الجزائرية**، العدد 6904، الصادرة بتاريخ 30 يوليو 2020م، ص. 4160

أو استخدام غير مشروع ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي وما إلى ذلك..."[1]. يقصد بالأمن السيبراني حماية الأنظمة والشبكات والبيانات من الاختراق أو الاستخدام غير المشروع، ويشمل أمن المعلومات والأمن الإلكتروني والرقمي.

مما سبق ذكره يمكن القول أن الأمن السيبراني هو مجموعة من التدابير والإجراءات التي تضمن حماية الأنظمة والشبكات والبيانات من التهديدات والاختراق والدخول الغير مصرح به، مع الحفاظ على سريتها وسلامتها وتوافرها.

1-2-نشأة الأمن السيبراني:

تبرز نشأة الأمن السيبراني من خلال الشكل الموالي:

الشكل رقم (02): نشأة الأمن السيبراني

المصدر: من من إعداد الطالبين بالاعتماد على دراسة

Rihab Yousfi, Mohamed El Bachir El Ibrahimi**, " Cybersecurity Challenges and International Cooperation",** Journal of law and humanities Sciences,Issue03, volume 17, 2024, P . 34

يمكن القول من خلال الشكل أعلاه، أن جذور الاهتمام بالأمن السيبراني تعود إلى عام 1962، عندما أعلنت السلطات الأمريكية، عبر وكالة مشاريع البحوث المتقدمة (ARPA)، عن نيتها إنشاء نظام اتصالات قادر على الصمود أمام هجوم نووي من الاتحاد السوفيتي. وفي عام 1969، بدأت جامعة كاليفورنيا –لوس أنجلوس في تطوير شبكة(ARPANET)، التي أصبحت فيما بعد الأساس لشبكة الإنترنت الحديثة .بحلول عام 1971، قاد مهندس الكمبيوتر الفرنسي لويس بوزان مشروع "سيكلاديز"، الذي ربط 25 جهاز كمبيوتر بين فرنسا وإيطاليا والمملكة المتحدة، مما مكّن الباحثين من التعاون عن بُعد وتطوير شبكة عالمية تعتمد على تبديل الحزم. وفي عام 1973، تعاونت جامعة كاليفورنيا – لوس أنجلوس مع روبرت كان من وكالة(ARPA)،لإنشاء بروتوكول اتصالات متطور .لكن في عام 1979، توقف مشروع سيكلاديز بسبب

[1] –أيمن احمد الحديدي، **الأمن السيبراني في ظل الانفجار المعرفي**، ط1،دار اليازوري للنشر والتوزيع، عمان، الأردن، 2023، ص. 72– 73

نقص التمويل من الحكومة الفرنسية، التي لم تعطه الأولوية، بينما واصلت الولايات المتحدة تطوير هذا المجال.[1]

مما سبق ذكره أعلاه يمكن القول أنه بدأ الاهتمام بالأمن السيبراني منذ 1962 بتطوير أنظمة اتصالات آمنة، مما أدى إلى ظهور شبكة (ARPANET) التي شكلت أساس الإنترنت الحديثة.

1-3-أهمية الأمن السيبراني:

يمكن إبراز أهمية الأمن السيبراني من خلال النقاط التالية:[2]

- ✓ حماية المصالح الوطنية من خلال تأمين أمن الدولة ومواطنيها، مع التركيز على حماية البنية التحتية الحيوية من التهديدات السيبرانية؛
- ✓ ضمان استمرارية عمل نظم المعلومات من خلال توفير آليات فعالة للحماية والصيانة، مما يضمن توفر البيانات والخدمات الرقمية دون انقطاع؛
- ✓ تعزيز سرية وخصوصية البيانات عبر تطبيق معايير الأمان لحماية معلومات الأفراد والشركات من التسريب أو الاستخدام غير المصرح به؛
- ✓ تأمين الأنظمة التشغيلية ضد أي محاولات اختراق أو وصول غير مشروع، مما يمنع الاستغلال غير القانوني للمعلومات أو تعطيل الأنظمة؛
- ✓ إنشاء بيئة إلكترونية آمنة وموثوقة تتيح للأفراد والمؤسسات التعامل عبر الشبكات العالمية بثقة، مع تقليل مخاطر التهديدات السيبرانية.

من خلال ما سبق أن الأمن السيبراني يسعى إلى حماية المصالح الوطنية، وضمان توافر واستمرارية نظم المعلومات، وتعزيز خصوصية البيانات، وتأمين الأنظمة من الاختراق، وتهيئة بيئة رقمية آمنة.

1-4-أهداف الأمن السيبراني:

تتمثل أهداف الأمن السيبراني في النقاط التالية:[3]

- ✓ حماية أنظمة التقنيات التشغيلية بمختلف مكوناتها، من أجهزة وبرمجيات وخدمات وبيانات، مع سد الثغرات الأمنية والقضاء على نقاط الضعف في الحواسيب والأجهزة المحمولة؛

[1]-Rihab Yousfi, Mohamed El Bachir El Ibrahimi, **" Cybersecurity Challenges and International Cooperation",** Journal of law and humanities Sciences,Issue03, volume 17, 2024, P . 34

[2]-مها بنت غزاي عبد الله العتيبي، **مرجع سابق**، ص ص. 142- 143

[3]-عبد الله اللقاني، **دور الأمن السيبراني في تعزيز أمن المعلومات المالية والإلكترونية**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2023، ص ص. 152- 153

- ✓ التصدي للهجمات الإلكترونية التي تستهدف المؤسسات الحكومية والقطاعين العام والخاص، وتعزيز قدرة البنى التحتية الحساسة على الصمود أمامها؛
- ✓ مكافحة البرمجيات الخبيثة والتهديدات السيبرانية التي تهدف إلى إلحاق الضرر بالمستخدمين أو سرقة بياناتهم، واتخاذ التدابير اللازمة لحماية الأفراد والمستهلكين أثناء استخدام الإنترنت؛
- ✓ تعزيز الوعي والتدريب من خلال تزويد الأفراد بآليات وإجراءات فعالة لحماية أجهزتهم ومعلوماتهم الشخصية من الاختراق أو التلف.

يمكن القول أن الأمن السيبراني يهدف إلى حماية الأنظمة والبيانات، والتصدي للهجمات الإلكترونية، وتوفير بيئة رقمية آمنة، مع تعزيز الوعي والتدابير الوقائية لمواجهة التهديدات السيبرانية.

1-5 -مصطلحات مرتبطة بالأمن السيبراني:

1-5-1-الفضاء السيبراني:

وفقًا لوزارة الدفاع الأمريكية، يُعرف بأنه: "مجال عالمي داخل بيئة المعلومات يتكون من شبكات معلومات البنية التحتية لتكنولوجيا المعلومات المترابطة، بما في ذلك الإنترنت، وشبكات الاتصالات، وأنظمة الكمبيوتر، والمعالجات والضوابط المدمجة". [1]

بينما ترى القمة الروسية-الأمريكية للأمن السيبراني أن الفضاء السيبراني هو: "مجال رقمي يتم فيه تخزين المعلومات ونقلها ومعالجتها وحذفها". [2]

من خلال ما سبق يمكن القول أن الفضاء السيبراني هو مجال رقمي عالمي يتكون من شبكات وأنظمة معلومات مترابطة، تستخدم لتخزين البيانات ومعالجتها وتبادلها، ويشكّل بيئة افتراضية للتفاعل والتواصل والعمل، تجمع بين التكنولوجيا والمجتمع.

1-5-2-الجريمة السيبرانية:

تعرف الجريمة السيبرانية على أنها: " الأفعال غير القانونية التي تكون فيها الأجهزة الرقمية أو أنظمة المعلومات إما أداة للجريمة أو هدفاً لها، أو مزيجاً من الاثنين". [3] وعليه يمكن القول أنالجريمة السيبرانية هي كل فعل غير قانوني يُرتكب باستخدام التكنولوجيا الرقمية أو عبر الإنترنت، ويستهدف أنظمة المعلومات أو البيانات الرقمية أو مستخدميها، بهدف التلاعب أو السرقة أو التخريب أو التشهير أو الابتزاز، سواء بدافع مادي أو سياسي أو شخصي.

---

[1]-Uche Mbanaso , Emmanuel s.Dandaura , **"The Cyberspace : Redefining A New World "**,IOSR Journal of Computer Engineering (IOSR- JCE), Issue03, volume 17, 2015, P . 18

[2]-**Op. Cit.**

[3]-Regner Sabillon, Jeimy J. Cano M . , Jordi Serra-Ruiz, Victor Cavaller, **" Cybercrime and Cybercriminals : A Comprehensive Study,** International Journal of Computer Networks and Communications Security, Issue 06, volume 04 , 2016, P . 166

وتتنوع الجرائم السيبرانية بحسب طبيعتها والهدف منها، ومن أبرز هذه الأنواع نذكر:[1]

- **الاعتداء على البيانات الرقمية:** مثل اختراق أو تعديل أو حذف البيانات دون إذن؛
- **الهجوم على الأنظمة المعلوماتية:** كتعطيل أو إتلاف الشبكات أو الخوادم أو البرامج؛
- **سوء استخدام الأجهزة والبرمجيات** : ويشمل ذلك استخدام البرمجيات لأغراض ضارة كزرع الفيروسات أو برمجيات التجسس؛
- **الجرائم المالية الرقمية:** مثل سرقة الأموال من الحسابات المصرفية أو الاحتيال الإلكتروني؛
- **الانتهاك الإلكتروني للملكية الفكرية:** كنسخ أو توزيع المحتوى الرقمي المحمي دون ترخيص؛
- **الاحتيال باستخدام البطاقات المصرفية والنقود الإلكترونية** : ويشمل سرقة بيانات البطاقات أو تزويرها؛
- **انتهاك الخصوصية:** كجمع أو تسريب المعلومات الشخصية دون موافقة أصحابها؛
- **الجرائم ذات الطابع العنصري أو الإنساني:** مثل نشر الكراهية أو التحريض على العنف عبر الوسائط الرقمية؛
- **الأنشطة غير القانونية عبر الإنترنت:** مثل المقامرة غير المشروعة أو ترويج المخدرات إلكترونيًا؛
- **جرائم تشفير المعلومات:** كاستخدام تقنيات التشفير لإخفاء أنشطة غير قانونية أو لحجب البيانات عن الجهات المخولة.

يمكن القول أن الجرائم السيبرانية تمثل تهديدًا متزايدًا للمجتمعات الحديثة، حيث تشمل مجموعة واسعة من الأنشطة غير القانونية التي تستهدف البيانات والأموال والخصوصية.

1-5-3-الهجمات السيبرانية:

تعرف على أنها:" هي أنشطة شريرة تُنفذ لسرقة المعلومات أو كشفها أو إتلافها أو تغييرها أو إتلافها أو تدميرها من خلال الوصول غير المصرح به إلى نظام الكمبيوتر، أو هي هجوم يشنه مهاجمون يستخدمون جهاز كمبيوتر واحدًا أو أكثر لمهاجمة أجهزة كمبيوتر وشبكات أخرى". [2] من خلال هذا التعريف يمكن القول أنالهجمات السيبرانية تُعد من أخطر التهديدات الرقمية، إذ تستهدف سرية وسلامة المعلومات والأنظمة عبر وسائل غير مشروعة. وتكشف عن الحاجة الملحة لتعزيز الأمن السيبراني لحماية الأفراد والمؤسسات من الاختراقات والتخريب.

---

[1]-فايزة أحمد الحسيني مجاهد، **مرجع سابق**، ص ص. 61-62

[2]-Mihret Sheleme, Rajesh Sharma Rajendran, **"Cyber-attack and Measuring its Risk,** IRO Journal on Sustainable Wireless Systems, Issue 04, volume 03, 2021, P. 219

وهناك أنواع مختلفة من الهجمات السيبرانية، التي تكمن فيمايلي: [1]

- **هجمات التصيد الاحتيالي:** تستهدف أفرادًا أو مؤسسات كالبنوك عبر رسائل إلكترونية مزيفة تطلب معلومات حساسة مثل البيانات البنكية، بهدف سرقة بيانات أو تثبيت برامج خبيثة؛
- **هجمات برامج الفدية:** تُستخدم لتشفير بيانات المستخدمين عبر برامج خبيثة وتطلب فدية لفك التشفير، وتهدف إلى تعطيل أنظمة البنك وابتزاز الأموال؛
- **هجمات الحرمان من الخدمة (DDoS):** تُغرق خوادم البنوك الإلكترونية بكمية هائلة من البيانات بهدف تعطيل الخدمات البنكية والإضرار بسمعة المؤسسة؛
- **هجمات الهندسة الاجتماعية:** تعتمد على التلاعب النفسي لخداع موظفي البنك للكشف عن معلومات سرية أو تنفيذ عمليات غير مصرح بها؛
- **هجمات البرامج الضارة:** تُثبّت على الأجهزة بهدف سرقة البيانات أو التحكم في النظام، وتؤثر على الأداء وتعطل الأنظمة البنكية؛
- **القنابل البرمجية:** شيفرات خبيثة تُزرع داخل برامج أخرى وتُفعّل عند وقت أو حدث معين لتدمير أو تعديل البيانات والأنظمة البنكية.

وعلى ضوء ما سبق يمكن القول أن الهجمات السيبرانية تهدد البيانات والخدمات البنكية، ووعي الأفراد أساسي للحد من مخاطرها.

1-5-4-التهديدات السيبرانية:

التهديدات السيبرانية تمثّل محاولات أو أنشطة ضارة تهدف إلى اختراق أو تعطيل أو إتلاف أنظمة المعلومات، أو الوصول غير المصرح به إلى البيانات الحساسة، مما يستدعي اتخاذ تدابير أمنية لحماية الأفراد والمؤسسات من الأضرار الرقمية المحتملة. [2]

1-5-5-الأمن المعلوماتي:

حسب اللجنة الوطنية لأنظمة أمن الاتصالات والمعلومات (NSTISSC) يعرف أمن المعلومات على أنه: "يعني حماية البيانات وأنظمة المعلومات من الوصول أو الاستخدام أو الكشف أو التعديل أو الإتلاف غير المصرح به، وذلك للحفاظ على قيمتها بالنسبة للمؤسسة. يدافع أمن المعلومات عن البيانات (والمرافق والأنظمة التي تخزنها وتستخدمها وتنقلها) من مجموعة واسعة من التهديدات".[3]

---

[1]-Omar Alobthany,**" Cybersecurity Career", https://cyberhub.sa/posts/4223**, Counsulter le, 07/03/2025, 20 :30

[2]-Vaman Ashqi Saeed, Renas Rajab Asaad, **"Cyber Security Threats, Vulnerability, Challenges With Proposed Solution"**, Applied Computing Journal, Issue 04, volume 02, 2022, P. 230

[3]-Yogesh P . Surwade, Hitendra J Patil, **" Information Security"**, SSRN (Social Science Research Network), 2024, P. 459

وتعد العلاقة بين أمن المعلومات والأمن السيبراني بمثابة علاقة جزئية، حيث يتعامل أمن المعلومات مع حماية البيانات من الوصول غير المصرح به سواء كانت إلكترونية أو ورقية. أما الأمن السيبراني فيشمل تأمين المعلومات في الفضاء السيبراني وضمان أمان الخدمات مثل الطاقة والاتصالات. لا يمكن القول إن أحدهما يشمل الآخر، إذ يختلفان في نطاق الاهتمام.[1]

يمكن القول من خلال ما تم التطرق إليه من مصطلحات مرتبطة بالأمن السيبراني أن لفضاء السيبراني يشمل الشبكات والأنظمة الرقمية، بينما الجريمة والهجمات السيبرانية تهدد البيانات والخدمات، أما أمن المعلومات والأمن السيبراني يتكاملان لحماية البيانات، لكن كل منهما يركز على مجالات مختلفة.

ثانيا: عناصر وأبعاد الأمن السيبراني

يشمل الأمن السيبراني عناصر وأبعاد تقنية وتنظيمية تهدف لحماية الأصول الرقمية، ويتطلب تطبيقا فعالاً ووعياً مستمراً، وهذا ما سيتم عرضه في هذا الفرع.

1-عناصر الأمن السيبراني:

لكي يتحقق الهدف من الأمن السيبراني، يجب توفر مجموعة من العناصر المتكاملة التي تعمل معاً لضمان تحقيق هذا الهدف، من أبرز هذه العناصر ما يلي:[2]

- **أمن التطبيقات (Application Security)**:يشمل حماية البرمجيات من الثغرات الأمنية خلال دورة حياة التطوير، بما في ذلك التصميم، البرمجة، النشر، والتحديثات؛
- **أمن المعلومات (Information Security)**: يركز على الحفاظ على سرية، تكامل، وتوافر المعلومات من خلال استراتيجيات وأدوات وسياسات؛
- **أمن البريد الإلكتروني (Email Security)**:يتضمن تقنيات لمنع هجمات التصيّد وحماية البيانات الحساسة من التسرب عبر البريد الإلكتروني؛
- **أمن الأجهزة المحمولة (Mobile Device Security)**: يتعلق بالتحكم في الأجهزة التي يمكنها الوصول إلى الشبكة وضمان سرية حركة البيانات؛
- **أمن الويب (Web Security)**: يهدف إلى حماية المواقع الإلكترونية من التهديدات، ومنع الوصول إلى مواقع خبيثة، وتأمين بوابات الويب؛

[1]-سليمان قطاف، بوقرين عبد الحليم، "**الأمن السيبراني والمضامين المفاهيمية المرتبطة به**" ، مجلة طبنة للدراسات العلمية الأكاديمية، العدد 02، المجلد 05، 2022، ص. 50

[2]-Parashu Ram Pal,"**A Recent Study over Cyber Security and its Elements** ", International Journal of Advanced Reseearch in Computer Science, Issue 03, volume 08, 2022, P. 791

- **أمن الشبكات اللاسلكية (Wireless Security):** حماية الشبكات اللاسلكية من الاختراقات، وهي أكثر عرضة للخطر مقارنة بالشبكات السلكية.

من خلال ما سبق يمكن القول أن عناصر الأمن السيبراني تتكامل لحماية الأنظمة من تهديدات متنوعة عبر تقنيات متقدمة في مجالات مختلفة، هذه العناصر تركز على الحفاظ على سرية البيانات واستمرارية الأمان في مواجهة التهديدات المتزايدة.

2-أبعاد الأمن السيبراني:

تتمثل الأبعاد الأساسية للأمن السيبراني في خمسة أبعاد وهي تكمل بعضها البعض، حيث تبرز فيمايلي:

2-1-البعد العسكري: تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية عبر الشبكات الإلكترونية لتبادل المعلومات بسرعة وتنفيذ الأوامر عن بعد. ولكن هذه الميزة قد تتحول إلى نقطة ضعف إذا لم تكن الشبكة محمية بشكل جيد ضد الهجمات الإلكترونية، مما قد يؤدي إلى اختراقات تجسس وتعطيل أنظمة الاتصال والدفاع الجوي، وفقدان السيطرة على الوحدات العسكرية.[1]

2-2-البعد الاقتصادي: يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد من خلال تعزيز استخدام تقنيات المعلومات والاتصالات التي تدعم التنمية الاقتصادية وتوفر فرصًا للشركات لتحسين إنتاجها. كما يسهم في تطور المال الإلكتروني والخدمات الإلكترونية، مما يعزز الاستثمار في القطاع المالي. إضافة إلى ذلك، يتطلب حماية البيانات من الجرائم الاقتصادية العابرة للحدود، مما يساهم في خلق بيئة آمنة للنمو الاقتصادي المستدام.[2]

2-3-البعد الاجتماعي: تساعد شبكات التواصل الاجتماعي في تمكين الأفراد من التعبير عن آرائهم السياسية وطموحاتهم الاجتماعية بطرق متنوعة، كما تتيح لجميع فئات المجتمع المشاركة في تطويره من خلال تبادل الأفكار والمعلومات. هذه المشاركة تعزز من استقرار الفضاء الإلكتروني والمجتمع المرتبط به، كما أن انفتاح المجتمع على الآخرين يسهم في تبادل الخبرات والأفكار وفتح آفاق للتعاون والتكامل.[3]

2-4-البعد السياسي: يتمثل البعد السياسي للأمن السيبراني في حق الدولة في حماية نظامها السياسي وكيانها ومصالحها الاقتصادية، بما يتضمن سعيها لتحقيق رفاهية شعبها. في الوقت الحالي، أصبح للأفراد دور كبير في السياسة بفضل الوصول إلى كم هائل من المعلومات التي تمكنهم من الاطلاع على خلفيات

---

[1]-إدريس عطية، **مرجع سابق**، ص. 105

[2]- **المرجع السابق.**

[3]-منى الأشقر جبور، **السيبرانية هاجس العصر**، مجلة المكتبات والمعلومات والتوثيق في العالم العربي، جامعة الدول العربية، قطاع الأعمال والاتصال-إدارة المعلومات والتوثيق والترجمة، بيروت -لبنان-، 2016، ص. 29

القرارات السياسية. في المقابل، يستغل العاملون في المجال السياسي هذه التقنيات للوصول إلى أكبر عدد ممكن من الناس للترويج لسياساتهم، ما يترك تأثيرًا كبيرًا على الرأي العام، بغض النظر عن صحة السياسات أو المبادئ التي يتم الترويج لها.[1]

2-5-البعد القانوني: البعد القانوني للأمن السيبراني يتطلب اهتمامًا خاصًا بالنزاعات الناتجة عن الأنشطة الفردية، المؤسساتية، والحكومية في الفضاء الإلكتروني. يتضمن ذلك حقوقًا جديدة مثل حق الوصول إلى المعلومات على الإنترنت، وإنشاء المدونات والتجمعات الإلكترونية، وحماية ملكية البرمجيات. كما ظهرت متطلبات قانونية اقتصادية مثل الاحتفاظ ببيانات الاتصالات والإبلاغ عن المخالفات المتعلقة بالمحتوى.[2]

من خلال ما سبق يمكن القول أن هذه الأبعاد الخمسة تشكل أساسًا أساسيًا للأمن السيبراني، وتساهم في تقليل المخاطر السيبرانية من خلال اتخاذ إجراءات وقائية مستمرة.

ثالثا: آليات الأمن السيبراني:

تتضمن آليات الأمن السيبراني إجراءات وتقنيات لحماية الأنظمة والشبكات من التهديدات السيبرانية، وضمان سرية البيانات وسلامتها، وهو ما سيتم التطرق إليه في هذا الفرع.

1-آليات الأمن السيبراني:

تكمن آليات الأمن السيبراني في الشكل التالي:

[1]-**المرجع السابق**، ص ص. 29-30

[2]-سمير بارة، "**الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات**"، المجلة الجزائرية للأمن الإنساني، العدد 04، بدون مجلد، 2017، ص. 263

الشكل رقم (03): آليات الأمن السيبراني

المصدر: من : من من إعداد الطالبين بالاعتماد على دراسة سمير بارة، "**الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات**"، المجلة الجزائرية للأمن الإنساني، العدد 04، بدون مجلد، 2017، ص. 263

يتضح من خلال الشكل أعلاه أن للأمن السيبراني أربعة أبعاد تكمن فيما يلي:

1-1-الموثوقية: يتطلب تحقيق الأمن السيبراني التأكد من استخدام المواقع الموثوقة عند إدخال أو تقديم المعلومات الشخصية عبر الإنترنت. أول خطوات ضمان الأمان هي التحقق من عنوان URLللموقع. إذا كان الموقع يحتوي على "https" في بدايته، فهذا يعني أن الاتصال مشفر وآمن. من جانب آخر، يجب توخي الحذر عند زيارة المواقع التي تبدأ بـ "http" فقط، حيث لا توفر هذه المواقع الحماية اللازمة. في هذه الحالة، يُنصح بتجنب إدخال بيانات حساسة مثل أرقام الحسابات البنكية أو أي معلومات شخصية قد تعرض الأفراد للسرقة أو الاختراق؛[1]

1-2-البريد الاحتيالي: يعد البريد الاحتيالي من أبرز طرق الهجوم التي يتعرض لها الأفراد، حيث يتم إرسال رسائل بريد إلكتروني متخفية على أنها من مصادر موثوقة، مثل الشركات أو الأصدقاء. قد تحتوي هذه الرسائل على مرفقات أو روابط ضارة تهدف إلى سرقة المعلومات الشخصية أو تثبيت برامج ضارة على الأجهزة. لضمان الأمان، يجب عدم فتح المرفقات أو النقر على الروابط المرفقة من مرسلين غير معروفين

[1]-فايزة أحمد الحسيني مجاهد، **مرجع سابق**، ص. 64

أو رسائل تبدو مشبوهة. كما يُنصح بالتحقق من صحة البريد الإلكتروني عبر التواصل المباشر مع المرسل؛[1]

1-3-التحديثات: الحفاظ على تحديث الأجهزة والبرامج هو أمر بالغ الأهمية في عالم الأمن السيبراني. تحتوي التحديثات البرمجية عادة على تصحيحات للثغرات الأمنية التي قد يستغلها القراصنة. مع مرور الوقت، تصبح الأجهزة والبرمجيات القديمة عرضة للهجمات السيبرانية، إذ لا تحتوي على أحدث التصحيحات الأمنية. لذلك، يجب التأكد من تثبيت آخر التحديثات بشكل دوري للأجهزة والبرامج من أجل تقليل المخاطر والحفاظ على الأمان؛[2]

1-4-النسخ الاحتياطي: يعد إجراء النسخ الاحتياطي بشكل منتظم جزءًا أساسيًا من إستراتيجية الأمان السيبراني. يساعد النسخ الاحتياطي في الحفاظ على البيانات الهامة في حال حدوث هجوم سيبراني أو فشل النظام. في حالة تعرض الأجهزة للاختراق أو فقدان البيانات، تتيح النسخ الاحتياطية استعادة الملفات الهامة بسرعة. يُنصح بأن تكون النسخ الاحتياطية مخزنة في مكان آمن، سواء كان ذلك في التخزين السحابي أو على وسائط تخزين خارجية، لضمان الحماية من أي تهديدات قد تتعرض لها البيانات المخزنة.[3]

وعليه يمكن القول أن تحقيق الأمن السيبراني يتطلب استخدام مواقع موثوقة، تجنب البريد الاحتيالي، تحديث الأجهزة بانتظام، وإجراء نسخ احتياطية للبيانات لضمان الحماية من التهديدات الإلكترونية.

رابعا: تحديات الأمن السيبراني

تواجه المؤسسات اليوم العديد من التحديات في مجال الأمن السيبراني، وذلك بسبب التطور التكنولوجي السريع وزيادة الاعتماد على الأنظمة الرقمية في مختلف المجالات، حيث سيتم التطرق إلى هذه التحديات من خلال هذا الفرع.

1-تحديات الأمن السيبراني:

تتمثل تحديات تطبيق الأمن السيبراني في المؤسسات فيما يلي:

1-1-المدة الزمنية لرصد الاختراقات: يُعتبر الوقت عاملاً حاسمًا في اكتشاف الهجمات السيبرانية والحد من آثارها. فكلما طالت مدة بقاء الهجوم غير مكتشف، زادت الأضرار الناتجة عنه. وتشير الإحصاءات إلى أن متوسط الوقت الذي تستغرقه المؤسسات لاكتشاف اختراق أمني يبلغ حوالي 55 يومًا، وهي فترة طويلة تمكّن المهاجمين من التوسع في أنشطتهم التخريبية. في هذا السياق، تبرز أهمية توظيف تقنيات الذكاء الاصطناعي والروبوتات، لما لها من قدرة على مراقبة الأنظمة وتحليل البيانات بشكل مستمر وعلى مدار

---

[1]-**المرجع السابق.**

[2]-أميرة هاتف حداوي، وآخرون، **مرجع سابق**، ص. 692

[3]-فايزة أحمد الحسيني مجاهد، **مرجع سابق**، ص.65.

الساعة، مما يعزز من سرعة اكتشاف التهديدات مقارنةً بالقدرات البشرية المحدودة من حيث الوقت والاستجابة.[1]

1-2-تهديدات إنترنت الأشياء (IoT): يمثل إنترنت الأشياء تحديًا أمنيًا متصاعدًا، حيث أظهرت الدراسات أن نحو 70% من الأجهزة المتصلة ضمن هذا المجال تحتوي على ثغرات أمنية خطيرة. تعود هذه الثغرات غالبًا إلى ضعف تصميم واجهات الويب، ونقل البيانات بطرق غير مشفّرة، بالإضافة إلى نقص وعي المستخدمين حول كيفية تأمين أجهزتهم. ويزداد الخطر نظرًا للطبيعة التفاعلية للأجهزة؛ فاختراق جهاز واحد قد يفتح المجال للوصول إلى شبكة كاملة من الأجهزة المتصلة، مما يضاعف من حجم الأضرار ويصعّب مهمة احتواء الهجمات.[2]

1-3-تأمين الخدمات السحابية: رغم أن 64% من خبراء تقنية المعلومات يرون في الحوسبة السحابية بيئة أكثر أمانًا للبنية التحتية، إلا أن التحديات الأمنية المرتبطة بها ما تزال قائمة. وتكمن الخطورة في الثغرات التي قد تنجم عن عدم تكامل حلول الحماية بين مزوّدي الخدمة والمستخدمين. إذ أن أي خلل في هذا التعاون أو ترك ثغرات غير مغطاة يُمكن أن يُستغل من قِبل المهاجمين. لذلك، يتطلب أمن السحابة إستراتيجية شاملة تضمن الرقابة، التشفير، والتحكم في الوصول، مع توزيع واضح للمسؤوليات الأمنية بين جميع الأطراف.[3]

1-4-نقص الكفاءات في مجال الأمن السيبراني : يُعد النقص الكبير في عدد الخبراء المؤهلين أحد أبرز التحديات التي تواجه المؤسسات حول العالم. فمع تزايد حجم وتعقيد الهجمات السيبرانية، تواجه أكثر من نصف المنشآت صعوبة في العثور على مختصين يمتلكون المهارات التقنية والخبرة اللازمة للتعامل مع التهديدات الحديثة. هذا العجز في الكفاءات يضعف القدرة على الوقاية، الاستجابة، والتعافي من الهجمات، ويؤكد على أهمية الاستثمار في التعليم والتدريب المستمر لتكوين كوادر مؤهلة في هذا المجال الحساس.[4]

من خلال ما سبق يمكن القول أن هذه التحديات تُظهر أن الأمن السيبراني يواجه مخاطر متزايدة تتطلب حلولًا سريعة وفعالة، تشمل تطوير التقنيات، تأمين البنى التحتية، وسد النقص في الكفاءات المتخصصة لضمان حماية الأنظمة والمعلومات.

---

[1]-ندى بنت خالد المرداس، " **الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)**"،المجلة الدولية لنشر البحوث والدراسات، العدد 49، المجلد 05، 2023، ص. 215

[2]-ساعد بوقرص، "**الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة**"، مجلة الأبحاث في الحماية الاجتماعية، العدد 01، المجلد 03، 2022، ص. 73

[3]-ندى بنت خالد المرداس،**مرجع سابق**، ص. 216

[4]-**المرجع السابق.**

في المجمل، يُعد الأمن السيبراني ضرورة لا غنى عنها في ظل التطور التكنولوجي المتسارع، لحماية البيانات والأنظمة من التهديدات الإلكترونية المتزايدة. فهو يشكّل ركيزة أساسية لاستمرارية العمل داخل المؤسسات، ويعتمد على تبني استراتيجيات وقائية، استخدام أدوات رقمية متقدمة، وتوفير كفاءات متخصصة لمواجهة التحديات المتجددة بفعالية.

المطلب الثالث: العلاقة بين القيادة الرقمية والأمن السيبراني

في ظل التحول الرقمي المتسارع، لم تعد القيادة تقليدية، بل أصبحت رقمية تتطلب وعيًا تقنيًا واستعدادًا لمواجهة التحديات السيبرانية المتزايدة. ومن هنا تبرز العلاقة الوثيقة بين القيادة الرقمية والأمن السيبراني، حيث يضطلع القائد الرقمي بدور محوري في بناء ثقافة أمنية واعية داخل المؤسسة.حيث يتناول هذا المطلب أوجه هذا التداخل، ويحلل كيف تسهم أبعاد القيادة الرقمية في تعزيز سلوك الأمن السيبراني.

أولا: القيادة الرقمية في ظل التحول الرقمي

يشهد العالم اليوم تسارعًا رقميًا غير مسبوق، أحدث تغييرات جوهرية في مختلف القطاعات الاقتصادية والإدارية والاجتماعية. فقد أصبحت التقنيات الحديثة مثل الذكاء الاصطناعي، والحوسبة السحابية، وإنترنت الأشياء، من العناصر الأساسية في بنية الأعمال المعاصرة. وفي ظل هذا الواقع المتغير، برزت الحاجة إلى نمط جديد من القيادة يعرف بالقيادة الرقمية، والتي تمثل استجابة استراتيجية لهذه التحولات المتسارعة.[1]

تنبع أهمية القيادة الرقمية من قدرتها على تسخير التكنولوجيا في خدمة الأهداف المؤسسية، وتوجيه عمليات التغيير، وتحفيز بيئة الابتكار. غير أن هذا التحول الرقمي الواسع أفرز تحديات أمنية متزايدة، أبرزها تصاعد التهديدات السيبرانية كالهجمات الإلكترونية، وتسريبات البيانات، والاختراقات الأمنية، التي تهدد البنية التحتية للمؤسسات وتهز ثقة العملاء والمستثمرين.[2]

وعليه، فإن العلاقة بين القيادة الرقمية والأمن السيبراني لم تعد ثانوية، بل أصبحت علاقة تكامل استراتيجي تفرض على القادة تبنّي أدوار جديدة تضمن الحماية والتطور في آنٍ واحد.

ثانيا: مظاهر العلاقة بين القيادة الرقمية والأمن السيبراني

تُعد القيادة الرقمية أحد العوامل الجوهرية في بناء منظومة أمن سيبراني فعّالة داخل المؤسسات، فبقدر ما تعزز القيادة الرقمية من قدرات المؤسسة التقنية، فإنها تفرض أيضًا مستوى أعلى من المسؤولية تجاه حماية المعلومات والأنظمة. وتتجلى مظاهر العلاقة بين القيادة الرقمية والأمن السيبراني من خلال أربعة محاور رئيسية تكمن فيمايلي:

1-تعزيز الثقافة الأمنية المؤسسية:

تُشكّل الثقافة التنظيمية أحد الخطوط الدفاعية الأولى في مواجهة التهديدات السيبرانية. ويضطلع القادة الرقميون بدور مركزي في ترسيخ ثقافة أمنية قائمة على الوعي، الالتزام، والممارسات اليومية

[1]-Ms.Karitika ,**"Leadership in the Cyber Age : Technology Integration for Excellence "**, Journal of Arts Humanities and Social Sciences (GASJAHSS), Issue 01, volume 01 , 2023, P. 15

[2]-**Op. Cit,** P. 16

الصحيحة. من خلال عقد برامج تدريبية منتظمة، وإطلاق حملات توعية داخلية، وتقديم القدوة في الالتزام بسياسات الأمان (مثل تحديث كلمات المرور أو تجنب الروابط المشبوهة)، كما يساهم القائد الرقمي في تحويل الأمن السيبراني من مسؤولية فردية إلى قيمة جماعية متجذّرة في المؤسسة. هذه الثقافة تقلل من احتمالية الأخطاء البشرية وتعزز الحس الأمني لدى جميع أفراد المؤسسة؛[1]

2-الدمج الاستراتيجي للأمن في عملية التحول الرقمي:

لا يمكن اعتبار الأمن السيبراني عنصرًا منفصلًا عن مشاريع التحول الرقمي، بل يجب أن يكون جزءًا لا يتجزأ من التخطيط والتنفيذ. القائد الرقمي الواعي يضمن أن أي مبادرة رقمية جديدة، مثل أتمته العمليات أو إطلاق منصة رقمية، تُرافقها إجراءات أمان مدروسة منذ المراحل الأولى للمشروع. وهذا الدمج الاستباقي يساعد على تقليل الثغرات الأمنية المحتملة، ويرفع من كفاءة المؤسسة في التصدي لأي تهديدات مصاحبة للنمو الرقمي. كما يُظهر التزامًا مؤسسيًا بالأمن بوصفه عنصراً من عناصر الجودة، وليس مجرد استجابة للأزمات؛[2]

3-التفاعل مع التحديات الجديدة:

في ظل التغير المتسارع للتقنيات والتهديدات، لم يعد كافيًا أن تقتصر القيادة على ردود الأفعال، بل باتت مطالبة بتبنّي نهج استباقي وتنبؤي. القيادة الرقمية الفعالة تقوم على متابعة أحدث المستجدات في عالم الأمن السيبراني، مثل هجمات الفدية (ransomware)، والهندسة الاجتماعية، والاختراقات عبر سلاسل التوريد الرقمية. ومن خلال بناء شبكات معلومات، والتواصل مع خبراء الأمن، واستخدام أدوات التحليل التنبؤي، يستطيع القائد الرقمي توجيه المؤسسة نحو حلول وقائية مرنة ومبنية على البيانات، مما يقلل من المفاجآت ويزيد من الجاهزية؛[3]

4-قيادة التغيير والتنسيق بين الفرق:

التحول الرقمي يتطلب بالضرورة تنسيقًا عابرًا للوظائف داخل المؤسسة، إذ لا يمكن ضمان أمن المعلومات دون تكامل جهود كل من قسم تكنولوجيا المعلومات، والموارد البشرية، والإدارة العامة، وحتى فرق التسويق والمبيعات. القائد الرقمي الناجح ينجح في كسر الحواجز بين هذه الأقسام، من خلال بناء فرق عمل متعددة التخصصات تعمل بشكل متناغم ضمن إستراتيجية أمنية موحّدة. كما يشجّع على المشاركة والتفاعل

[1]-RiteshVerma, **"Cyber Security Challenges In The Era of Digital Transformation ",** In Trans disciplinary Threads: Crafting the Future Through Multidisciplinary Research, Volume 01, 2024, P. 179
[2]-**Op. Cit.**
[3]-**Op. Cit,** P. 180

في اتخاذ قرارات الأمان، مما يؤدي إلى رفع مستوى الالتزام والانضباط الداخلي تجاه سياسات الحماية السيبرانية.[1]

يتضح أن القيادة الرقمية تُعد ركيزة أساسية في بناء بيئة أمنية مستدامة داخل المؤسسات، من خلال دمج السياسات السيبرانية في صلب التحول الرقمي . كما أن قدرتها على تنمية الوعي، وتنسيق الجهود، والاستجابة للتحديات، يجعل منها عاملًا فاعلًا في الحد من المخاطر الإلكترونية.

ثالثا: دور القائد الرقمي في تعزيز الأمن السيبراني

يلعب القائد الرقمي دورًا حاسمًا في الحوكمة السيبرانية من خلال مجموعة من الوظائف والمهارات التي تؤثر مباشرةً على الحماية الرقمية للمؤسسة، حيث يكمن دوره فيمايلي:

1-التخطيط الاستراتيجي الأمني:

القائد الرقمي لا يتعامل مع الأمن السيبراني كإجراء طارئ، بل كعنصر أساسي في التخطيط الاستراتيجي للمؤسسة. يشارك في صياغة الرؤية الأمنية طويلة المدى، وتحديد الأولويات والمخاطر، وربطها بأهداف المؤسسة العامة .ويشمل ذلك تطوير السياسات والإجراءات الأمنية، واختيار الأدوات والتقنيات المناسبة، وضمان تخصيص الموارد الكافية لحماية المعلومات. هذا النوع من التخطيط يضمن أن الأمن السيبراني ليس مجرد استجابة للحوادث، بل جزء من إستراتيجية استباقية واضحة المعالم؛[2]

2-تبنّي الذكاء الاصطناعي والتحليلات التنبؤية:

يمتلك القادة الرقميون الفعّالون رؤية متقدمة تُمكّنهم من استثمار أدوات الذكاء الاصطناعي والتعلم الآلي في دعم جهود الأمن السيبراني. فهم يستفيدون من هذه الأدوات لتحليل الأنماط السلوكية للمستخدمين، واكتشاف الشذوذ في البيانات، والتنبؤ بالهجمات المحتملة قبل وقوعها. حيث يساهم هذا التبني الذكي للتقنيات في تعزيز قدرة المؤسسة على الوقاية من التهديدات، والتقليل من الاعتماد على الاستجابة اليدوية، مما يُسرّع من زمن الاستجابة ويقلّل الخسائر؛[3]

3-التدريب والتمكين:

من أهم أدوار القائد الرقمي في مجال الأمن السيبراني هو بناء القدرات الداخلية. حيث يعمل على تطوير برامج تدريبية مستمرة تستهدف جميع العاملين، وتُركز على رفع الوعي الأمني، وتعليم ممارسات الحماية الجيدة، مثل التعامل مع رسائل التصيّد، إدارة كلمات المرور، واستخدام الشبكات الأمنة .كما يشجع القائد الرقمي على ثقافة التعلّم الذاتي والمشاركة، ويمنح الموظفين الثقة والأدوات التي تمكّنهم من اتخاذ

---

[1]-**Op. Cit.**

[2]-Anderson, Ashley, et al, **"Case-Based Learning for Cyber security Leaders: A Systematic Review and Research Agenda."**Information & Management, vol. 61, 2024, p. 104015. DOI : 10.1016/j.im.2024.104015, P1

[3]-**Op. Cit,**P. 2

قرارات صحيحة عند مواجهة مواقف أمنية. وعليه يتحول كل موظف إلى خط دفاع فاعل، مما يقلل من المخاطر الناتجة عن الأخطاء البشرية التي تمثل نسبة كبيرة من الاختراقات الأمنية.[1]

يتبين أن القائد الرقمي يلعب دورًا جوهريًا في تعزيز الأمن السيبراني، من خلال دمج الرؤية الإستراتيجية بالتقنيات الحديثة، وتفعيل دور العنصر البشري، ما يضمن استجابة مرنة وفعالة لمختلف التهديدات السيبرانية.

رابعا: تأثير أبعاد القيادة الرقمية على تعزيز سلوك الأمن السيبراني

تؤثر أبعاد القيادة الرقمية بشكل فعّال في تشكيل السلوكيات الأمنية داخل المؤسسات، حيث تمثل كل بُعد منها ركيزة أساسية تسهم في رفع مستوى الوعي والامتثال الأمني لدى العاملين. ويمكن تلخيص هذه الأبعاد على النحو التالي:

1-المعرفة الرقمية:

تعكس مدى إلمام القائد بالمفاهيم والأدوات التكنولوجية، وقدرته على نقل هذه المعرفة إلى الموظفين بطرق مبسطة وعملية. فكلما ارتفع مستوى المعرفة الرقمية لدى القيادة، ازداد وعي الموظفين بمخاطر الإنترنت وأهمية الالتزام بالإجراءات الوقائية مثل حماية كلمات المرور وتحديث الأنظمة؛[2]

2-الابتكار الرقمي:

يرتبط هذا البعد بقدرة القائد على دفع المؤسسة نحو تبنّي حلول أمنية مبتكرة وغير تقليدية، ما يساعد في التصدي للتهديدات الجديدة بفعالية. كما يُشجع هذا النهج على تطوير أدوات وتقنيات داخلية تعزز من الحماية وتكشف الثغرات قبل استغلالها؛[3]

3-الرؤية الرقمية:

يمثل هذا البعد الإدراك القيادي بضرورة دمج الأمن السيبراني ضمن رؤية المؤسسة المستقبلية، ووضعه كأولوية ضمن الخطط الإستراتيجية، بما يضمن استدامة التحول الرقمي في بيئة آمنة ومنضبطة؛[4]

4-المشاركة والتعاون:

يشير إلى قدرة القيادة على خلق بيئة تشاركية تعزز من انخراط الموظفين في جهود الحماية، وتدفعهم للإبلاغ عن المخاطر دون تردد. كما يعزز هذا البعد العمل الجماعي بين الوحدات المختلفة، بما يسهم في

---

[1]-**Op. Cit,**P. 3

[2]-أميرة هاتف حداوي، وآخرون، **مرجع سابق**، ص. 697

[3]-**المرجع السابق**، ص. 698

[4]-**المرجع السابق.**

تعزيز سرعة الاستجابة للأحداث السيبرانية وتقليل آثارها.[1]

من خلال ما سبق يمكن القول أن هذه الأبعاد أهمية القيادة الرقمية كأداة فاعلة في غرس ثقافة أمنية متكاملة، حيث تساهم مجتمعة في رفع كفاءة المؤسسة في مواجهة التهديدات الرقمية من خلال تحسين سلوكيات الأفراد نحو المزيد من الانضباط والوعي الأمني.

وعليه فللقيادة الرقمية تُعد ركيزة أساسية في تعزيز الأمن السيبراني داخل المؤسسات، حيث تعتمد على التكنولوجيا المتقدمة واليقظة السيبرانية لرصد التهديدات واستباقها. وتساعد هذه القيادة في اتخاذ قرارات سريعة وفعالة من خلال أنظمة الإنذار المبكر وتحليل البيانات، مما يضمن حماية البنية الرقمية وتقليل آثار الهجمات المحتملة .كما يتضح أن القيادة الرقمية تمثل أحد الأساليب الحديثة في إدارة المخاطر الإلكترونية، بفضل دورها في تمكين الكفاءات البشرية، وتطوير الأداء المؤسسي، والتفاعل السريع مع الإشارات الرقمية الضعيفة، ما يعزز قدرة المؤسسة على التنبؤ بالهجمات والتحكم فيها بفعالية في بيئة رقمية متغيرة . وكما تناولت العديد من الدراسات موضوع القيادة الرقمية في سياق حماية الفضاء السيبراني، وأخرى ركزت على الأمن السيبراني كأحد مكونات استدامة المؤسسات.

[1]–**المرجع السابق**، ص. 699

المبحث الثاني: الدراسات السابقة

تُعدُّ الدراسات السابقة خطوة أساسية لبدء أي دراسة جديد، حيث تشكّل الأساس الذي يعتمد عليه الباحث لفهم الموضوع بشكل متعمق، كما تساهم في تقديم نظرة شاملة حول تطور المفهوم محل الدراسة، وتساعد في تحديد اتجاهات البحث المستقبلية. إضافةً إلى ذلك، تُثري الدراسات السابقة البحث العلمي من خلال توفير السياق العلمي والتأسيس للعمل الجديد، كما تُعدُّ مصدراً قيّماً للمعرفة لما تتضمنه من نتائج وتحليلات ومناقشات تسهم في التعرف على مختلف أبعاد المشكلة البحثية وفرضياتها وطرق معالجتها .وبناءً على ذلك، من الضروري استعراض أهم الدراسات المتعلقة بالقيادة الرقمية وتأثيرها على تعزيز سلوك الأمن السيبراني، حيث سيتم تقديم عرض متكامل لأبرز الأبحاث ذات الصلة بهذا الموضوع. ولتحقيق ذلك، سيتم تقسيم الدراسات إلى ثلاثة محاور رئيسية، كما سيتم توضيحها فيما يلي:

- **المطلب الأول: الدراسات باللغة العربية؛**
- **المطلب الثاني: الدراسات باللغة الأجنبية؛**
- **المطلب الثالث: الاختلاف بين الدراسة الحالية والدراسات السابقة.**

المطلب الأول: الدراسات باللغة العربية

تناول العديد من الباحثين في الدول العربية دراسة القيادة الرقمية والأمن السيبراني، حيث اختلفت وجهات نظرهم تبعا لطبيعة المؤسسة التي طُبّقت فيها هذه الدراسات. ومن بين الأبحاث التي تناولت هذا الموضوع ما يلي:

أولا: الدراسات السابقة المتعلقة بالقيادة الرقمية

تكمن أهم الدراسات المتعلقة بالقيادة الرقمية باللغة العربية فيمايلي:

1-دراسة جمال زمورة، ليلى بن عيسى، " **دور القيادة الرقمية في نجاح التحول الرقمي للخدمات العمومية في الجزائر**"، مجلة الاقتصاديات المالية البنكية وإدارة الأعمال، العدد 02، المجلد 11، 2022.

استعرضت هذه الدراسة دور القيادة الرقمية في نجاح التحول الرقمي للخدمات العمومية في الجزائر، حيث ركزت على أهمية القيادة الرقمية في ظل الثورة التكنولوجية المتسارعة وضرورة تبني نماذج قيادية جديدة في الفضاء الافتراضي.ولقد تمحورت إشكالية الدراسة حول مدى تأثير القيادة الرقمية على نجاح عملية التحول الرقمي في القطاع العمومي الجزائري. كما استخدمت الدراسة منهجًا وصفيًا وتحليليًا لتشخيص واقع القيادة الرقمية وأهميتها في الإدارة العمومية، في حين أنها توصلت إلى أن غياب القيادة الرقمية يشكل عائقًا أمام التحول الرقمي الناجح، مما يستدعي تطوير برامج تدريبية وتأهيلية للقادة في القطاع العمومي. وأوصت بضرورة تعزيز الثقافة الرقمية، وتبني نماذج قيادية متطورة، والتركيز على تطوير الموارد البشرية لضمان تحقيق تحول رقمي فعال ومستدام.

2-دراسة حنان البدري كمال، حنان عبد الستار محمود، "**القيادة الرقمية كمدخل لتعزيز المرونة التنظيمية لدى القيادات الأكاديمية بجامعة أسوان**"، المجلة التربوية كلية التربية، العدد 100، المجلد 01، 2022.

استهدفت هذه الدراسة استكشاف دور القيادة الرقمية في تعزيز المرونة التنظيمية لدى القيادات الأكاديمية في جامعة أسوان، من خلال تحليل الإطار النظري لكل من القيادة الرقمية والمرونة التنظيمية، بالإضافة إلى رصد واقع ممارستها في الجامعة. حيث تمحورت الإشكالية حول التساؤل التالي: ما مدى تأثير القيادة الرقمية على تحسين القدرة التنظيمية للجامعة في مواجهة التحديات والتغيرات السريعة؟

كما اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث شملت أربعة محاور: الإطار العام، الإطار النظري، الإجراءات الميدانية، والنتائج والتوصيات. وفي الجانب التطبيقي، قامت الدراسة برصد واقع القيادة الرقمية ومدى تأثيرها على المرونة التنظيمية لدى القيادات الأكاديمية.

وقد توصلت الدراسة إلى مجموعة من النتائج، من أهمها: أن مستوى نشر ثقافة التعلم الرقمي لدى القيادات الأكاديمية كان متوسطًا، حيث تراوحت مستويات التبني بين ضعف الدعم التقني وتعقيد الإجراءات الإدارية، مما أثر على فاعلية القيادة الرقمية. كما تبين أن تحقيق المواطنة الرقمية داخل الجامعة لا يزال بحاجة إلى تعزيز البنية التحتية الرقمية والتدريب المستمر لضمان التحول الرقمي الفعّال. بالإضافة إلى ذلك، أظهرت الدراسة أن المرونة التنظيمية للقيادات الأكاديمية كانت في مستوى متوسط، مما يشير إلى الحاجة لتطوير استراتيجيات قيادية أكثر تكيفًا مع التحولات الرقمية . إلى جانب ذلك، قدمت الدراسة تصورًا مقترحًا لتعزيز المرونة التنظيمية لدى القيادات الأكاديمية في جامعة أسوان، من خلال تحسين البنية التحتية الرقمية، وتبني أساليب القيادة الرقمية الحديثة، وتعزيز مهارات القادة الأكاديميين في التعامل مع التحول الرقمي.

3-دراسة منى عبد عليّ المهنّديّ ، **دور القيادة العليا في تبني حالة التغيير وتضمين إستراتيجية التحول الرقميّ دراسة حالة: الهيئة العامة لشؤون القاصرين بدولة قطر** ، رسالة ماجستير للحصول على درجة الماجستير التنفيذي في القيادة جامعة قطر، 2023.

هدفت هذه الدراسة إلى استكشاف دور القيادة الرقمية في دعم استراتيجيات التحول الرقمي في المؤسسات الحكومية، وذلك من خلال دراسة حالة الهيئة العامة لشؤون القاصرين في دولة قطر. حيث تمحورت الإشكالية حول التساؤل التالي: كيف يمكن للقيادة الرقمية أن تسهم في تحقيق تحول رقمي ناجح داخل المؤسسات الحكومية، وما هي التحديات التي تواجه القادة في تبني هذا التحول؟

كما سعت الدراسة إلى تحليل دور القيادة العليا في تضمين التحول الرقمي ضمن استراتيجياتها، ومدى تأثير ذلك على كفاءة المؤسسات الحكومية وقدرتها على التكيف مع التطورات التكنولوجي.

إلى جانب ذلك اعتمدت الدراسة على المنهج النوعي التحليلي، حيث تم جمع البيانات من خلال مقابلات معمقة مع القادة والمديرين في الهيئة، بالإضافة إلى تحليل استراتيجيات التحول الرقمي المتبعة. في حين أن أظهرت النتائج وجود علاقة قوية بين تبني القيادة الرقمية ونجاح التحول الرقمي، حيث لعبت القيادة العليا دورًا حاسمًا في تهيئة البنية التحتية الرقمية، وتطوير ثقافة الابتكار، وتعزيز التعلم المستمر داخل المؤسسة. كما أوضحت أن القيادة الرقمية الفعالة تساهم في التغلب على تحديات التحول الرقمي مثل مقاومة التغيير وضعف المهارات

الرقمية، وأوصت الدراسة بضرورة تعزيز الاستثمار في تطوير القادة الرقميين، وتوفير برامج تدريبية مستدامة، وصياغة استراتيجيات واضحة للتحول الرقمي، لضمان تحقيق تحول رقمي ناجح ومستدام في المؤسسات الحكومية.

4-دراسة سرين عزيز "حسن حسني" الجيوسي، **القيادة الرقمية وعلاقتها بالاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية** ، مذكرة ماجستير تخصص الإدارة والقيادة التربوية، جامعة الشرق الأوسط، 2024.

هدفت هذه الدراسة إلى تحليل العلاقة بين ممارسة القيادة الرقمية ومستوى الاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية، من خلال دراسة تأثير أبعاد القيادة الرقمية، مثل الابتكار، المواطنة الرقمية، ثقافة التعلم في العصر الرقمي، والاستثارة الفكرية، على مستويات الاحتراق الرقمي. حيث تمحورت إشكالية الدراسة حول التساؤل التالي: ما مدى تأثير القيادة الرقمية على مستويات الاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية؟

في حين أنها سعت إلى توضيح العلاقة بين ممارسات القيادة الرقمية ومستوى الإجهاد الرقمي الناتج عن الاستخدام المفرط للتكنولوجيا. كما أظهرت النتائج أن مستوى ممارسة القيادة الرقمية في المدارس الخاصة الأردنية كان متوسطًا، مع تفاوت في تطبيق أبعادها المختلفة، كما كان مستوى الاحتراق الرقمي لدى المعلمين متوسطًا، حيث ظهرت فروق في الأبعاد مثل الإرهاق العاطفي، الإدمان الرقمي، الحرمان الرقمي، وتبدد الشخصية. كما توصلت الدراسة إلى علاقة ارتباطية إيجابية ذات دلالة إحصائية بين القيادة الرقمية والاحتراق الرقمي، مما يعني أن تعزيز ممارسات القيادة الرقمية قد يسهم في تقليل مستويات الاحتراق الرقمي. وأوصت الدراسة بضرورة توفير الأدوات الرقمية المناسبة، وتنظيم ورش تدريبية لتعزيز مهارات المعلمين في التعامل مع التكنولوجيا، والتوعية بالمخاطر المرتبطة بالاستخدام المفرط للأدوات الرقمية، وذلك لضمان بيئة تعليمية أكثر توازنًا واستدامة.

ثانيا: الدراسات حول الأمن السيبراني

تتمثل أهم الدراسات المتعلقة بالأمن السيبراني باللغة العربية فيمايلي:

1-دراسة سمير بارة، "**الأمن السيبراني (Cyber Security) في الجزائر: السياسات والمؤسسات**" ، المجلة الجزائرية للأمن الإنساني، العدد 04،2017.

تناولت هذه الدراسة موضوع الأمن السيبراني في الجزائر، مسلطة الضوء على السياسات والمؤسسات المعنية بحماية الفضاء الإلكتروني. حيث هدف الباحث من خلال هذه الدراسة إلى الإجابة على الإشكالية التالية: ما هو دور الدفاع الوطني في تحقيق الأمن السيبراني في الجزائر، أمام التحديات الوطنية والعالمية التي يفرضها الفضاء السيبراني حاليا ومستقبلا؟

كما ركزت الدراسة على تحليل جهود الدولة في تعزيز الأمن السيبراني من خلال الأجهزة الأمنية المتخصصة والهياكل التنظيمية المختلفة. ومن أهم النتائج التي توصلت إليها أن الاعتماد المتزايد على

التكنولوجيا يزيد من المخاطر الأمنية، مما يتطلب استراتيجيات دفاعية قوية وتعاوناً دولياً لمكافحة الجرائم الإلكترونية. وأوصت الدراسة بضرورة تعزيز التشريعات وتطوير الكفاءات الوطنية في مجال الأمن السيبراني.

2-دراسة مروة فتحى السيد البغدادي، "**اقتصاديات الأمن السيبراني في القطاع المصرفي**"، مجلة البحوث القانونية والاقتصادية، العدد 76، المجلد 11، 2021.

تهدف هذه الدراسة إلى محاولة إظهار اقتصاديات الأمن السيبراني في القطاع المصرفي، مركزة على التحديات والتهديدات التي تواجه البنوك الإلكترونية في ظل التطور التكنولوجي المتسارع. حيث تمحورت الإشكالية حول: مدى تأثير الأمن السيبراني على تحسين الخدمات المصرفية الإلكترونية، والتهديدات المرتبطة بها، وطرق التحوط منها. كما عالجت الدراسة الموضوع من خلال تحليل طبيعة الأمن السيبراني، وأنواع المخاطر السيبرانية، وتأثيرها على العمليات المصرفية الإلكترونية. في حين أن توصلت الدراسة إلى أن القطاع المصرفي يعد من أكثر القطاعات تعرضًا للمخاطر السيبرانية، مما يستدعي تعزيز التشريعات واللوائح التنظيمية، وتطوير برامج الحماية الإلكترونية، وزيادة وعي المؤسسات المصرفية حول أساليب الوقاية من الهجمات السيبرانية.

3-دراسة فايزة أحمد الحسني مجاهد، "**الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية**"،مجلة بحث وتربية المعهد الوطني للبحث في التربية،العدد 02، المجلد 13، 2023.

هدفت هذه الدراسة إلى استكشاف دور الوعي بالأمن السيبراني في العصر الرقمي، من خلال تحليل مدى تأثيره في حماية الأفراد والمؤسسات من المخاطر الإلكترونية. حيث تمحورت الإشكالية حول التساؤل: هل الوعي بالأمن السيبراني يحافظ على الهوية الثقافية للطلاب في عصر المعلوماتية؟

حيث سعت الدراسة إلى توضيح العلاقة بين التقدم التكنولوجي وزيادة التهديدات السيبرانية، مع التركيز على أهمية تعزيز الثقافة الأمنية الرقمية. وأظهرت النتائج أن الوعي بالأمن السيبراني يعد ضرورة وليس ترفًا، إذ تبين أن قلة الإدراك بالمخاطر الإلكترونية تؤدي إلى ارتفاع معدل الاختراقات والهجمات السيبرانية. كما أكدت الدراسة على دور التعليم والتدريب المستمر في تعزيز الحماية السيبرانية، وأوصت بضرورة إدماج الأمن السيبراني في المناهج الدراسية، وتنظيم حملات توعوية، ووضع سياسات صارمة للحد من الجرائم الإلكترونية.

4-دراسة عبد القادر صوادق، وآخرون، "**أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية**"، مجلة أبحاث اقتصادية معاصرة، العدد 01، المجلد 06، 2023.

هدفت هذه الدراسة إلى تحليل أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة، وذلك عبر دراسة حالة بنك التنمية المحلية (BDL) في ولاية غرداية. حيث تمحورت الإشكالية حول التساؤل التالي: ما مدى تأثير جاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة لدى عملاء البنك؟

في حين أنها سعت إلى تحديد العلاقة بين هذه العوامل ومدى تأثيرها على ثقة العملاء في التعاملات المصرفية الرقمية، كمااعتمدت الدراسة على المنهج الكمي باستخدام نموذج تحليل المسار (Path Analysis) لاختبار التأثيرات المباشرة وغير المباشرة لمتغيرات الدراسة، حيث تم جمع البيانات من عينة مكونة من 121 مفردة بنسبة استجابة 91.09%، وتم تحليلها باستخدام برنامج (AMOS V.25).

حيثأظهرت النتائج أن جاهزية البيئة المادية والبشرية للأمن السيبراني تؤثر بشكل غير مباشر على استخدام الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة، حيث يفضل العملاء التعامل مع بنك يوفر خدمات إلكترونية آمنة وموثوقة، كماأوصت الدراسة بضرورة تعزيز آليات تقليل المخاطر المدركة لدى العملاء، واعتماد تقنيات متقدمة للحماية السيبرانية، وتحسين جاهزية البيئة التكنولوجية والبشرية داخل البنوك، لضمان خدمات مصرفية إلكترونية أكثر أمانًا وثقة.

ثالثا: دراسة حول القيادة الرقمية والأمن السيبراني

تتمثل الدراسة السابقة التي جمعت بين القيادة الرقمية والأمن السيبراني باللغة العربية فيمايلي:

1-دراسة أميرة هاتف حداوي، وآخرون، "**القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في الالمؤسسات**"، مجلة العلوم الإنسانية والطبيعية، العدد 01، المجلد 05، 2024.

هدفت هذه الدراسة إلى تحليل دور القيادة الرقمية في تعزيز سلوك الأمن السيبراني في الالمؤسسات، وذلك من خلال دراسة حالة لمجموعة من المصارف الأهلية في محافظة النجف الأشراف. حيث تمحورت الإشكالية حول التساؤل التالي: ما مدى مساهمة القيادة الرقمية في تعزيز سلوك الأمن السيبراني داخل المصارف الأهلية؟

في حين أن الدراسة سعت إلى تحديد تأثير أبعاد القيادة الرقمية، مثل الرؤية الرقمية، الابتكار الرقمي، المعرفة الرقمية، والمشاركة والتعاون، على سلوكيات الأمن السيبراني للعاملين، والتي تشمل تأمين الأجهزة، إنشاء كلمات المرور، الوعي الاستباقي، والتحديث المستمر. كما اعتمدت الدراسة على المنهج الكمي باستخدام الاستبيانات كأداة رئيسية لجمع البيانات، حيث تم توزيع 120 استبانة على عينة من العاملين في المصارف الأهلية، وتم تحليل 97 استبانة صالحة باستخدام برمجيات إحصائية مثل:(SPSS V.25)و(SMARTPLS V.4)لاختبار علاقات التأثير والارتباط بين المتغيرات.

حيث أظهرت النتائج وجود علاقة إيجابية ذات دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني، حيث تبين أن تطبيق ممارسات القيادة الرقمية يعزز مستوى الوعي والتفاعل مع إجراءات الحماية السيبرانية لدى العاملين . وأوصتالدراسة بضرورة تعزيز استخدام القيادة الرقمية في المؤسسات المصرفية، وتطوير برامج تدريبية لرفع الوعي الأمني السيبراني، واعتماد تقنيات متقدمة لحماية المعلومات، مما يسهم في تقليل المخاطر السيبرانية وتحسين الأداء الأمني داخل المصارف.

المطلب الثاني: الدراسات السابقة باللغة الأجنبية

وجددت العديد من الدراسات الأجنبية التي تدرس موضوع القيادة الرقمية وسلوك الأمن السيبراني من وجهات نظر مختلفة في قطاعات مختلفة من بينها ما يلي:

أولا: الدراسات حول القيادة الرقمية

تكمن أهم الدراسات المتعلقة بالقيادة الرقمية باللغة الأجنبية فيمايلي:

1-دراسة أمينة دهيمات، محمد بارودي، " **مراجعة الأدبيات حول العلاقة بين خصائص القيادة الرقمية والتحول الرقمي القائم على القدرات الديناميكية**" ، مجلة النمو الاقتصادي وريادة الأعمال مختبر دراسات التنمية المكانية وريادة الأعمال، العدد 03، المجلد 05، 2022.

- Amina Dehimat, Mohammed Baroudi, **"Reviewing the literature on the link between Digital Leadership characteristics and Digital Transformation Based on Dynamic Capabilities"**, Journal of Economic Growth and Entrepreneurship JEGE Spatial and entrepreneurial development studies laboratory, Issue 03, volume 05, 2022.

تناولت الدراسة العلاقة بين خصائص القيادة الرقمية والتحول الرقمي استنادًا إلى نظرية القدرات الديناميكية، حيث تؤكد أن التحول الرقمي ليس مجرد تبنٍ للتكنولوجيا، بل يتطلب قيادة قوية قادرة على استشعار التغيرات، اقتناص الفرص، وإعادة تشكيل المؤسسات لمواكبة التطورات الرقمية.

حيث تنطلق الدراسة من خلال طرح التساؤل التالي: كيف تؤثر خصائص القيادة الرقمية على نجاح عملية التحول الرقمي في المؤسسات من خلال القدرات الديناميكية؟

مما يستدعي فهمًا أعمق للقدرات القيادية المطلوبة لضمان نجاح هذه العملية، كما تعتمد الدراسة على مراجعة الأدبيات السابقة لاستخلاص العوامل الحاسمة في نجاح التحول الرقمي، وتبرز دور القادة في تحسين نماذج الأعمال، تعزيز الابتكار، وتحفيز التعاون داخل المؤسسات. في حين أنها تقترح دراسة نموذجًا نظريًا يوضح الروابط بين القيادة الرقمية والقدرات الديناميكية، مشيرة إلى الحاجة لمزيد من الأبحاث التجريبية للتحقق من فعاليته في بيئات تنظيمية مختلفة.

2-دراسة مبارك محسن الفارس، مرعي حسن حمد بني خالد، " **تأثير القيادة الرقمية على أداء العاملين في المستشفيات الكويتية**"، مجلة العلوم الاقتصادية والإدارية والقانونية، العدد 19، المجلد 06، 2022.

- Mubarak Mohsen Al- Faris, Merei Hassan Hamad Bani Khaled, **" Impact of Digital Leadership on Kuwaiti Hospitals' Employees' Performance"**, Journal of Economic, Administrative and Legal Sciences , Issue 19, volume 06, 2022 .

تهدف هذه الدراسة إلى تحليل أثر القيادة الرقمية بأبعادها الثلاثة (الابتكار، الإقناع، والمعرفة) على أداء الموظفين في المستشفيات الكويتية، حيث تم استخدام المنهج الوصفي التحليلي عبر استبيان موزع على 372 إداريًا، واسترجاع 277 استبيانًا صالحًا للتحليل، حيث انطلقت الدراسة من خلال التساؤل التالي: ما هو تأثير القيادة الرقمية على أداء الموظفين في المستشفيات الكويتية؟

كما تتعلق الدراسة بالحاجة إلى تحسين أداء الموظفين في المستشفيات، خاصة في ظل جائحة كورونا، مع ندرة الأبحاث حول تأثير القيادة الرقمية في هذا القطاع. في حين أنها أظهرت النتائج وجود تأثير إيجابي ذي دلالة إحصائية للقيادة الرقمية، حيث كان بُعد المعرفة الأكثر تأثيرًا، بينما لم يكن للابتكار تأثير واضح، وكان للإقناع تأثير ضعيف. وأوصت الدراسة بتعزيز مفهوم القيادة الرقمية في بيئة العمل، وتطوير وعي الموظفين حول أهميتها، بالإضافة إلى توفير برامج تدريبية تسهل تبادل المعرفة ورفع مستوى الأداء، كما دعت إلى توسيع نطاق الدراسات المستقبلية لتشمل قطاعات أخرى مثل الاتصالات.

3-دراسة تيتيانا إيرتو وآخرون، "**دور الذكاء العاطفي للقادة الرقميين في الحد من إجهاد التكنولوجيا لدى الموظفين**"، آفاق الأعمال، العدد 03، المجلد 67، 2024.

- Titiana Ertiö et al , **"The Role of Digital Leaders' Emotional Intelligence in Mitigating Employee Techno stress",** Business Horizons, Issue 03, volume 67, 2024.

تهدف الدراسة إلى تحليل دور الذكاء العاطفي للقادة الرقميين في الحد من إجهاد التكنولوجيا لدى الموظفين، وذلك في ظل التحول الرقمي المتسارع الذي يفرض تحديات جديدة على بيئات العمل. حيث تنطلق الدراسة من إشكالية رئيسية مفادها: إلى أي مدى يمكن للذكاء العاطفي للقادة الرقميين أن يساهم في التخفيف من إجهاد التكنولوجيا لدى الموظفين في سياق التحول الرقمي؟

وقد اعتمدت الدراسة على مراجعة الأدبيات السابقة وتحليل استراتيجيات القيادة الرقمية، حيث أظهرت النتائج أن الذكاء العاطفي للقادة يسهم بشكل كبير في تقليل الضغوط النفسية الناتجة عن الاستخدام المفرط للتكنولوجيا من خلال تعزيز التواصل الفعّال، الشفافية، والثقة بين القادة والموظفين. كما أوضحت الدراسة أن تطوير المهارات العاطفية للقادة، مثل الوعي الذاتي، التنظيم الذاتي، والتعاطف، يساعد في تحسين بيئة العمل الرقمية ويحد من التأثيرات السلبية للإجهاد التكنولوجي. كما توصي الدراسة بضرورة تبني استراتيجيات قيادة قائمة على الذكاء العاطفي لضمان تحول رقمي أكثر توازناً، وتعزيز رفاهية الموظفين في ظل التطورات التكنولوجية المستمرة.

ثانيا: الدراسات حول الأمن السيبراني

تتمثل أهم الدراسات المتعلقة بالأمن السيبراني باللغة الأجنبية فيمايلي:

1-دراسة حياة سرير الحرتسي، "**دراسة معمقة لإستراتيجية مقترحة للأمن السيبراني في ظل الاقتصاد الرقمي في الجزائر**"، مجلة الاقتصاد والإدارة،العدد 01، المجلد 23، 2023.

- Hayet Sereir El Hirtsi**, " An In-Depth Study For A Proposed National Cyber Strategy For Digital Economy In Algeria"**, Journal Of Economics And Management**,** Issue 01, volume 23, 2023.

تهدف الدراسة إلى تحليل استراتيجيات الأمن السيبراني الوطنية في ثمانية عشر دولة، من حيث المفاهيم، الرؤية، الأهداف، المبادئ، وخطط العمل التشغيلية، وذلك لتقديم رؤية مقترحة لإستراتيجية وطنية للأمن السيبراني تدعم الاقتصاد الرقمي في الجزائر. حيث تنطلق الدراسة من إشكالية رئيسية تتمثل فيما يلي: ما هي الحاجة إلى تطوير إستراتيجية وطنية للأمن السيبراني في الجزائر تواكب التحول الرقمي المتسارع وتحمي الاقتصاد الرقمي من التهديدات السيبرانية المتزايدة؟

بينما أظهرت النتائج أن بناء إستراتيجية فعالة يجب أن يعتمد على تحسين أنظمة أمن المعلومات، توفير تقنيات متقدمة للأمن السيبراني، تطوير القدرات البشرية، وتحديث الأطر القانونية والقضائية بما يتماشى مع المعايير الدولية. كما أوصت الدراسة بتأسيس هيئة وطنية متخصصة في الأمن السيبراني، إصدار قوانين صارمة لمكافحة الجرائم الإلكترونية، تعزيز التعاون الدولي في المجال، وتشجيع البحث والتطوير في التقنيات السيبرانية، لضمان بيئة رقمية آمنة ومستدامة تدعم نمو الاقتصاد الرقمي في الجزائر.

2-دراسة رحاب يوسفي، محمد البشير الإبراهيمي، "**تحديات الأمن السيبراني والتعاون الدولي**" ، مجلة العلوم القانونية والإنسانية،العدد 03، المجلد 17، 2024.

- Rihab Yousfi, Mohamed El Bachir El Ibrahimi, **"Cyber security Challenges and International Cooperation"** , Journal of law and humanities Sciences,Issue03, volume 17, 2024.

تهدف الدراسة إلى تحليل التحديات التي تواجه الأمن السيبراني والتعاون الدولي في ظل تزايد الجرائم الإلكترونية وضرورة تبادل المعلومات بين الدول لضمان حماية البنية التحتية الرقمية والبيانات الشخصية. حيث تنطلق الدراسة من إشكالية رئيسية مفادها: إلى أي مدى يمكن تحقيق تكامل فعال بين الأطر القانونية والسياسات المتعلقة بالأمن السيبراني وحماية البيانات الشخصية لضمان أمن المعلومات وسرية الأفراد في ظل التهديدات الرقمية المتزايدة؟

وقد تناولت الدراسة جهود التعاون الدولي في مكافحة الجرائم السيبرانية، بما في ذلك الاتفاقيات الدولية مثل اتفاقية بودابست، إلى جانب الاستراتيجيات الوطنية مثل القوانين الجزائرية لمكافحة الجرائم

الإلكترونية. كما أشارت إلى التحديات المرتبطة بتوازن حماية البيانات الشخصية مع الحاجة إلى تبادل المعلومات، موصية بتعزيز الأطر القانونية وتطوير آليات تعاون دولية أكثر فعالية لحماية الأمن السيبراني دون المساس بحقوق الأفراد في الخصوصية.

3-دراسة عبد الرزاق برادة، فاطمة دهماني، "**مستوى الوعي بالأمن السيبراني والاستجابة للجرائم السيبرانية لدى مستخدمي الإنترنت في الجزائر: دراسة ميدانية على طلبة كلية العلوم الإنسانية والاجتماعية بجامعة جيلالي بونعم خميس مليانة**"، مجلة الرسالة للدراسات الإعلامية،العدد 03، المجلد 08، 2024.

- Abd rrezzaq Barada, Fatima Dahmani, **" The Level of Cyber security Awareness and Cybercrime Response among Internet Users in Algeria: A Field Study on Students of the Faculty of Humanities and Social Sciences at the University of Djilali Bounaam in Khamis Miliana"**, The journal of El-Ryssala for media studies,Issue03, volume 08, 2024.

تهدف الدراسة إلى تقييم مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية بين مستخدمي الإنترنت في الجزائر، من خلال دراسة ميدانية على عينة مكونة من 355 طالبًا من كلية العلوم الإنسانية والاجتماعية بجامعة جيلالي بونعامة بخميس مليانة. حيث تنطلق الدراسة من إشكالية رئيسية مفادها: ما هو مستوى الوعي بالأمن السيبراني والاستجابة للجرائم الإلكترونية بين طلاب الجامعة في الجزائر؟

وقد أظهرت النتائج أن 53.23% من الطلاب يستخدمون الإنترنت بانتظام، و 61.97% يقضون أكثر من ثلاث ساعات يوميًا على الإنترنت، في حين كان مستوى الوعي بالأمن السيبراني متوسطًا بنسبة 59.15%. كما أوضحت الدراسة أن 46.47% من الطلاب يرون أن الوعي السيبراني ضروري لمنع الجرائم الإلكترونية، بينما 28.73% يؤيدون تشجيع الإبلاغ عن الحوادث السيبرانية، و 27.60% يقترحون تنظيم ورش عمل ودورات تدريبية لتعزيز الأمن السيبراني.

كما أوصت الدراسة بضرورة تحسين التوعية السيبرانية في البيئة الجامعية، من خلال تعزيز ثقافة الحماية الرقمية، وتوفير دورات تدريبية متخصصة، وتشجيع التعاون بين المؤسسات الأكاديمية والجهات الأمنية لمواجهة الجرائم السيبرانية بفعالية.

ثالثا: دراسة حول القيادة الرقمية والأمن السيبراني

تتمثل الدراسة السابقة التي لمّت بين القيادة الرقمية والأمن السيبراني باللغة الأجنبية فيمايلي:

1-دراسة كارتيكا، "**القيادة في العصر السيبراني: دمج التكنولوجيا من أجل التميز**"، مجلة الفنون والعلوم الإنسانية والاجتماعية (GASJAHSS)، العدد 01، المجلد 01، 2023.

-Ms.Karitika ,**"Leadership in the Cyber Age : Technology Integration for Excellence "**, Journal of Arts Humanities and Social Sciences (GASJAHSS), Issue 01, volume 01 , 2023.

تناولت هذه دراسة مفهوم القيادة في العصر الرقمي من زاوية تكاملها مع متطلبات الأمن السيبراني، مشيرة إلى أن القائد الحديث مطالب بتجاوز الأدوار التقليدية، ليتحول إلى عنصر فاعل في التوجيه الاستراتيجي الرقمي وضمان الحماية المعلوماتية. وقد انطلقت الدراسة من إشكالية محورية تتمثل في: كيف يمكن للقادة في العصر الرقمي تحقيق التوازن بين تسريع التحول التكنولوجي وتعزيز الأمن السيبراني في ظل بيئة مليئة بالمخاطر الرقمية المتجددة؟

كما أكّدت الدراسة أن القيادة الرقمية تمثل مزيجًا من الرؤية المستقبلية والقدرة على استثمار التكنولوجيا الحديثة، مثل الذكاء الاصطناعي وأنظمة الإنذار المبكر، في التنبؤ بالتهديدات الإلكترونية والحد من آثاره ا. وأبرز النتائج أظهرت أن فعالية الأمن السيبراني تتوقف بدرجة كبيرة على وعي القائد وتفاعله مع المخاطر الرقمية، وأن القيادة الواعية تُسهم في بناء ثقافة أمنية تشاركية، تدعم سرعة الاستجابة، وتُقلل من الأخطاء البشرية.

أما التوصيات، فقد دعت الدراسة إلى إعداد برامج تدريب متخصصة للقادة الرقميين، وإشراكهم في صياغة السياسات الأمنية، وضرورة دمج البعد السيبراني في رؤية المؤسسة على المدى الطويل، لضمان تحول رقمي آمن ومستدام.

المطلب الثالث: الاختلاف بين الدراسة الحالة والدراسات السابقة

من خلال عرض بعض الدراسات السابقة ذات الصلة بمتغيري القيادة الرقمية وسلوك الأمن السيبراني، والتي أسفرت عن العديد من النتائج والتوصيات التي يمكن أن تثري الدراسة الحالية، سيتم في هذا المطلب تناول أوجه التشابه ونقاط الاتفاق، بالإضافة إلى أوجه الاختلاف والتباين، مع تسليط الضوء على أبرز الجوانب المستفادة من هذه الدراسات.

أولا: أوجه التشابه

تتوافق الدراسة الحالة مع الدراسات السابقة في النقاط التالية:

1-منهج الدراسة:

اتفقت الدراسات السابقة مع الدراسة الحالية في اعتماد الاستبانة كأداة بحثية، كما اعتمدت بعض الدراسات على المنهج الكمي باستخدام نموذج تحليل المسار (Path Analysis) لدراسة العلاقات بين المتغيرات المختلفة بدقة أكبر. بالإضافة إلى ذلك، استعانت بعض الدراسات ببرامج الحزم الإحصائية للعلوم الاجتماعية في تحليل البيانات. وتأتي الدراسة الحالية في سياق مماثل، حيث استخدمت برنامج (SPSS)، إلى جانب هذه المناهج الإحصائية لتعزيز دقة النتائج وتقديم تحليل أعمق للبيانات.

2-بيئة ومجتمع الدراسة:

تتشابه الدراسة الحالية مع الدراسات السابقة في تناولها لبيئة العمل داخل المؤسسات، حيث اهتمت الأبحاث السابقة بدراسة العوامل البيئية والتنظيمية التي تؤثر على السلوكيات الأمنية في مختلف القطاعات. وتنسجم الدراسة الحالية مع هذا التوجه من خلال تسليط الضوء على دور القيادة الرقمية في تعزيز الوعي بسلوك الأمن السيبراني داخل المؤسسات، مع التركيز على القطاع المالي كأحد مجالات التطبيق.

3-الأبعاد:

تشابهت الدراسة الحالية مع إحدى الدراسات السابقة في اعتمادها على عدة أبعاد للقيادة الرقمية، مثل الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، والمشاركة والتعاون، وأبعاد الأمن السيبراني المتمثلة في تأمين الأجهزة، توليد كلمة المرور، الوعي الاستباقي والتحديث الأمنية. حيث تنسجم هذه الدراسة مع النهج السابق من خلال تحليل تأثير هذه الأبعاد في سياق المؤسسات المالية.

ثانيا: أوجه الاختلاف

هناك العديد من أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة من حيث الزمن والمكان، العينة والمتغيرات، والجدول التالي يوضح الاختلافات بين الدراسة الحالية والدراسات السابقة:

الجدول رقم (03): أوجه الاختلاف بين الدراسة الحالة والدراسات السابقة

أوجه الاختلاف	الدراسة الحالية	الدراسة السابقة
الزمان والمكان	تمت الدراسة الحالية سنة 2025 ببنك الجزائر الخارجي BEA –فرع تبسة–	تمت في ولايات أخرى (الجزائر العاصمة، غرداية، البليدة ...)، وفي دول مختلفة (مصر، لبنان، الأردن، الولايات المتحدة الأمريكية، الصين ...)، وفي سنوات مختلفة (2016، 2017، 2021، 2022، 2023، 2024). وهناك من قام بالدراسة في المدارس، الجامعات، المستشفيات.
العينة	23 موظف من بنك الجزائر الخارجي وكالة تبسة –46–	تناولت الدراسات السابقة عينات مختلفة أكبر وأقل أو تساوي عينة الدراسة الحالية.
المتغيرات	اعتمدت الدراسة الحالية دراسة أبعاد القيادة الرقمية ودورها في تعزيز الوعي بسلوك الأمن السيبراني.	اعتمدت الدراسات السابقة دراسة القيادة الرقمية مع متغيرات أخرى ونفس الشيء بالنسبة للأمن السيبراني، ماعدا دراسة واحدة باللغة العربية وكذا باللغة الأجنبية جمعت بين المتغيرين.
هدف الدراسة	هدفت الدراسة الحالية إلى دراسة أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني في المؤسسات المالية على أرض الواقع في بنك الجزائر الخارجي BEA وكالة تبسة –46–.	هدفت الدراسات السابقة إلى دراسة كل متغير من الدراسة الحالية مع متغير آخر، إلا دراسة باللغة العربية التي كانت دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية، ودراسة باللغة الأجنبية كانت دراسة نظرية شملت المتغيرين.

المصدر: من إعداد الطالبين بالاعتماد على الدراسات السابقة.

تمتاز الدراسة الحالية عن الدراسات السابقة بمحاولتها دراسة واقع القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في بيئتنا المحلية، وذلك من خلال تحليل مدى تطبيق القيادة الرقمية في المؤسسات المالية الجزائرية وتأثيرها على التزام الموظفين بسلوكيات الأمن السيبراني. كما تهدف الدراسة إلى استكشاف

الأبعاد المختلفة للقيادة الرقمية وتأثيرها على الوعي بالمخاطر السيبرانية، الامتثال للسياسات الأمنية، والاستجابة الفعالة للتهديدات السيبرانية.

وإجمالًا، استفاد البحث الحالي من الدراسات السابقة في الجوانب التالية:

- ✓ الاستفادة من المصادر العربية والأجنبية التي تناولت موضوع القيادة الرقمية والأمن السيبراني؛
- ✓ المساهمة في بناء الإطار النظري للدراسة من خلال الاطلاع على الأبحاث السابقة؛
- ✓ الرجوع إلى العديد من الكتب والمجلات العلمية والرسائل الأكاديمية ذات الصلة؛
- ✓ تحديد مشكلة الدراسة وصياغة أسئلتها البحثية بناءً على ما تناولته الدراسات السابقة؛
- ✓ تطوير استبيان يتوافق مع أهداف الدراسة، مستفيدًا من أدوات قياس تم استخدامها في أبحاث سابقة؛
- ✓ الاطلاع على الأساليب الإحصائية المستخدمة سابقًا وتحليل مدى ملاءمتها للدراسة الحالية.

يمكن القول من خلال ما تم تقديمه في هذا المبحث أن هذه الدراسة الحالية تساهم في سد فجوة بحثية من خلال تسليط الضوء على أثر القيادة الرقمية في تعزيز الأمن السيبراني داخل المؤسسات المالية الجزائرية.

خلاصة الفصل الأول

لقد تم في هذا الفصل تسليط الضوء على أبرز الأسس النظرية التي يقوم عليها موضوع البحث، والمتمثلة في القيادة الرقمية والأمن السيبراني، حيث تم تناول التأصيل النظري لمفهوم القيادة الرقمية من حيث التعريفات المتعددة التي أثير حولها الجدل نتيجة اختلاف زوايا النظر والاتجاهات الفكرية للباحثين، إضافة إلى استعراض أبرز الخصائص التي تميز هذا النمط القيادي، وأبعاده الأساسية، مع التركيز على أدواره الحيوية داخل المؤسسة .كما تم التطرق إلى أهمية القيادة الرقمية في ظل التحول الرقمي المتسارع، ودورها في رفع كفاءة الأداء وضمان التكيف مع التحديات، خصوصًا في مجال الأمن السيبراني، حيث أصبح القائد الرقمي مطالبًا بأن يجمع بين الرؤية الإستراتيجية، والقدرة على استخدام التكنولوجيا الحديثة في التنبؤ بالمخاطر والتعامل مع التهديدات السيبرانية بمرونة وفعالية.

إضافة إلى ذلك، تم إبراز أهمية الأمن السيبراني باعتباره أحد المرتكزات الأساسية في بيئة الأعمال المعاصرة، ووسيلة ضرورية لضمان استمرارية النشاط المؤسسي وحماية الأصول الرقمية. وقد تم ربط ذلك بدور القيادة الرقمية في توجيه الموظفين نحو تبني سلوكيات أمنية سليمة، وتفعيل ثقافة الوعي السيبراني، من خلال التدريب والتواصل الفعّال وتطبيق استراتيجيات الحماية الحديثة .وتبيّن من خلال هذا الفصل أن العلاقة بين القيادة الرقمية والأمن السيبراني تمثل توجهًا استراتيجيًا في المؤسسات الاقتصادية، لما له من أثر مباشر في تقوية منظومة الحماية الرقمية، وتحقيق التوازن بين التطور التكنولوجي ومتطلبات الأمان المعلوماتي.

وفي هذا السياق، سيتم في الفصل الموالي تناول هذه العلاقة من منظور تطبيقي، من خلال دراسة ميدانية على مستوى بنك الجزائر الخارجي (BEA) وكالة تبسة-46-، باعتباره نموذجًا لمؤسسة مالية تسعى إلى مواءمة التحول الرقمي مع متطلبات الأمن السيبراني.

الفصل الثاني: الدراسة الميدانية للقيادة الرقمية وأثرها على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-

تمهيد:

بعد تناول الجوانب النظرية المتعلقة بالموضوع، وتحليل المتغير المستقل المتمثل في القيادة الرقمية بأبعادها المختلفة، وكذلك المتغير التابع المتمثل في سلوك الأمن السيبراني، وسعيا لفهم طبيعة العلاقة بينهما، يركز هذا الفصل على التطبيق العملي في بيئة بنك الجزائر الخارجيBEA وكالة تبسة -46-.

ويهدف هذا الجزء إلى الإجابة عن إشكالية الدراسة واختبار فرضياتها من خلال استعراض واقع القيادة الرقمية ومستوى الوعي بالأمن السيبراني في البنك محل الدراسة، ويتضمن ذلك تحديد مجتمع وعينة الدراسة، ووصف أدوات جمع البيانات، خاصة الاستبانة، من حيث إعدادها وخصائصها المتعلقة بالصدق والثبات ، كما يعرض هذا الفصل الإجراءات المعتمدة في اختيار الأدوات الإحصائية وتطبيقها، إلى جانب الأساليب الإحصائية المستخدمة في تحليل البيانات وتفسيرها، واختبار الفرضيات باستخدام الأدوات المناسبة. وبناء على ذلك، تم تقسيم فصل الدراسة الميدانية إلى مبحثين على النحو الموالي:

المبحث الأول: الإطار المنهجي للدراسة الميدانية؛

المبحث الثاني: تحليل نتائج الدراسة واختبار الفرضيات.

المبحث الأول: الإطار المنهجي للدراسة الميدانية

يعد الإطار المنهجي من العناصر الأساسية في أي دراسة علمية، كونه يحدد الأسس التي تنطلق منها عملية البحث، ويساهم في تنظيم الإجراءات التي يتم إتباعها لتحقيق أهداف الدراسة ، ويشمل هذا الإطار تحديد نوع المنهج المستخدم، وأدوات جمع البيانات، ومجتمع الدراسة وعينتها، إلى جانب الأساليب الإحصائية المعتمدة في تحليل البيانات واختبار الفرضيات ، وفي هذا السياق، يتناول هذا المبحث الإطار المنهجي للدراسة الميدانية من خلال توضيح مختلف الجوانب المنهجية التي تم اعتمادها، وذلك بهدف ضمان الدقة والموضوعية في معالجة الإشكالية المطروحة والوصول إلى نتائج علمية موثوقة وقابلة للتعميم ، والتي من خلالها سيتم الحكم على أثر القيادة الرقمية في تعزيز الأمن السيبراني في البنك محل الدراسة، وهذا ما سيتم توضيحه من خلال المطالب التالية:

المطلب الأول: إجراءات الدراسة الميدانية؛

المطلب الثاني: الأدوات المستخدمة في جمع البيانات؛

المطلب الثالث: صدق وثبات أداة الدراسة.

المطلب الأول: إجراءات الدراسة الميدانية

تعد الدراسة الميدانية أحد الأركان الأساسية في البحث العلمي، إذ تمكن الباحث من جمع بيانات واقعية ومباشرة من مصادرها الأصلية، مما يسهم في فهم الظاهرة قيد الدراسة وتحليلها بدقة وموضوعية. وفي هذا الإطار، تم تصميم إجراءات الدراسة الميدانية بعناية لتتناسب مع أهداف البحث وأسئلته، مع مراعاة اختيار الأدوات المناسبة لجمع البيانات وتحديد العينة المستهدفة بدقة، كما تم الحرص على تنظيم عملية جمع البيانات وفق خطوات منهجية تضمن الموثوقية والصدق في النتائج، بما يدعم تحقيق أهداف الدراسة ويعزز من مصداقيتها العلمية.

أولا: مجتمع الدراسة

يتمثل مجتمع الدراسة في موظفي البنك محل الدراسة، وذلك لسنة 2025، حيث يقدر عددهم ب 27 موظفا.[1] ونظرا لصغر حجم مجتمع الدراسة، تم دراسة المجتمع ككل أي المسح الشامل.

ثانيا: عينة الدراسة

تتمثل عينة الدراسة التطبيقية في الموظفين العاملين في البنك محل الدراسة ، من مختلف الوظائف الإدارية حيث يبلغ عدد العينة (23) فردا، وقد تم اختيار هذه العينة بطريقة عشوائية وهي الأنسب في حالة وجود تجانس بين أفراد المجتمع، وعدم وجود فروقات ذات دلالة إحصائية بين المستجوبين.

وقد شكلت عينة الدراسة من نسبته 85.19%من مجتمع الدراسة، ويمكن توضيح عدد الاستبيانات الموزعة وتلك التي لم يتم استرجاعها أو المستبعدة من خلال الجدول التالي:

الجدول رقم (04): عينة الدراسة

الاستبيانات	العدد	النسبة (%)
الموزعة	27	100
التي لم يتم استرجاعها	03	11.11
الغير صالحة للتحليل	01	3.70
الصالحة للتحليل	23	85.19

المصدر: من إعداد الطالبين بناء على نتائج الاستبيان

[1]- معلومات مقدمة من بنك الجزائر الخارجي BEA وكالة تبسة-46-.

يلاحظ من الجدول رقم (03) أعلاه أنه تم توزيع 27 استبيان بما يوافق حجم عينة الدراسة، حيث تم استرجاع وتحليل 23 استمارة بنسبة 85.19%من مجموع الاستبيانات الموزعة، وهي نسبة مقبولة لأغراض البحث العلمي.

ثالثا: منهج الدراسة

يمثل اختيار المنهج العلمي خطوة جوهرية في بناء البحث، إذ يحدد الإطار الذي من خلاله تجمع البيانات وتحلل للوصول إلى نتائج دقيقة وموثوقة، وبما أن طبيعة المشكلة البحثية وأهداف الدراسة تتطلب فهما عميقا وتحليلا منهجيا، فقد تم اعتماد منهج دراسة الحالة نظرا لملاءمته لطبيعة الموضوع وقدرته على تحقيق أهداف الدراسة، ويعتمد هذا المنهج على طرق وأدوات جمع البيانات مثل الاستبيان ، كما يعتمد على المنهج التحليلي كأدا ة داعمة لتحليل البيانات المستخلصة من الاستبيا ن، مما يمكن من دراسة الظاهرة بموضوعية واستنباط النتائج بناء على بيانات ميدانية دقيقة.

رابعا: نموذج الدراسة ومصادر جمع البيانات

1 نموذج الدراسة:

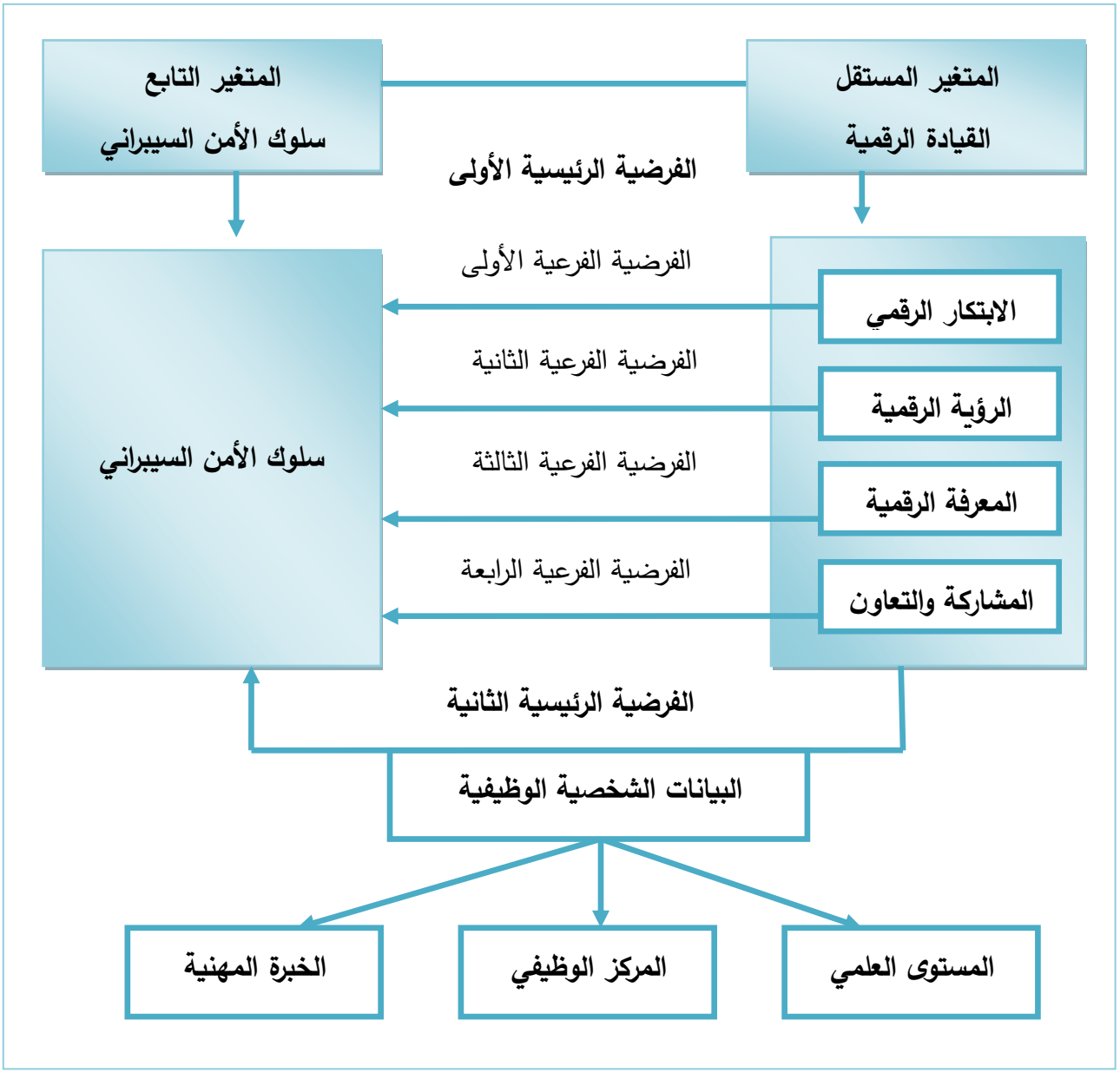
تتناول الدراسة في جانبها النظري البحث في أثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني، وبالتالي فهي تشتمل على المتغيرات التالية:

-**المتغير المستقل:** القيادة الرقمية (الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون)؛

-**المتغير التابع:** سلوك الأمن السيبراني.

ويمكن عرض مختلف تلك المتغيرات بيانيا من خلال الشكل التالي:

الشكل رقم (04): نموذج الدراسة



المصدر: من إعداد الطالبين بالاعتماد على الإطار النظري للدراسة.

وبالتالي يشمل نموذج الدراسة على متغير مستقل (القيادة الرقمية) تم الاعتماد في قياسه على أبعاد القيادة الرقمية والمتمثلة في (الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون)، وشمل متغير أيضا تابع (سلوك الأمن السيبراني)، كما تم الاعتماد على متغيرات المراقبة والمتمثلة في (المستوى العلمي، المركز الوظيفي، الخبرة المهنية) لقياس ومعرفة العلاقة بين متغيري الدراسة وذلك من خلال الإجراءات الموضوعة بغية الوصول إلى نتائج دقيقة.

2 مصادر جمع البيانات:

اعتمدت هذه الدراسة على نوعين من المصادر، هما:

2-1-المصادر الثانوية:

وتشمل المصادر النظرية المستقاة من الكتب، الدراسات السابقة، الملتقيات العلمية، الرسائل الجامعية، إضافة إلى بعض المراجع الأجنبية ذات الصلة بموضوع الدراسة. وقد استُخدمت هذه المصادر لتغطية الجانب النظري الذي يُعدّ أساسياً في دعم وتحليل نتائج الدراسات الميدانية.

2-2-المصادر الأولية:

تُعد المصادر الأولية المحور الأساسي في الجانب التطبيقي للدراسة، وتم جمعها باستخدام الأداتين التاليتين:

- **الاستبيان:** صُمم الاستبيان لجمع المعلومات المتعلقة بموضوع الدراسة، خاصة فيما يتعلق بتأثير القيادة الرقمية على سلوك الأمن السيبراني في البنك محل الدراسة . وقد تم تطويره بطريقة تسهّل جمع المعطيات ومعالجتها إحصائياً بهدف الوصول إلى نتائج دقيقة وموثوقة؛
- **المقابلة:** استُخدمت المقابلة كأداة مكملة لدعم نتائج الاستبيان، من خلال الحصول على معلومات نوعية تُعزز فهم أعمق لموضوع الدراسة وتعطي مصداقية أكبر للبيانات المحصّلة.

تم إجراء مقابلة واحدة مع موظف إطار وكالة بنك الجزائر الخارجي بتبسة، وقد كان الأسلوب شفهيًا، باستخدام أسئلة شبه موجهة، حيث تم إعداد مجموعة من المحاور مسبقًا مع ترك المجال للمستجوَب للإجابة بحرية وتفصيل، من أجل الحصول على رؤى معمقة حول ممارسات القيادة الرقمية وأثرها على سلوكيات الأمن السيبراني داخل الوكالة .تم تحليل محتوى المقابلة باستخدام التحليل النوعي للمحتوى، مع تصنيف الإجابات حسب محاور الدراسة، مما ساعد على استخراج مؤشرات مهمة دعّمت نتائج الدراسة الكمية وساهمت في تفسيرها بشكل أعمق[1].

خلاصة القول، تمثل مجتمع الدراسة في مجموعة من موظفي بنك الجزائر الخارجي بولاية تبسة، حيث تم توزيع 27 استبيان على الأفراد باستخدام أسلوب العينة العشوائية البسيطة. وقد تم دعم عملية جمع البيانات بالمقابلة لتعزيز دقة المعلومات وتحقيق شمولية في المعطيات المتعلقة بمتغيرات الدراسة، والمتمثلة في القيادة الرقمية وسلوك الأمن السيبراني. وتجدر الإشارة إلى أن المطلب الموالي سيعرض الأدوات المعتمدة في جمع البيانات وتحليلها ضمن إطار الدراسة الميدانية.

[1]-أنظر الملحق رقم (03)، ص ص. 115- 116

المطلب الثاني: الأدوات المستخدمة في جمع البيانات

لغرض إتمام عمليات البحث تم الاستعانة بالوسائل اللازمة والمناسبة لكل مرحلة من مراحل البحث، والمتمثلة في السجلات والوثائق التي تم تسّلمها من قبل البنك محل الدراسة، والتي ساعدت على توفير بعض المعلومات المتعلقة بها ومنها تلك التي توضح الجانب التاريخي والتنظيمي للمؤسسة وعلاقتها بالمحيط الاقتصادي.

أولا: وسائل جمع المعلومات

تعد أداة الدراسة الوسيلة التي يعتمد عليها الباحث في جمع بياناته، ولا يوجد تصنيف موحد لهذه الأدوات، إذ يعتمد اختيار الأداة المناسبة على طبيعة فرضية الدراسة ، لذلك ينبغي على الباحث الإلمام بمجموعة متنوعة من الأساليب والأدوات البحثية المختلفة، ليتمكن من معالجة مشكلة البحث والتحقق من صحة الفرضية، وقد يستخدم الباحث أكثر من أداة في دراسته. ويُعد اختيار العينة المراد دراستها من أولى الخطوات التي يجب اتخاذها، ثم يحدد الباحث الوسيلة الأنسب للتحقق من فرضيته، كما قد تتطلب طبيعة البحث استخدام أكثر من أداة في الوقت ذاته.

- **الاستبيان:** هو أداة من أدوات البحث الكمي تستخدم لجمع البيانات والمعلومات من عينة الدراسة بطريقة منهجية، من خلال مجموعة من الأسئلة المكتوبة والمؤسسة مسبقا، يطلب من المبحوثين الإجابة عنها بشكل مباشر، سواء باستخدام خيارات مغلقة أو أسئلة مفتوحة. يعد الاستبيان من أكثر الأدوات استخداما في الدراسات الاجتماعية والاقتصادية، نظرا لقدرته على الوصول إلى عدد كبير من المشاركين في وقت قصير وبتكلفة منخفضة.[1]

وبالنسبة للاستبيان المستخدم في هذه الدراسة فقد تم إعداده على عدة مراحل استنادا إلى ال جانب النظري للدراسة وبما يتلاءم مع نموذج وفروض الدراسة، وذلك بناء على المراحل التالية:

- مراجعة الأدبيات ذات الصلة بالموضوع وتحرير العبارات منها؛
- إعداد استمارة أولية من أجل استخدامها في جمع البيانات والمعلومات؛
- عرض الاستمارة الأولية على مجموعة من الأساتذة المحكمين؛
- ضبط النموذج النهائي من الاستمارة بناء على ملاحظات المحكمين رفقة الأستاذة المشرفة.

حيث اشتمل الاستبيان على محورين أساسيين، وفيمايلي وصف لهما:

[1]-ذوقان عبيدات، عبد الرحمن عدس، محمد عبد الحق ، **البحث العلمي: مفهومه، أدواته، وأساليبه**، ط3،دار الفكر للنشر والتوزيع، عمان، 1998، ص. 305

- ✓ **المحور الأول:** ويشتمل على متغيرات الدراسة الديمغرافية والمتمثلة في كل من (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)؛
- ✓ **المحور الثاني:** ويتضمن أسئلة الدراسة التي يقدر عددها بـ 34 سؤال تم تقسيمه إلى جزأين أساسيين يعكسان القضايا الأساسية التي تناولتها الدراسة، ويوضح الجدول الموالي متغيرات الدراسة والفقرات التي تقيس كل متغير.

الجدول رقم (05): توزيع أسئلة استمارة الاستبيان على أجزاء الدراسة

أجزاء الدراسة	مضمون الأجزاء	عدد الفقرات	
القيادة الرقمية	الابتكار الرقمي	05	20
	الرؤية الرقمية	05	
	المعرفة الرقمية	05	
	المشاركة والتعاون	05	
سلوك الأمن السيبراني		14	
إجمالي الفقرات		34	

المصدر:من إعداد الطالبين بناء على الاستبيان.

كما تم تحديد طول خلايا مقياس لكارت (LikertScale) الخماسي والذي يتضمن خمسة مقاييس هي : (موافق جدا بدرجة **5**، موافق بدرجة **4**، محايد بدرجة **3**، غير موافق بدرجة **2**، غير موافق جدا بدرجة **1**)، وقد تم اختيار هذا المقياس لكونه يسمح للمجيب أن يحدد مستوى تطبيق المتغيرات المدروسة وفق ما يراه، خاصة وأن طبيعة العبارات تتطلب الإجابة بدرجات مختلفة، حيث تم حساب المدى (5-1=4) ومن ثم تقسيمه على أكبر قيمة في المقياس للحصول على طول الخلية أي (4/5=0.80)، وبعد ذلك تم إضافة هذه القيمة إلى بداية المقياس وهي واحد وذلك لتحديد الحد الأعلى لهذه الخلية ويمكن توضيح طول الخلايا في الجدول الموالي:

الجدول رقم (06): طول خلايا مقياس ليكارت الخماسي

المتوسط المرجح	[1.79-1]	[2.59-1.8]	[3.39-2.60]	[4.19-3.4]	[5-4.20]
اتجاه الإجابة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
المستوى	منخفض جدا	منخفض	متوسط	مرتفع	مرتفع جدا

المصدر: الهادي بوقلقول، **تحليل البيانات باستخدام SPSS**، ندوة علمية، جامعة باجي مختار، عنابة، 2013، ص. 24

بالنسبة لطريقة جمع المعلومات في هذه الدراسة كانت عن طريق الاعتماد على الاستمارة، حيث تم استخدام أسلوب التوزيع والجمع المباشر، إذ أن العامل حصل على الاستمارة في الصباح وتم جمعها في نهاية اليوم، وقد تم توزيع27 استمارة لكن تم الاعتماد في عملية التحليل على 23 استمارة فقط، أما الباقي فمنها ما لم تسترجع أو غير صالحة للتحليل.

المطلب الثالث: صدق وثبات أداة الدراسة

يشير صدق أداة الدراسة إلى مدى قدرة الأداة على قياس ما وضعت لقياسه فعليا، أي أن تكون نتائجها معبرة بدقة عن الظاهرة أو المفهوم الذي تستهدف دراسته،وشمولها لكل العناصر التي يجب أن تدخل في التحليل من ناحية ووضوح فقراتها ومفرداتها من ناحية أخرى، ويعد الصدق من أهم معايير الحكم على جودة الأداة وعلى قياس المتغيرات التي وصفت لقياسها ، إذ أن الأداة غير الصادقة لا يمكن الوثوق بنتائجها حتى وإن كانت ثابتة.

أولا: صدق أداة الدراسة

تم التأكد من صدق أداة الدراسة من خلال عرضها على محكمين من أساتذة مختصين في كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، تخصص إدارة أعمال-جامعة تبسة- [1]، وفي ضوء الملاحظات تم تعديل الاستمارة وذلك رفقة الأستاذة المشرفة للحصول على النسخة النهائية للاستبيان.[2]

كما تم التحقق من صدق أداة الدراسة (الاستبيان) من خلال حساب معامل "بيرسون"، ويمكن توضيح ذلك من خلال الجدول التالي: [3]

الجدول رقم (07): قيمة معامل الصدق لمتغيرات الدراسة التابعة والمستقلة

رقم العبارة	متغيرات الدراسة		معامل الصدق بيرسون (%)
العبارات من 01 إلى 05	القيادة الرقمية	• الابتكار الرقمي	0.854
العبارات من 06 إلى 10		• الرؤية الرقمية	0.908
العبارات من 11 إلى 15		• المعرفة الرقمية	0.762
العبارات من 16 إلى 20		• المشاركة والتعاون	0.859
العبارات من 01 إلى 20	القيادة الرقمية		0.938
العبارات من 21إلى 34	سلوك الأمن السيبراني		0.959

المصدر:من إعداد الطالبين بناء على مخرجات برنامج التحليل الإحصائي Spss.

يتضح من الجدول أن معاملات الصدق لبيرسون لجميع الأبعاد كانت موجبة ودالة إحصائيا ، حيث يشير التحليل الإحصائي لمعاملات الصدق (بيرسون) إلى تمتع أد اة القياس (الاستبيان) بدرجة عالية من

[1]-أنظر الملحق رقم (01)، ص. 108

[2]-أنظر الملحق رقم (02)، ص ص. 109- 114

[3]-أنظر الملحق رقم (04)، ص. 120

الصدق البنائي، حيث تراوحت معاملات الارتباط بين أبعاد المتغيرات الرئيسة وقيمها الكلية ما بين (0.762) و(0.959). وقد حققت أبعاد متغير القيادة الرقمية صدقًا متفاوتًا، إذ كان أدنى ارتباط في بعد "ا لمعرفة الرقمية" (0.762)، مما يشير إلى صدق مقبول، بينما سجل بعد " الرؤية الرقمية" أعلى ارتباط (0.908)، بما يعكس قوة العلاقة بين العبارات الخاصة بمتغير القيادة الرقمية، كما بلغ معامل الصدق الكلي لمتغير القيادة الرقمية (0.938)، مما يدل على تماسك مرتفع بين أبعاده المختلفة. وبالمثل، أظهر متغير سلوك الأمن السيبراني ارتباطا قويا (0.959)، ما يعزز من صلاحية الأداة لقياس المتغيرات قيد الدراسة بدقة وموثوقية، ويدعم إمكانية استخدامها في لقياس ما صممت من أجله.

كما أنه قبل أن تطرح استمارة الاستبيان في شكلها النهائي مرت بعدة مراحل لاختبار صدقها وثباتها من أجل تنفيذ الدراسة، ومن أجل التحقق من صدق الأداة والتأكد من مدى صلاحيتها للقياس، تم الاعتماد على الصدق الظاهري لعدد من المحكمين والأساتذة وأصحاب الخبرة والتخصص، وقد تمت دراسة ملاحظات المحكمين واقتراحاتهم بعناية لإجراء التعديلات المطلوبة لتصبح الاستبانة أكثر فهما ووضوحا وتحقيقا لأهداف البحث، لتوزيعها على العينة المدروسة.[1]

ثانيا: ثبات أداة الدراسة

تم توزيع عدد من استمارات الاستبيان وعددها 27 على مجتمع الدراسة لتأكد من ثباتها طبقا لمعامل الثبات ألفا كرونباخ (AlphaCronbach's)[2]، للاتساق الداخلي لمتغيرات الدراسة التابعة والمستقلة[3]، وكانت النتائج كما هي موضحة في الجدول التالي:

[1]-أنظر الملحق رقم (01)، ص. 108

[2]-**ألفا كرونباخ:** "هو اختبار لفحص مدى انسجام أسئلة المحور فيما بينها وكذا مدى انسجام محاور الدراسة مجتمعة وعليه فهو يحدد مدى اعتمادية استمارة الاستبيان للدراسة وقدرتها على إعطاء بيانات وقياسات مستقرة نوعا ما وغير متباينة، فكلما كانت قيمة معامل" ألفا كرونباخ " أعلى تكون أداة القياس (استمارة) أفضل وتتراوح قيمة المعامل بين0 و1 ويعتبر الحد الأدنى المقبول لهذا المعامل هو 60% (أنظر محمود مهدي العتبي، **تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي SPSS**، دار حامد، الأردن، 2005، ص: 49).

[3]-أنظر الملحق رقم (04)، ص ص. 120- 121

الجدول رقم (08): قيمة معامل الثبات للاتساق الداخلي لمتغيرات الدراسة التابعة والمستقلة

رقم العبارة	متغيرات الدراسة	معامل الثبات ألفا كرونباخ
العبارات من 01 إلى 05	الابتكار الرقمي	0.565
العبارات من 06 إلى 10	الرؤية الرقمية	0.746
العبارات من 11 إلى 15	المعرفة الرقمية	0.755
العبارات من 16 إلى 20	المشاركة والتعاون	0.857
العبارات من 01 إلى 20	القيادة الرقمية	0.905
العبارات من 21 إلى 34	سلوك الأمن السيبراني	0.896
العبارات من 01 إلى 34	الاستبيان ككل	0.943

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يوضح التحليل الإحصائي لمعاملات الثبات (ألفا كرونباخ) أن أداة القياس تتمتع بدرجات متفاوتة من الثبات، حيث تشير النتائج إلى أن قيم معامل الثبات (ألفا كرونباخ) تراوحت بين (0.565) و(0.943). وقد سجّل بُعد "الابتكار الرقمي" أدنى قيمة بثبات قدره (α = 0.565)، وهي قيمة تقع دون الحد المقبول علميًا (0.70)، مما يشير إلى قصور في هذا البُعد، والذي قد يعود إلى ضعف في صياغة بعض الفقرات أو إلى تباين تقديرات أفراد العينة . في المقابل، أظهرت بقية أبعاد "القيادة الرقمية" ثباتًا مقبولًا إلى مرتفع؛ حيث بلغ معامل الثبات لبُعد "الرؤية الرقمية" (0.746)، و"المعرفة الرقمية" (0.755)، وهما يقعان ضمن المستوى الجيد من الثبات. كما حقق بُعد "المشاركة والتعاون" أعلى ثبات (0.857)، ليكون الأكثر اتساقًا بين أبعاد القيادة الرقمية .أما الثبات الكلي لمتغير "القيادة الرقمية" فقد بلغ (0.905)، مما يعكس درجة عالية من التماسك الداخلي بين أبعاده. من جهة أخرى، سجل متغير "سلوك الأمن السيبراني" ثباتًا مرتفعًا (0.896)، في حين أظهر الاستبيان ككل أعلى مستوى للثبات بواقع (0.943)، حيث تشير هذه النتائج على أن الأداة البحثية المعتمدة تتمتع بدرجة عالية من الموثوقية ويمكن الاعتماد عليها في قياس المتغيرات محل الدراسة بدقة وفعالية.

ثالثا: أدوات التحليل الإحصائي

لتحقيق أهداف الدارسة والتحليل البيانات سيتم الاعتماد على طرق إحصائية يتم من خلالها وصف المتغيرات وتحديد نوعية العلاقة الموجودة بينها، بداية بجمع البيانات الموزعة وترميزها ثم إدخال البيانات الموزعة وترميزها بالحاسوب الآلي باستعمال برنامج الحزمة الإحصائية الاجتماعية "SPSS" في إصداره الخامس والعشرين، حيث تضمنت المعالجة الأساليب الإحصائية الموالية.

1-التكرارات والنسب المئوية: حيث استخدمت في وصف خصائص مجتمع الدراسة، ولتحديد الاستجابة اتجاه محاور أداة الدراسة وتحسب بالقانون الموالي:

$$\text{النسبة المئوية} = \frac{\text{تكرارات المجموعة} \times 100}{\text{المجموع الكلي للتكرارات}}$$

2-معامل ألفا كرونباخ (AlphaCronbach's): تم استخدامه لتحديد معامل ثبات أداة الدراسة، ويعبر عنه بالمعادلة الموالية :

$$a = \frac{n}{n-1}\left(1 - \frac{\sum vi}{vt}\right)$$

حيث:

a: يمثل ألفا كرونباخ؛

n: .يمثل عدد الأسئلة؛

Vt: يمثل التباين في مجموع المحاور للاستمارة؛

Vi: يمثل التباين لأسئلة المحاور.

3-المتوسط الحسابي والانحراف المعياري: يتم حسابهما لتحديد استجابات أفراد الدراسة نحو محاور وأسئلة أداة الدارسة، حيث أن الانحراف المعياري عبارة عن مؤشر إحصائي يقيس مدى التشتت في التغيرات ويعبر عنه بالعلاقة الموالية:

$$X = \sum_{N}^{n} Xi$$

حيث:

X:يمثل المتوسط الحسابي؛

Xi:يمثل قيمة الأسئلة؛

N: يمثل عدد الأسئلة.

$$\delta = \frac{\sqrt{\sum(xi - x)2}}{N}$$

حيث:

δ: يمثل الانحراف المعياري؛

Xi: يمثل قيمة الأسئلة؛

X: يمثل المتوسط الحسابي.

4-معامل ارتباط بيرسون: يستخدم معامل الارتباط "بيرسون" لتحديد مدى ارتباط متغيرات الدراسة ببعضها، وتم حسابه انطلاقا من برنامج الحزمة الإحصائية الاجتماعية SPSS ،ويعبر عنه بالعلاقة التالية:

$$r_{xy} = \frac{\sum(xi-x)(y1-\bar{y})}{(n-1)sxsy}$$

حيث:

n: عدد المشاهدات؛

xi: قيم المتغير الأول؛

yi: قيم المتغير الثاني؛

sx: الانحراف المعياري للمتغير الأول؛

Sy: الانحراف المعياري للمتغير الثاني.

5-اختبار التوزيع الطبيعي (Smirnov-Sample Kolmogrov): أستخدم لمعرفة نوع البيانات هل تتبع التوزيع الطبيعي أم لا، لأن إجراء بعض الاختبارات الإحصائية يتطلب أن يكون توزيع البيانات يتبع التوزيع الطبيعي.

6-اختبارt للعينات المستقلة (T-Test Independent-Samples): أستخدم لاختبار الفرضيات المتعلقة بمدى وجود فروق ذات دلالة إحصائية بين أفراد العينة ترتبط بالخصائص الوظيفية.

7-تحليل التباين الأحادي (ANOVA One Wa): أستخدم لاختبار الفرضيات المتعلقة بمدى وجود فروقات ذات دلالة إحصائية ترتبط بالخصائص والوظيفية التي تحتوي على أكثر من مجموعتين، وتتمثل في هذه الدارسة العمر والمستوى التعليمي والصنف المهني وعدد سنوات الخدمة.

8-الانحدار الخطي البسيط (Analysis Simple Regression): يتعلق تحليل الانحدار بالتنبؤ بالمستقبل غير معروف اعتمادا على بيانات جمعت عن الماضي المعروف، فهو يحلل احد المتغيرا ت المتغير التابع متأثرا بعامل أخر أو أكثر من عامل مستقل [1] ، وقد تم استخدام تحليل الانحدار الخطي البسيط لاختبار أثر الاستغراق الوظيفي على أداء العاملين .

تغيير الكلمة في مجمل التعليقات اعتمدت هذه الدراسة على استخدام مجموعة من البرامج الإحصائية، من بينها برنامج Microsoft Excel 2013،وبرنامج الحزمة الإحصائية للعلوم الاجتماعية Spss (الإصدار25)، بالإضافة إلى مجموعة من الأدوات الإحصائية شملت التكرارات، النسب المئوية، معامل ألفا كرونباخ، اختبار T للعينات المستقلة، المتوسط الحسابي، الانحراف المعياري، ومعامل الارتباط بيرسون .

أما بالنسبة لمجتمع الدراسة، فقد تمثل في كل موظفي البنك محل الدراسة . وتم جمع البيانات باستخدام أدا تي الاستبانة والمقابلة ، حيث تضمن الاستبيان 34 عبارة موزعة على جزأين، تم بناؤه وفق مقياس ليكرت الخماسي، وتم التأكد من صدق وثبات أداة الدراسة من خلال معامل ألفا كرونباخ ، وقد تم إدخال وتحليل البيانات باستخدام برنامجي SPSS وExcel، مع الاعتماد على الأدوات الإحصائية المذكورة لتحليل نتائج الاستبيان واختبار الفرضيات، التي سيتم تناولها بالتفصيل في المبحث الموالي.

[1]- خالد محمد السواعي، **مدخل إلى تحليل البيانات باستخدام SPSS**، ط1 ،عالم الكتب الحديث، 2011، ص. 195

المبحث الثاني: تحليل نتائج الدراسة واختبار الفرضيات

اعتمدت هذه الدراسة في جانبها التطبيقي على أداة الاستبيان لجمع البيانات المتعلقة بمتغيرات البحث، حيث تم توزيعها على عينة الدراسة وتحليلها باستخدام الأساليب الوصفية والنوعية. يهدف هذا التحليل إلى استخراج نتائج دقيقة وموثوقة يمكن البناء عليها في ضوء أهداف الدراسة. ويُركز هذا المبحث على عرض وتحليل البيانات المتحصّل عليها من الاستبيانات، من أجل قياس مدى تبنّي البنك محل الدراسة لنمط القيادة الرقمية، ومدى إسهام هذا النمط القيادي في تعزيز سلوك الأمن السيبراني داخل البنك . كما يهدف إلى الإجابة عن تساؤلات الدراسة واختبار صحة فرضياتها، مما سبق يمكن تقسيم هذا المبحث إلى المطالب الموالية:

- **المطلب الأول: الوصف الإحصائي لعينة الدراسة؛**
- **المطلب الثاني: عرض وتحليل نتائج الدراسة الميدانية؛**
- **المطلب الثالث: اختبار فرضيات الدراسة.**

المطلب الأول: الوصف الإحصائي لعينة الدراسة

تم توزيع استمارات الاستبيان على عينة الدراسة والتعرف على البيانات الشخصية والوظيفية لعينة الدراسة وفيمايلي تحليل لذلك.

أولا:متغير المستوى العلمي

يوضح الجدول الآتي توزيع أفراد عينة الدراسة من حيث متغير الم ستوى العلمي:

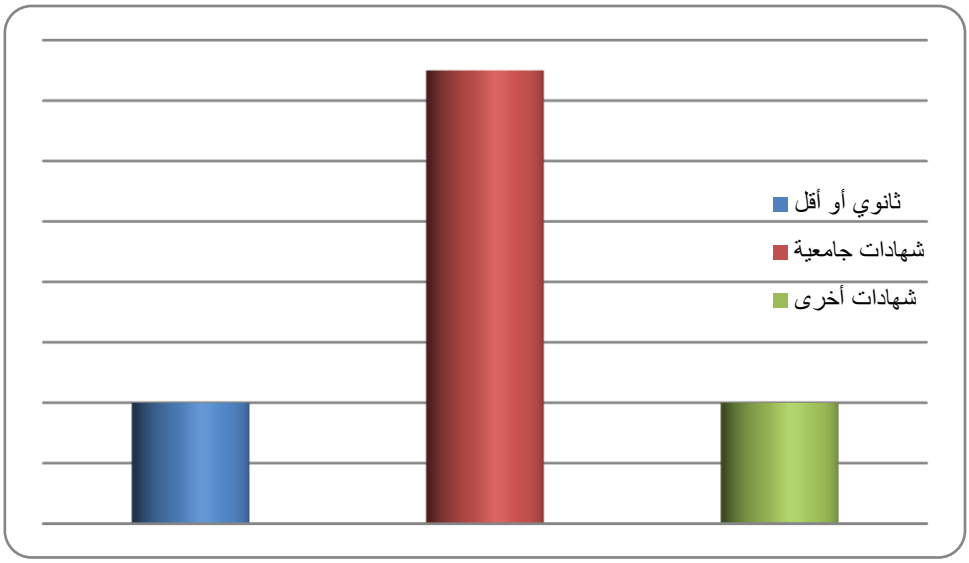
الجدول رقم (09): توزيع عينة الدراسة حسب متغير المستوى العلمي

المستوى العلمي	التكرار	النسبة (%)
ثانوي أو أقل	4	17,4
شهادات جامعية	15	65,2
شهادات أخرى	4	17,4
المجموع	23	100

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

من خلال ما سبق يلاحظ أن نسبة مستوى ال جامعي هي النسبة الأعلى مقارنة بباقي المستويات الأخرى، حيث سجل نسبة قدره ا 65.2% وهذا ما يدل على وجود مستوى مرتفع لعينة الدراسة، وجاءت باقي المستويات متساوية بنسبة 17.4%، كما هو موضح في نتائج الجدول، وما يمكن استخلاصه هنا أن البنك يعتمد على الكفاءات الجامعية في تسيير مختلف شؤونها، وهذا ما يوضحه الشكل التالي:

الشكل رقم (05): توزيع عينة الدراسة حسب متغير المستوى العلمي



المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

وعليه يتبين أن أكثر المستويات التعليمية الموجودة في البنك هو مستوى الجامعي، لهذا يمكن القول أن بنك محل الدراسة يستهدف بصفة أولية في عملية استقطابه للموظفين الجامعيين، وذلك يدل على توفير الجامعة للكفاءات البشرية المطلوبة من قبل البنوك.

ثانيا: متغير المركز الوظيفي

يمثل الجدول التالي توزيع أفراد عينة الدراسة من خلال متغير المركز الوظيفي:

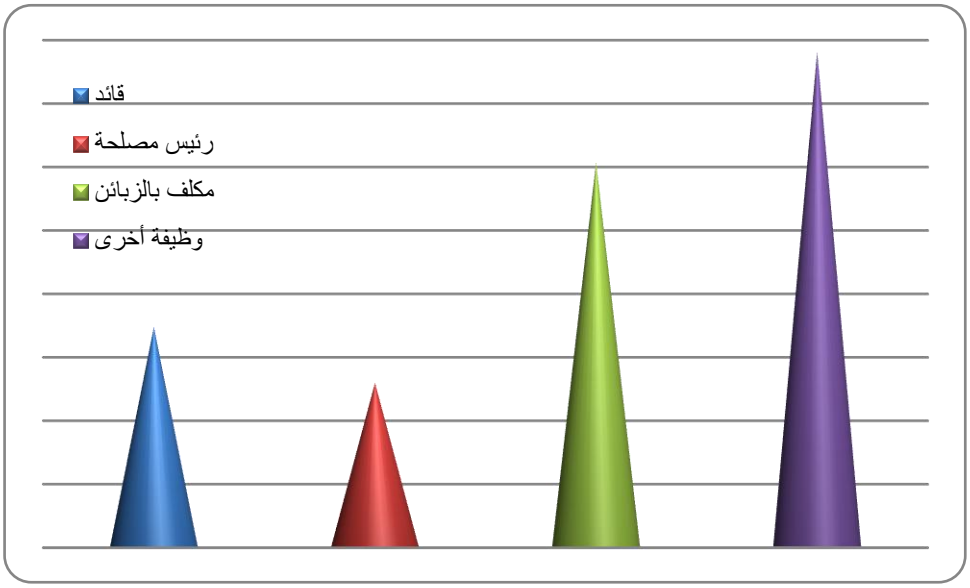
الجدول رقم (10): توزيع عينة الدراسة حسب متغير المركز الوظيفي

المركز الوظيفي	التكرار	النسبة (%)
قائد	4	17,4
رئيس مصلحة	3	13,0
مكلف بالزبائن	7	30,4
وظيفة أخرى	9	39,1
المجموع	23	100

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

في ضوء توزيع أفراد العينة حسب المركز الوظيفي، يتبين أن عينة الدراسة ضمت تمثيلا متنوعا للمناصب داخل البنك محل الدراسة، حيث شكلت فئة "وظائف أخرى" النسبة الأكبر (39.1%)، تليها فئة "مكلف بالزبائن" بنسبة (30.4%)، في حين شكلت فئتا "قائد" و"رئيس مصلحة" نسبًا أقل بلغت (17.4%) و(13.0%) على التوالي ، هذا التوزيع يعكس شمولية نسبية للعينة من حيث تغطية المستويات الوظيفية المختلفة، وهو ما يعزز من مصداقية النتائج وواقعيتها، حيث تم استقصاء آراء المشاركين من مواقع تنفيذية وتشغيلية مختلفة، ويلخص الشكل الموالي أهم هذه المعطيات:

الشكل رقم (06): توزيع عينة الدراسة حسب متغير المركز الوظيفي



المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتضح من الشكل أن أغلب المشاركين يشغلون "وظائف أخرى" بنسبة 39.1%، وهو ما يمثل النسبة الأكبر من العينة المدروسة، مما قد يشير إلى تنوع في المناصب غير المصنفة ضمن الفئات المحددة. يلي ذلك فئة "مكلف بالزبائن" بنسبة 30.4%، ما يعكس تركيزا واضحا على الوظائف التي تتعامل مباشرة مع العملاء. أما فئتا "قائد" و"رئيس مصلحة" فتمثلان نسباً أقل، بـ 17.4% و13.0% على التوالي، مما يدل على قلة تمثيل المناصب الإدارية العليا في العينة.

ثالثا: متغير الخبرة المهنية

يمثل الجدول التالي توزيع أفراد عينة الدراسة من خلال متغير الخبرة المهنية في إطار البنك محل الدراسة:

الجدول رقم (11): توزيع عينة الدراسة حسب متغير الخبرة المهنية

الخبرة المهنية	التكرار	النسبة (%)
أقل من 5 سنوات	6	26,1
من 05 إلى 10 سنوات	6	26,1
من 11 إلى 15 سنة	4	17,4
أكثر من 15 سنة	7	30,4
المجموع	23	100

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

نلاحظ من خلال الجدول أن النسبة الأكثر خبرة هي الأكثر تكرارا، حيث بلغت نسبتها 30,4 %، وهي الفئة " أكثر من 15 سنة"، لتليها الفئة "من 05 إلى 10سنوات " بنسبة 26,1% لتحل المرتبة الثانية وهي الفئة متوسطة الخبرة، ثم لتأتي الفئة " أقل من 5 سنوات" في المرتبة الثالثة بنسبة متساوية مع المرتبة الثانية ب 26,1%، واحتلت الفئة (من 11 إلى 15 سنة) في المرتبة الأخيرة بنسبة قدرت ب 17,4%، وهو ما يفسر وجود خبرة وكفاءات يمكن الاعتماد عليها في تطوير وتحسين أداء البنك محل الدراسة.

والشكل الموالي يوضح توزيع متغير الخبرة المهنية :

الشكل رقم (07): توزيع عينة الدراسة حسب متغير الخبرة المهنية

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

وعليه يتبين أن متغير الخبرة المهنية محقق بنسب معتبرة في البنك ، ومنه يمكن القول أن هذا التوزيع يعكس بيئة عمل صحية تلتئم فيها الخبرة المهنية مع الابتكار المستمر ، بجانب وجود قاعدة عريضة من الكفاءات التي يمكن البناء عليها لضمان استدامة الأداء.

بناءً على ما سبق، يتناول هذا المطلب عرض الوصف الإحصائي لعينة الدراسة، وذلك من خلال تحليل البيانات الشخصية للمبحوثين، والتي تشمل المستوى ال علمي، المركز الوظيفي، الخبرة المهنية، داخل المؤسسة. ويهدف هذا التحليل إلى تكوين صورة واضحة عن خصائص العينة، تمهيداً لعرض نتائج الدراسة في المطلب الموالي.

المطلب الثاني: عرض وتحليل نتائج الدراسة الميدانية؛

يتناول هذا المطلب عرض البيانات الأساسية والتي تمثل اتجاهات إجابات أفراد عينة الدراسة نحو متغير الدراسة الواردة في أداة الدراسة المتمثلة في الاستبيان[1]، وقد تم الاستعانة في ذلك ببرنامج Spss.

أولا: عرض وتحليل نتائج إجابات أفراد العينة نحو متغير القيادة الرقمية

1-نتائج إجابات أفراد عينة الدراسة حول متغير القيادة الرقمية:

1-1-متغير الابتكار الرقمي:

يمثل الجدول التالي إجابات عينة الدراسة حول متغير الابتكار الرقمي، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (12): نتائج إجابات أفراد عينة الدراسة حول متغير الابتكار الرقمي

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	يساهم الابتكار الرقمي في تحسين جودة الخدمات الرقمية التي يقدمها البنك لعملائه؛	4,347	0,486	مرتفع جدا	02
02	تعد التقنيات الحديثة ضرورية لدعم الابتكار الرقمي في القطاع المصرفي؛	4,304	1,019	مرتفع جدا	03
03	تعزز البرمجيات الحديثة قدرة البنك على المنافسة في السوق؛	4,347	0,831	مرتفع جدا	01
04	يسمح البنك للموظفين بتقديم اقتراحات تتعلق بتطوير التقنيات والبرمجيات الحديثة؛	3,695	0,875	مرتفع	05
05	يساعد الابتكار الرقمي البنك على تطوير خدمات وحلول بنكية جديدة تميزه عن البنوك الأخرى؛	3,826	0,834	مرتفع	04
	متغير الابتكار الرقمي	4,021	0,520	مرتفع	-

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتبين من الجدول أعلاه أن متغير الابتكار الرقمي ذو اتجاه مرتفع؛ بمتوسط حسابي قدره (4,021) وانحراف معياري (0.520)، حيث ينتمي المتوسط الحسابي لهذا المتغير في سلم ليكارت الخماسي للمجال [3.40-4.19]، وهو ما يعكس إدراكا إيجابيا لدى موظفي البنك محل الدراسة لأهمية الابتكار الرقمي في تحسين جودة الأداء وتطوير الخدمات، ومنه هذه النتائج تؤكد أن الابتكار الرقمي يمثل ركيزة إستراتيجية لدى

[1]-أنظر الملحق رقم (04)، ص ص. 117- 119

البنك محل الدراسة، ويمكنه من تقديم خدمات متطورة ومنافسة في السوق ، وتم قياس هذا المتغير من خلال (05) عبارات أشارت إلى درجة مرتفعة كالآتي:

- ✓ **العبارة رقم (01):** قدر المتوسط الحسابي للعبارة بـ (4,347) بانحراف معياري قدره (0.486)، وجاءت باتجاه مرتفع جدا، وهذا يدل على إدراك واضح من طرف المبحوثين أن الابتكار الرقمي ليس مجرد تحسين شكلي، بل يترجم مباشرة إلى رفع مستوى جودة الخدمة المقدمة للعملاء؛
- ✓ **العبارة رقم (02):** قدر المتوسط الحسابي للعبارة بـ (4,304) بانحراف معياري قدره (1,019)، وجاءت باتجاه مرتفع جدا،وهذا يؤكد وعي العمال بأن الابتكار الرقمي لا يمكن تحقيقه في معزل عن البنية التحتية التقنية الحديثة، فالتقنيات الحديثة تعد الحاضنة الأساسية التي يبنى عليها الابتكار، سواء من حيث تطوير الأنظمة أو خلق منتجات مالية جديدة، وهذا الاتفاق يعزز أهمية الاستثمار المستمر في التكنولوجيات الحديثة؛
- ✓ **العبارة رقم(03):**قدر المتوسط الحسابي للعبارة بـ (4,347) بانحراف معياري قدره (0.831)، وجاءت باتجاه مرتفع جدا، وهذا يدل أن الابتكار الرقمي يلعب دورا محوريا في الموقع الاستراتيجي للبنك داخل السوق. إذ تتيح البرمجيات الذكية تقديم خدمات أسرع، أكثر دقة وبتكلفة أقل، ما يعطي للبنك ميزة تنافسية فعلية أمام البنوك الأخرى؛
- ✓ **العبارة رقم (04):** قدر المتوسط الحسابي للعبارة بـ (3,695) بانحراف معياري قدره (0,875)، وجاءت باتجاه مرتفع، رغم أن المتوسط لا يزال ضمن المجال المرتفع، إلا أنه الأقل بين العبارات الخمس .هذا يشير إلى وجود نوع من التحفظ أو عدم الرضا التام من طرف الموظفين بخصوص فرص المشاركة التي تمنح لهم في جانب الابتكار ، وقد يفسر ذلك بوجود فجوة في ثقافة الابتكار التشاركي داخل البنك محل الدراسة، ما يستدعي تعزيز سياسات الانفتاح على اقتراحات العاملين، خاصة أولئك الذين يتعاملون مباشرة مع الأنظمة والزبائن؛
- ✓ **العبارة رقم (05):** قدر المتوسط الحسابي للعبارة بـ (3,826) بانحراف معياري قدره (0,834)، وجاءت باتجاه مرتفع،ما يدل على اقتناع جيد بأن الابتكار الرقمي يشكل وسيلة فعالة للتميز السوقي، فالتطوير المستمر للخدمات الرقمية يمكن أن يجعل البنك محل الدراسة يعتبر سباقا في تقديم حلول جديدة.

1-2-متغير الرؤية الرقمية:

يمثل الجدول التالي إجابات عينة الدراسة حول متغير الرؤية الرقمية، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (13): نتائج إجابات أفراد عينة الدراسة حول متغير الرؤية الرقمية

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	يحرص البنك على مواكبة الابتكارات الرقمية لضمان تحقيق رؤيته المستقبلية؛	4,260	0,810	مرتفع جدا	01
02	تلتزم قيادة البنك بتطوير استراتيجيات رقمية تتماشى مع متطلبات السوق البنكي الحديث؛	3,869	0,548	مرتفع	04
03	يحرص قادة البنك على توظيف البيانات وتحليلها رقمياً لدعم اتخاذ القرارات الإستراتيجية؛	3,739	0,864	مرتفع	05
04	يستخدم البنك تقنيات وبرمجيات رقمية حديثة من أجل التكيف مع التحديات الرقمية؛	3,913	1,083	مرتفع	02
05	يركز البنك على تحسين تجربة العملاء من خلال استخدام التقنيات والبرمجيات الرقمية المبتكرة؛	3,869	0,919	مرتفع	03
	متغير الرؤية الرقمية	3,930	0,607	مرتفع	-

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتبين من الجدول أعلاه أن متغير الرؤية الرقمية ذو اتجاه مرتفع؛ بمتوسط حسابي قدره (3,930) وانحراف معياري (0.607)، حيث ينتمي المتوسط الحسابي لهذا المتغير في سلم ليكارت الخماسي للمجال [3.40-4.19]، وهذا يبين على أن للبنك محل الدراسة رؤية رقمية واضحة في نظر المبحوثين، تتجلى في حرصه على مواكبة الابتكارات والتكيف مع المتغيرات الرقمية. ومع ذلك، تشير بعض العبارات إلى أن هذه الرؤية تواجه تحديات في التطبيق العملي، خاصة فيما يخص استخدام البيانات والتحليل الرقمي أو إشراك الموظفين بعمق في صنع القرار الرقمي .وتم قياس هذا المتغير من خلال (05) عبارات أشارت إلى درجة مرتفعة كالآتي:

- ✓ **العبارة رقم (01):** قدر المتوسط الحسابي للعبارة بـ (4,260) بانحراف معياري قدره (0,810)، وجاءت باتجاه مرتفع جدا، وهذا يظهر أن البنك محل الدراسة، لديه توجه واضح نحو المستقبل الرقمي ، هذا يعكس قناعة قوية لدى المشاركين بأن البنك لا يتعامل مع الابتكار الرقمي كرد فعل، بل كمسار استباقي مدروس ينسجم مع رؤيته الإستراتيجية بعيدة المدى؛

- ✓ **العبارة رقم (02):**قدر المتوسط الحسابي للعبارة بـ (3,869) بانحراف معياري قدره (0,548)، وجاءت باتجاه مرتفع،وهذا ما يوضح تشير العبارة إلى أن قيادة البنك هي الجهة المسؤولة عن التوجه الاستراتيجي، مما يعكس دعما مؤسسيا قويا للتحول الرقمي؛
- ✓ **العبارة رقم(03):** قدر المتوسط الحسابي للعبارة ب (3,739) بانحراف معياري قدره (0.864)، وجاءت باتجاه مرتفع، هو أدنى متوسط بين العبارات الخمس، ويعني أن البنك يستخدم البيانات الرقمية في دعمه للقرارات، ولكن هذا الاستخدام قد لا يكون منهجيا أو معمما بعد. وقد يعكس ذلك إما ضعف البنية التحتية التحليلية أو نقص الكفاءات المتخصصة في تحليل البيانات داخل البنك؛
- ✓ **العبارة رقم (04):** قدر المتوسط الحسابي للعبارة بـ (3,913) بانحراف معياري قدره (1,083)، وجاءت باتجاه مرتفع، هذا يشير إلى أن المشاركين يتفقون بشكل جيد على أن البنك يتبنى أدوات وتقنيات رقمية حديثة استجابة للتحولات الرقمية، ولكن المتوسط لا يرقى لمستوى "مرتفع جدًا"، مما يعني وجود مساحة لتطوير وتوسيع نطاق استخدام تلك التقنيات بشكل أكثر تكاملًا؛
- ✓ **العبارة رقم (05):** قدر المتوسط الحسابي للعبارة بـ (3,869) بانحراف معياري قدره (0,919)، وجاءت باتجاه مرتفع، وهذا عكس اتفاقا جيدا على أن البنك يستخدم الأدوات الرقمية لتحسين تفاعل العملاء وخدمتهم، وهي نقطة مهمة في تعزيز الولاء والرضا.

1-3-متغير المعرفة الرقمية:

يمثل الجدول التالي إجابات عينة الدراسة حول متغير المعرفة الرقمية، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (14): نتائج إجابات أفراد عينة الدراسة حول متغير المعرفة الرقمية

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	يستقطب البنك أشخاص بكفاءات عالية متمكنة من استخدام التقنيات والبرمجيات الحديثة؛	4,000	0,797	مرتفع	04
02	توفر قيادة البنك برامج تدريبية لتعزيز المعرفة الرقمية لدى الموظفين؛	4,043	0,928	مرتفع	03
03	يتمتع قادة البنك بالمعرفة الرقمية الكافية لتوجيه عمليات التحول الرقمي بفعالية؛	4,260	0,810	مرتفع جدا	01
04	تحرص قيادة البنك على تطوير مهاراتها الرقمية لمواكبة التطورات في القطاع البنكي؛	3,956	0,928	مرتفع	05
05	يشارك البنك في الملتقيات والندوات التي تهتم بموضوع القيادة الرقمية من أجل مواكبة التطورات البنكية؛	4,217	0,951	مرتفع جدا	02
	متغير المعرفة الرقمية	4,095	0,629	مرتفع	-

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتبين من الجدول أعلاه أن متغير المعرفة الرقمية ذو اتجاه مرتفع؛ بمتوسط حسابي قدره (4.095) وانحراف معياري (0.629)، حيث ينتمي المتوسط الحسابي لهذا المتغير في سلم ليكارت الخماسي للمجال [3.40-4.19]، وهذا يدل على أن البنك محل الدراسة يمتلك أسسا متينة في مجال المعرفة الرقمية، سواء من خلال الكفاءات البشرية المستقطبة، أو من خلال التطوير المستمر لقدرات القيادة والموظفين. ويلاحظ من النتائج أن قادة البنك يحظون بثقة كبيرة فيما يخص كفاءتهم الرقمية، مما يعزز فاعلية توجيه عمليات بناء معرفة رقمية، بينما تشير بعض النتائج إلى إمكانية تعزيز برامج التطوير الذاتي والتدريب الداخلي بشكل أعمق وأكثر استدامة، وتم قياس هذا المتغير من خلال (05) عبارات أشارت إلى درجة مرتفعة كالآتي:

- ✓ **العبارة رقم (01):** قدر المتوسط الحسابي للعبارة بـ (4,000) بانحراف معياري قدره (0,797)، وجاءت باتجاه مرتفع، وهذا يدل على أن البنك محل الدراسة يولي أهمية لجذب الموارد البشرية ذات الكفاءة الرقمية، هذا يعكس توجها استراتيجيا نحو بناء قاعدة بشرية قادرة على التعامل مع متطلبات التحول الرقمي؛
- ✓ **العبارة رقم (02):** قدر المتوسط الحسابي للعبارة بـ (4,043) بانحراف معياري قدره (0,928)، وجاءت باتجاه مرتفع،وهذا يعكس التزاما جيدا من طرف قيادة البنك بتدريب العاملين في مجال المهارات الرقمية،

وهو مؤشر إيجابي على أن البنك لا يكتفي بالاستقطاب، بل يعمل على تأهيل الموظفين الحاليين لمواكبة التغيرات التكنولوجية؛

- ✓ **العبارة رقم(03):** قدر المتوسط الحسابي للعبارة ب (4,260) بانحراف معياري قدره (0.810)،وجاءت باتجاه مرتفع جدا، وهذا يشير إلى ثقة كبيرة من المبحوثين في كفاءة القيادة الرقمية، ويعدّ عنصرا حاسما في نجاح التحول الرقمي ، فالمعرفة القيادية العميقة بمجال التكنولوجيا تمثل المحرك الرئيسي للرؤية الرقمية الفعالة والتطبيق العملي السلس؛
- ✓ **العبارة رقم (04):** قدر المتوسط الحسابي للعبارة بـ (3,956) بانحراف معياري قدره (0,928)، وجاءت باتجاه مرتفع، وهذا يشير إلى وجود مستوى مرتفع من الوعي الذاتي لدى القيادة بضرورة التعلم المستمر، إلا أن هذا المتوسط هو الأقل ضمن العبارة المتعلقة بهذا المحور، مما قد يدل على أن وتيرة تطوير المهارات قد تحتاج إلى تسريع أكثر؛
- ✓ **العبارة رقم (05):** قدر المتوسط الحسابي للعبارة بـ (4,217) بانحراف معياري قدره (0,951)، وجاءت باتجاه مرتفع جدا،وهذا عكس نشاطا خارجيا قويا للبنك في المشهد الرقمي، ويشير إلى أن البنك يسعى لتحديث معرفته باستمرار من خلال المشاركة الفعالة في البيئات التفاعلية والمعرفية، ما يعزز تبادل الخبرات ومواكبة أفضل الممارسات في القيادة الرقمية.

1-4-متغير المشاركة والتعاون:

يمثل الجدول التالي إجابات عينة الدراسة حول متغير المشاركة والتعاون، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (15): نتائج إجابات أفراد عينة الدراسة حول متغير المشاركة والتعاون

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	توفر القيادة الرقمية في البنك قنوات اتصال فعالة لتعزيز تبادل المعارف الرقمية بين أصحاب المصلحة؛	3,913	0,900	مرتفع	04
02	يدعم البنك بيئة عمل تعاونية تعتمد على الأدوات الرقمية لزيادة الإنتاجية وتحسين الأداء ؛	4,043	0,705	مرتفع	02
03	تساهم ثقافة المشاركة الرقمية في تحسين جودة الخدمات البنكية المقدمة للعملاء .	4,130	0,694	مرتفع	01
04	يعمل البنك على تعزيز الشراكات مع المؤسسات التكنولوجية لتطوير حلول رقمية مبتكرة؛	3,782	0,998	مرتفع	05
05	يشجع البنك موظفيه على تبادل الخبرات الرقمية والمساهمة في مبادرات التحول الرقمي.	3,913	1,164	مرتفع	03
	متغير المشاركة و التعاون	3,956	0,726	مرتفع	-

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتبين من الجدول أعلاه أن متغير المشاركة والتعاون ذو اتجاه مرتفع؛ بمتوسط حسابي قدره (3.956) وانحراف معياري (0.726)، حيث ينتمي المتوسط الحسابي لهذا المتغير في سلم ليكارت الخماسي للمجال [3.40-4.19]، وهذا ما يشير إلى أن البنك محل الدراسة يظهر اهتماما واضحا بتعزيز ثقافة التعاون الرقمي الداخلي والخارجي ، كما أن استنادا إلى نتائج العبارات، يتضح أن أقوى الجوانب تتمثل في ترسيخ ثقافة المشاركة وتحسين الخدمات عبر أدوات رقمية، في حين يبقى تعزيز الشراكات مع مؤسسات التكنولوجيا الخارجية أحد المجالات التي يمكن تقويتها مستقبلا، وتم قياس هذا المتغير من خلال (05) عبارات أشارت إلى درجة مرتفعة كالآتي:

- ✓ **العبارة رقم (01):** قدر المتوسط الحسابي للعبارة بـ (3,913) بانحراف معياري قدره (0,900)، وجاءت باتجاه مرتفع، وهذا يدل على أن العبارة بالبنك محل الدراسة يولي أهمية كبيرة لقنوات الاتصال الرقمية ، هذا يدل على وجود بنية تواصلية فعالة تتيح تبادل المعرفة داخل البنك ومع الأطراف الأخرى، وهي نقطة جوهرية لضمان تفعيل العمل الرقمي المشترك؛
- ✓ **العبارة رقم (02):** قدر المتوسط الحسابي للعبارة بـ (4,043) بانحراف معياري قدره (0,705)، وجاءت باتجاه مرتفع،ما يشير إلى نجاح البنك محل الدراسة في ترسيخ بيئة تعتمد على التقنيات التعاونية (مثل

المنصات الرقمية، أدوات العمل الجماعي، نظم الاتصالات الحديثة)، مما يعزز من كفاءة الأداء والإنتاجية؛

- ✓ **العبارة رقم(03):** قدر المتوسط الحسابي للعبارة بـ (4,130) بانحراف معياري قدره (0.694)، وجاءت باتجاه مرتفع جدا، وهذا يدل أن ثقافة المشاركة الرقمية لها أثر إيجابي مباشر على رضا العملاء وجودة الخدمات، يشير ذلك إلى وعي موظفي بنك الجزائر الخارجي BEA وكالة تبسة - 46-بدور التعاون الرقمي في تقديم حلول مصرفية أكثر مرونة وابتكارا؛
- ✓ **العبارة رقم (04):** قدر المتوسط الحسابي للعبارة بـ (3,782) بانحراف معياري قدره (0,998)، وجاءت باتجاه مرتفع، رغم كونه ضمن المجال "المرتفع"، إلا أنه يمثل أدنى متوسط في البعد، مما قد يشير إلى وجود جهود ملموسة لكنها غير كافية من وجهة نظر المبحوثين فيما يخص التعاون الخارجي مع شركاء التكنولوجيا، ويستدعي ذلك تطوير إطار شراكة أوضح وأوسع مع مؤسسات الابتكار الرقمي؛
- ✓ **العبارة رقم (05):** قدر المتوسط الحسابي للعبارة بـ (3,913) بانحراف معياري قدره (1,164)، وجاءت باتجاه مرتفع جدا ،وهذا يدل على وجود اهتمام بتشجيع التبادل المعرفي الداخلي والمبادرات الذاتية لدى الموظفين، هذا النوع من التحفيز يعزز من جاهزية الفريق للتفاعل الإيجابي مع متطلبات التحول الرقمي المستمر.

1-5-ترتيب أبعاد متغير القيادة الرقمية:

يمثل الجدول التالي إجابات عينة الدراسة حول ترتيب أبعاد متغير القيادة الرقمية، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (16): ترتيب أبعاد متغير القيادة الرقمية

الرقم	الأبعاد	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	الابتكار الرقمي	4,104	0,500	مرتفع	01
02	الرؤية الرقمية	3,930	0,607	مرتفع	04
03	المعرفة الرقمية	4,095	0,629	مرتفع	02
04	المشاركة والتعاون	3,956	0,726	مرتفع	03
متغير القيادة الرقمية		4,021	0,520	مرتفع	-

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

من خلال الجدول أعلاه الذي يتناول آراء واتجاهات أفراد العينة فيما يتعلق بالقيادة الرقمية في البنك محل الدراسة، حيث يتضح أن مستوى القيادة الرقمية في البنك جاء بدرجة مرتفعة بمتوسط حسابي كلي بلغ (4,021) وانحراف معياري (0.520)، مما يعكس مستوى جيدا من تفعيل أبعاد القيادة الرقمية في البنك. وقد أظهرت النتائج أن أعلى الأبعاد ترتيبا هو "الابتكار الرقمي" بمتوسط (4.104)، مما يدل على أن البنك يولي أهمية كبيرة لاستخدام التقنيات والبرمجيات الحديثة كأداة إستراتيجية لتطوير الخدمات وتعزيز التميز التنافسي، يليه "المعرفة الرقمية" بمتوسط (4.095)، وهو مؤشر إيجابي على كفاء ة قادة البنك محل الدراسة في توظيف المهارات الرقمية واتخاذ القرارات المرتبطة بالتحول الرقمي. أما بعد "المشاركة والتعاون" فقد سجل متوسطا قدره (3.956)، ويشير إلى وجود بيئة تنظيمية داعمة للتواصل وتبادل الخبرات الرقمية، في حين أن "الرؤية الرقمية" جاء في المرتبة الأخيرة بمتوسط (3.930)، ما قد يعكس حاجة البنك إلى مزيد من الوضوح والتكامل الاستراتيجي في بلورة رؤى رقمية بعيدة المدى.

وبناء على هذه النتائج، يمكن الاستنتاج أن البنك محل الدراسة يمتلك قاعدة صلبة من القدرات القيادية الرقمية، إلا أن تعزيز البعد الاستراتيجي للرؤية الرقمية يعد ضرورة لتحسين فعالية التحول الرقمي وضمان استدامته على المدى الطويل.

ثانيا: عرض وتحليل نتائج إجابات أفراد العينة نحو متغير سلوك الأمن السيبراني

يمثل الجدول التالي إجابات عينة الدراسة حول متغير الأمن السيبراني، من خلال المتوسط الحسابي والانحراف المعياري لكل عبارة كما يوضح الجدول الموالي:

الجدول رقم (17): نتائج إجابات أفراد عينة الدراسة حول متغير الأمن السيبراني

الرقم	العبارات	المتوسط الحسابي	الانحراف المعياري	الاتجاه	الترتيب
01	يمتلك البنك الوعي الكافي بالمخاطر السيبرانية التي قد تهدد أنظمته؛	4,347	0,714	مرتفع جدا	01
02	يتبع البنك إجراءات وقائية فعالة لمواجهة الهجمات السيبرانية؛	4,043	0,877	مرتفع	04
03	يطبق البنك سياسات واضحة ومحدثة للأمن السيبراني؛	3,869	1,057	مرتفع	07
04	يعتمد البنك على آليات رصد وسياسات أمنية فعالة للحد من التهديدات السيبرانية؛	4,087	0,949	مرتفع	03
05	يعتمد البنك تقنيات تشفير معترف بها عالمياً لحماية بيانات العملاء ؛	3,826	1,266	مرتفع	09
06	يتم تطبيق التحقق المزدوج، مثل رموز التحقق لضمان الوصول الأمن إلى الأنظمة البنكية؛	3,869	0,919	مرتفع	08
07	تقلل سياسات الأمان الرقمي، مثل التشفير والمراقبة، من مخاطر الاختراقات وتسريب البيانات؛ مما يعزز ثقة العملاء ؛	4,043	0,767	مرتفع	05
08	تساهم استراتيجيات الأمن السيبراني في تعزيز مكانة البنك في السوق المالية وتحقيق الاستدامة المالية.	3,956	0,824	مرتفع	06
09	تساهم الاستثمارات المستمرة في الأمن السيبراني في تحسين كفاءة العمليات المصرفية وضمان استمراريتها؛	3,652	0,831	مرتفع	11
10	يمثل الانتقال إلى البنية الرقمية تحدياً رئيسياً للبنك بسبب صعوبة تحديث الأنظمة التقليدية لمواكبة التطورات الأمنية؛	4,173	0,650	مرتفع	02
11	يعاني البنك من نقص في الموارد البشرية المؤهلة لتنفيذ استراتيجيات الأمن السيبراني؛	3,434	1,079	مرتفع	13
12	يواجه البنك مشكلة عدم ثقة العملاء وتخوفهم من الهجمات السيبرانية؛	3,434	1,160	مرتفع	12
13	يعاني البنك من مشاكل بسبب ضعف الأنظمة القانونية التي توفرها الدولة في مجال الأمن السيبراني؛	3,304	1,329	متوسط	14
14	يواجه البنك تحدياً في الموازنة بين تعزيز الأمن السيبراني وتسهيل الخدمات الرقمية المقدمة.	3,739	0,915	مرتفع	10
	متغير الأمن السيبراني	3,841	0,634	مرتفع	-

المصدر: من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتبين من الجدول أعلاه أن متغير الأمن السيبراني ذو اتجاه مرتفع؛ بمتوسط حسابي قدره (3.841) وانحراف معياري (0.634) ،حيث ينتمي المتوسط الحسابي لهذا المتغير في سلم ليكارت الخماسي للمجال [3.40-4.19]، وهذا يدل على أن البنك محل الدراسة يدرك جيدا أهمية الأمن السيبراني و يقوم بخطوات معتبرة لتطوير آلياته، وهو ما تعكسه القيم العالية للمتوسطات الحسابية في غالبية العبارات ، ومع ذلك فإن بعض العبارات سجلت متوسطات أقل تعكس تحديات حقيقية، أبرزها نقص الكفاءات، ضعف التشريعات، وثقة العملاء،وتم قياس هذا المتغير من خلال (14) عبارة أشارت إلى درجة مرتفعة كالآتي:

- ✓ **العبارة رقم (01):** قدر المتوسط الحسابي للعبارة بـ (4,347) بانحراف معياري قدره (0.714) باتجاه مرتفع جدا ، ما يشير إلى أن المشاركين يعتقدون بقوة أن البنك محل الدراسة يمتلك وعيا عاليا ومسبقا بالمخاطر السيبرانية ، و هذا يدل على نضج في الثقافة الأمنية الرقمية، ما يضع أساسا متينا لأي إستراتيجية أمنية فعالة؛
- ✓ **العبارة رقم (02):** قدر المتوسط الحسابي للعبارة بـ (4.043) بانحراف معياري قد ره (0.877) باتجاه مرتفع، يشير هذا التقدير المرتفع إلى أن البنك محل الدراسة لا يكتفي بالوعي، بل يطبق إجراءات عملية واستباقية لمواجهة الهجمات، ما يعكس وجود بروتوكولات أمنية مفعلة وتدابير وقائية قائمة؛
- ✓ **العبارة رقم(03):** قدر المتوسط الحسابي للعبارة ب (3.869) بانحراف معياري قدره (1.057) باتجاه مرتفع، وهذا يدل على أن البنك يمتلك إطارا تنظيميا واضحا للأمن السيبراني، لكنه ليس الأعلى تقييما، مما قد يشير إلى الحاجة إلى مراجعة وتحديث مستمر للسياسات بشكل أعمق؛
- ✓ **العبارة رقم (04):** قدر المتوسط الحسابي للعبارة بـ (4.087) بانحراف معياري قدره (0.949) باتجاه مرتفع، يدل على وجود نظم تتبع ومراقبة معتبرة في البنك، مما يعزز جاهزيته للتعامل مع الهجمات، كما يشير إلى مستوى جيد من الاستباقية التقنية؛
- ✓ **العبارة رقم (05):** قدر المتوسط الحسابي للعبارة بـ (3.826) بانحراف معياري قدره (1.266) باتجاه مرتفع، رغم كونه تقييما مرتفعا، إلا أنه أقل من بعض العبارات الأخرى، ما قد يشير إلى تفاوت في استخدام التشفير أو تطوره عبر أقسام البنك، أو وجود بعض القصور في التقنيات المعتمدة؛
- ✓ **العبارة رقم (06):** قدر المتوسط الحسابي للعبارة بـ (3.869) بانحراف معياري قدره (0.919) باتجاه مرتفع، يعكس هذا التقدير الإيجابي أن البنك يعتمد بالفعل على ممارسات مصادقة مزدوجة أو متعددة، ما يعزز الأمان التشغيلي، لكنه يشير أيضا إلى إمكانية تعزيز هذه الممارسات أو تعميمها على كل الخدمات؛

- ✓ **العبارة رقم (07):** قدر المتوسط الحسابي للعبارة بـ (4.043) بانحراف معياري قدره (0.767) باتجاه مرتفع، وهذا يظهر أن هذه السياسات مقدرة بشكل جيد من المشاركين، ويعتقد بأنها تساهم فعليا في بناء الثقة، مما يعكس نجاحا نسبيا في الجانب الوقائي والأمني؛
- ✓ **العبارة رقم (08):** قدر المتوسط الحسابي للعبارة بـ (3.956) بانحراف معياري قدره (0.824) باتجاه مرتفع، وهذا يشير إلى أن هناك قناعة بأن الأمن السيبراني عنصر استراتيجي مؤثر في التنافسية والاستدامة، مما يعكس دمجه في الخطط الإدارية للبنك؛
- ✓ **العبارة رقم (09):** قدر المتوسط الحسابي للعبارة بـ (3.652) بانحراف معياري قدره (0.831) باتجاه مرتفع، وهذا يظهر أن المشاركين يرون أن هذه الاستثمارات لها أثر إيجابي متوسط إلى مرتفع، لكن المستوى قد يشير إلى تحديات في التمويل أو تطبيق الاستثمار الأمثل؛
- ✓ **العبارة رقم (10):** قدر المتوسط الحسابي للعبارة بـ (4.173) بانحراف معياري قدره (0.650) باتجاه مرتفع، وهذا من أعلى التقديرات، ما يعكس أن هناك إجماعا على وجود صعوبات كبيرة في التحديث التقني، مما يتطلب إعادة هيكلة جذرية في البنية الرقمية الحالية للبنك؛
- ✓ **العبارة رقم (11):** قدر المتوسط الحسابي للعبارة بـ (3.434) بانحراف معياري قدره (1.079) باتجاه مرتفع، يعد هذا التقدير ضعيف، مما يشير إلى وجود مشكلة فعلية في رأس المال البشري المؤهل، وهو تحد خطير يجب أن يؤخذ بعين الاعتبار ضمن أي خطة إصلاحية؛
- ✓ **العبارة رقم (12):** قدر المتوسط الحسابي للعبارة بـ (3.434) بانحراف معياري قدره (1.160) باتجاه مرتفع، هذا يبرز أن ثقة العملاء في النظام الرقمي ما تزال محل تساؤل، وهو ما قد يؤثر على وتيرة التحول الرقمي وتقبله من طرف المستخدمين؛
- ✓ **العبارة رقم (13):** قدر المتوسط الحسابي للعبارة بـ (3.304) بانحراف معياري قدره (1.329) باتجاه متوسط،هو أدنى متوسط في العينة، ما يشير إلى أن البيئة القانونية تعتبر عامل ضعف كبير ومصدر تهديد غير مباشر لأمن البنك، ما يتطلب تدخلا تشريعيا واضحا على مستوى الدولة؛
- ✓ **العبارة رقم (14):** قدر المتوسط الحسابي للعبارة بـ (3.739) بانحراف معياري قدره (0,915) باتجاه مرتفع، يشير هذا التقدير إلى إدراك نسبي للتحدي القائم بين زيادة الأمان دون التأثير على راحة العميل، وهو ما يستدعي حلولا ذكية تحقق التوازن المطلوب.

وعليه، يتناول هذا المطلب عرضا وتحليلا لبيانات استجابات العينة حول بعدي القيادة الرقمية والأمن السيبراني، تمهيدا لاختبار فرضيات الدراسة في المطلب الموالي.

المطلب الثالث: نتائج اختبار فرضيات الدراسة

من خلال هذا المطلب، تم مناقش نتائج الدراسة في ضوء فرضيات البحث بهدف الوقوف على مدى تحققها أو رفضها، وذلك عبر اختبار الفرضية الرئيسية والفرضيات الفرعية، مع التأكد من التوزيع الطبيعي لبيانات الدراسة.

أولا: عرض وتحليل نتائج الفرضيات الفرعية (الفرضية الرئيسية الأولى)

يتضمن هذا الفرع عرض وتحليل نتائج اختبار الفرضيات الفرعية للفرضية الرئيسية الأولى والتي تتعلق بدراسة تأثير القيادة الرقمية على تعزيز الأمن السيبراني في البنك محل الدراسة، وذلك وفقا لأبعاد القيادة الرقمية المتمثلة في الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون.

1-اختبار التوزيع الطبيعي:

قبل تطبيق تحليل الانحدار لاختبار الفرضية الرئيسية تم إجراء اختبار كلمجروف-سمرنوف (Kolmogorov-Smirnov) من أجل ضمان ملائمة البيانات لافتراضات تحليل الانحدار أو بعبارة أخر للتحقق من مدى إتباع البيانات للتوزيع الطبيعي (Normal Distribution) كاختبار ضروري للفرضيات لأن معظم الاختبارات العلمية تشترط أن يكون توزيع البيانات طبيعيا.

وقد تم إجراء الاختبار بعد توزيع كل الاستمارات وجمعها من قبل أفراد عينة الدراسة، وكانت النتائج كما يوضحها الجدول التالي:[1]

الجدول رقم (18): نتائج اختبار التوزيع الطبيعي

محاور الاستبيان	محتوى المحور	قيمة Z	مستوى الدلالة (Sig)
المحور الأول	القيادة الرقمية	0.163	0.118
المحور الثاني	سلوك الأمن السيبراني	0.125	0.200
الاستبيان ككل		0.115	0.200

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتضح من خلال نتائج الجدول أعلاه أن قيمة مستوى الدلالة لكل محور من محاور الاستبيان وكذا بالنسبة للاستبيان ككل كان أكبر من (0.05)، أي أن (Sig>0.05) وهذا يدل على أن البيانات تتبع التوزيع الطبيعي ويمكن استخدام الاختبارات المعملية.

[1]-أنظر الملحق رقم (04)، ص. 122

2-نتائج الفرضيات الفرعية (الفرضية الرئيسية الأولى)

تم عرض وتفسير النتائج ومناقشتها من خلال ما تم التوصل إليه في أدوات الدراسة من أجل معرفة العلاقة بين (الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون) كأبعاد القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في البنك محل الدراسة، ومن أجل اختبار الفرضيات الفرعية تم الاعتماد على نتائج تحليل الانحدار الخطي البسيط (Y= ax+b) الذي يسمح بدراسة إمكانية وجود علاقة بين المتغير المستقل القيادة الرقمية والمتغير التابع سلوك الأمن السيبراني ، كما تم الاعتماد على معامل الارتباط (R) لمعرفة طبيعة العلاقة (طردية أو عكسية) عند مستوى دلالة ($\alpha \leq 0.05$) وقد تم حساب معامل التحديد (R2) لمعرفة نسبة التغير في المتغير التابع نتيجة للتغير في المتغير المستقل. ويمكن توضيح نتائج اختبار الفرضيات الفرعية من خلال الجدول التالي:[1]

الجدول رقم (19): نتائج اختبار الفرضيات الفرعية (الفرضية الرئيسية الأولى)

المتغيرات المستقلة	المتغير التابع	ثابت الانحدار (β)	معامل الانحدار (α)	معامل الارتباط (R)	معامل التحديد (R^2)	قيمة(t)	القيمة المحسوبة (F)	مستوى الدلالة (sig)
الابتكار الرقمي	سلوك الأمن السيبراني	0.238	0.878	0.693	0.480	4.403	19.391	0.000
الرؤية الرقمية		0.994	0.725	0.695	0.482	4.424	19.567	0.000
المعرفة الرقمية		1.750	0.511	0.507	0.257	2.694	7.257	0.014
المشاركة والتعاون		1.078	0.698	0.800	0.639	6.101	37.228	0.000

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتضح من خلال نتائج تحليل الانحدار البسيط الذي استخدم لمعرفة ما إذا كان هناك دور للمتغيرات المستقلة الجزئية في تعزيز سلوك الأمن السيبراني بالبنك محل الدراسة، ما يلي:

2-1-الفرضية الفرعية الأولى:

- **الفرضية الصفرية H_0**: لا يوجد أثر ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة ($\propto \leq 0.05$)؛

- **الفرضية البديلة H_1**: يوجد أثر ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة ($\propto \leq 0.05$).

[1]- أنظر الملحق رقم (04)، ص ص. 122- 125

يوضح الجدول أعلاه نتائج تحليل الانحدار الخطي البسيط الذي أستخدم لمعرفة العلاقة بين الابتكار الرقمي وتعزيز سلوك الأمن السيبراني في البنك محل الدراسة، وعليه تبين أن هناك تأثير ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ، إذ بلغت قيمة معامل الانحدار (0.878) وقد بلغ معامل الارتباط بين المتغيرين (0.693)، وهو ارتباط قوي وإيجابي وهذه المعاملات – معامل الانحدار والارتباط– ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$)، وهذا ما أوضحه اختبار (T)، وهذا دليل على أن الأمن السيبراني يتحقق من خلال الابتكار الرقمي بالبنك محل الدراسة، أما القابلية التفسيرية لنموذج الانحدار المتمثلة في معامل التحديد (R^2) فقد بلغت (0.480) مما يعني أن نسبة (48%) فقط من التغيرات في تعزيز سلوك الأمن السيبراني ترجع للابتكار الرقمي والباقي يعود لعوامل أخرى وقد أظهر اختبار (F) بأن نموذج الانحدار بشكل عام ذو دلالة إحصائية.

كما أن مستوى الدلالة بلغ (0.000) وهو أقل من مستوى المعنوية (0.05) وبهذه النتائج تقبل الفرضية البديلة الموالية:

" يوجد أثر ذو دلالة إحصائية للابتكار الرقمي على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة($\alpha \leq 0.05$)."

ويمكن كتابة العلاقة بين الابتكار الرقمي وتعزيز سلوك الأمن السيبراني في شكلها الرياضي من خلال المعادلة الخطية للانحدار كما يلي: **Y=0.878x+0.238**، حيث أن:

X :الابتكار الرقمي؛

Y : سلوك الأمن السيبراني.

وبالتالي ومن خلال تحليل نتائج التحليل الإحصائي تم برهنة أن القيادة الرقمية لها أثر في تعزيز الأمن السيبراني بالبنك محل الدراسة من خلال بعد الابتكار الرقمي.

2-2-الفرضية الفرعية الثانية:

- **الفرضية الصفرية H_0:** لا يوجد أثر ذو دلالة إحصائية للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة ($\alpha \leq 0.05$)؛

- **الفرضية البديلة H_1:** يوجد أثر ذو دلالة إحصائية للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة ($\alpha \leq 0.05$).

يوضح الجدول أعلاه نتائج تحليل الانحدار الخطي البسيط الذي أستخدم لمعرفة العلاقة بين ا لرؤية الرقمية وتعزيز سلوك الأمن السيبراني في البنك محل الدراسة، وعليه تبين أن هناك تأثير ذو دلالة إحصائية

للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ، إذ بلغت قيمة معامل الانحدار (0.725) وقد بلغ معامل الارتباط بين المتغيرين (0.695)، وهو ارتباط قوي وإيجابي وهذه المعاملات – معامل الانحدار والارتباط – ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$)، وهذا ما أوضحه اختبار (T)، وهذا دليل على أن الأمن السيبراني يتحقق من خلال الرؤية الرقمية بالبنك محل الدراسة، أما القابلية التفسيرية لنموذج الانحدار المتمثلة في معامل التحديد (R^2) فقد بلغت (0.482) مما يعني أن نسبة (48.2%) فقط من التغيرات في تعزيز سلوك الأمن السيبراني ترجع للرؤية الرقمية والباقي يعود لعوامل أخرى وقد أظهر اختبار (F) بأن نموذج الانحدار بشكل عام ذو دلالة إحصائية.

كما أن مستوى الدلالة بلغ (0.000) وهو أقل من مستوى المعنوية (0.05) وبهذه النتائج تقبل الفرضية البديلة الموالية:

" يوجد أثر ذو دلالة إحصائية للرؤية الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46– عند مستوى الدلالة($\propto \leq 0.05$)."

ويمكن كتابة العلاقة بين الرؤية الرقمية وتعزيز سلوك الأمن السيبراني في شكلها الرياضي من خلال المعادلة الخطية للانحدار كما يلي: **$Y=0.725\ x+0.994$**، حيث أن:

X :للرؤية الرقمية؛

Y :سلوك الأمن السيبراني.

وبالتالي ومن خلال تحليل نتائج التحليل الإحصائي تم برهنة أن القيادة الرقمية لها أثر في تعزيز الأمن السيبراني بالبنك محل الدراسة من خلال بعد الرؤية الرقمية.

2-3-الفرضية الفرعية الثالثة:

- **الفرضية الصفرية H_0**: لا يوجد أثر ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46– عند مستوى الدلالة ($\propto \leq 0.05$)؛

- **الفرضية البديلة H_1**: يوجد أثر ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46– عند مستوى الدلالة ($\propto \leq 0.05$).

يوضح الجدول أعلاه نتائج تحليل الانحدار الخطي البسيط الذي أستخدم لمعرفة العلاقة بين ا لمعرفة الرقمية وتعزيز سلوك الأمن السيبراني في البنك محل الدراسة، وعليه تبين أن هناك تأثير ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ، إذ بلغت قيمة معامل الانحدار (0.511) وقد بلغ معامل الارتباط بين المتغيرين (0.507)، وهو ارتباط متوسط وإيجابي وهذه المعاملات –معامل الانحدار والارتباط– ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$)، وهذا ما أوضحه اختبار (T)، وهذا دليل على أن

الأمن السيبراني يتحقق من خلال المعرفة الرقمية بالبنك محل الدراسة، أما القابلية التفسيرية لنموذج الانحدار المتمثلة في معامل التحديد (R^2) فقد بلغت (0.257) مما يعني أن نسبة (25.7%) فقط من التغيرات في تعزيز سلوك الأمن السيبراني ترجع للمعرفة الرقمية والباقي يعود لعوامل أخرى وقد أظهر اختبار (F) بأن نموذج الانحدار بشكل عام ذو دلالة إحصائية.

كما أن مستوى الدلالة بلغ (0.014) وهو أقل من مستوى المعنوية (0.05) وبهذه النتائج تقبل الفرضية البديلة الموالية:

" يوجد أثر ذو دلالة إحصائية للمعرفة الرقمية على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة - 46- عند مستوى الدلالة($\alpha \leq 0.05$)."

ويمكن كتابة العلاقة بين المعرفة الرقمية وتعزيز سلوك الأمن السيبراني في شكلها الرياضي من خلال المعادلة الخطية للانحدار كما يلي: **$Y=0.511\ x+1.750$**، حيث أن:

X :المعرفة الرقمية؛

Y :سلوك الأمن السيبراني.

وبالتالي ومن خلال تحليل نتائج التحليل الإحصائي تم برهنة أن القيادة الرقمية لها أثر في تعزيز الأمن السيبراني بالبنك محل الدراسة من خلال بعد المعرفة الرقمية.

2-4-الفرضية الفرعية الرابعة:

- **الفرضية الصفرية H_0:** لا يوجد أثر ذو دلالة إحصائية للمشاركة والتعاون على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة - 46- عند مستوى الدلالة ($\alpha \leq 0.05$)؛

- **الفرضية البديلة H_1:** يوجد أثر ذو دلالة إحصائية للمشاركة والتعاون على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة - 46- عند مستوى الدلالة ($\alpha \leq 0.05$).

يوضح الجدول أعلاه أيضا، نتائج تحليل الانحدار الخطي البسيط الذي أستخدم لمعرفة العلاقة بين المشاركة والتعاون وتعزيز سلوك الأمن السيبراني في البنك محل الدراسة، وعليه تبين أن هناك تأثير ذو دلالة إحصائية للمشاركة والتعاون في تعزيز سلوك الأمن السيبراني، إذ بلغت قيمة معامل الانحدار (0.698) وقد بلغ معامل الارتباط بين المتغيرين (0.800)، وهو ارتباط قوي وإيجابي وهذه المعاملات – معامل الانحدار والارتباط– ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$)، وهذا ما أوضحه اختبار (T)، وهذا دليل على أن الأمن السيبراني يتحقق من خلال المشاركة والتعاون بالبنك محل الدراسة ، أما القابلية التفسيرية لنموذج الانحدار المتمثلة في معامل التحديد (R^2) فقد بلغت (0.639) مما يعني أن نسبة (63.9%) فقط

من التغيرات في تعزيز سلوك الأمن السيبراني ترجع للمشاركة والتعاون والباقي يعود لعوامل أخرى وقد أظهر اختبار(F) بأن نموذج الانحدار بشكل عام ذو دلالة إحصائية.

كما أن مستوى الدلالة بلغ (0.000) وهو أقل من مستوى المعنوية (0.05) وبهذه النتائج تقبل الفرضية البديلة الموالية:

" يوجد أثر ذو دلالة إحصائية للمشاركة والتعاون على تعزيز سلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46– عند مستوى الدلالة($0.05 \geq \propto$)."

ويمكن كتابة العلاقة بين بعد المشاركة والتعاون وتعزيز سلوك الأمن السيبراني في شكلها الرياضي من خلال المعادلة الخطية للانحدار كما يلي: **Y=0.698 x+1.078**، حيث أن:

X :المشاركة والتعاون؛

Y :سلوك الأمن السيبراني.

وبالتالي ومن خلال تحليل نتائج التحليل الإحصائي تم برهنة أن القيادة الرقمية لها أثر في تعزيز الأمن السيبراني بالبنك محل الدراسة من خلال بعد المشاركة والتعاون.

ثانيا: عرض وتحليل نتائج الفرضيات الفرعية (الفرضية الرئيسية الثانية)

يتضمن هذا الفرع عرض وتفسير النتائج ومناقشتها من خلال ما تم التوصل إليه في أدوات الدراسة من أجل معرفة ما إذا كان هناك فروق ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إجابات أفراد العينة لأثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية) بالبنك محل الدراسة ، حيث لأجل اختبار الفرضيات الفرعية تم الاعتماد على نتائج تحليل التباين الأحادي ANOVA الذي يعتبر اختبار معلمي يهدف للمقارنة بين المتوسطات أو الوصول إلى قرار بوجود أو عدم وجود فروق بين متوسطات الأداء عند المجموعات التي تعرضت لمعالجات مختلفة بهدف التوصل إلى العوامل التي تجعل متوسط من المتوسطات يختلف عن المتوسطات الأخرى باعتبار قيمة F المحسوبة والجدولية والدلالة الإحصائية التي تشير إلى أقل أو تساوي (0.05) ويمكن توضيح نتائج اختبار الفرضيات الفرعية من خلال الجدول التالي:[1]

[1]–أنظر الملحق رقم (04)، ص ص. 125– 126

الجدول رقم (20): تحليل التباين الأحادي ANOVA للبيانات الشخصية والوظيفية

المحور	المتغير التابع	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمةF المحسوبة	مستوى الدلالة (sig)
المستوى العلمي	أثر القيادة على تعزيز سلوك الأمن السيبراني	بين المجموعات	1.192	2	0.596	2.199	0.137
		داخل المجموعات	5.420	20	0.271		
		المجموع	6.612	22			
المركز الوظيفي		بين المجموعات	0.461	3	0.152	0.474	0.704
		داخل المجموعات	6.151	19	0.324		
		المجموع	6.612	22			
الخبرة المهنية		بين المجموعات	1.232	3	0.411	1.450	0.260
		داخل المجموعات	5.380	19	0.283		
		المجموع	6.612	22			

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائي Spss.

يتضح من خلال نتائج تحليل التباين الأحادي ANOVA الذي استخدم لمعرفة ما إذا كان هناك فروق ذات دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إجابات أفراد العينة لأثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية) بالبنك محل الدراسة، حيث تبين أنه:

1-الفرضية الفرعية الأولى:

-**الفرضية الصفرية H_0**: لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المستوى العلمي، ببنك الجزائر الخارجي BEA وكالة تبسة -46- عند مستوى الدلالة ($\propto \leq 0.05$)؛

-**الفرضية البديلة H_1**: توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المستوى العلمي، ببنك الجزائر الخارجي BEA وكالة تبسة -46- عند مستوى الدلالة ($\propto \leq 0.05$).

يتضح من الجدول أعلاه أن مستوى الدلالة أكبر من (0.05)، وعليه فإنه لا توجد اختلافات ذات دلالة إحصائية لأثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعود لاختلاف المستوى العلمي في البنك محل الدراسة، حيث أن كل الفئات من المستويات التعليمية المختلفة التي تتكون منها عينة الدراسة تتفق على أن البنك محل الدراسة يسعى إلى تعزيز سلوك الأمن السيبراني من خلال الاعتماد على أبعاد القيادة الرقمية، وعليه تقبل الفرضية الصفرية الموالية:

"لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المستوى العلمي، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$)."

2-الفرضية الفرعية الثانية:

-**الفرضية الصفرية H_0:** لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المركز الوظيفي، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$)؛

-**الفرضية البديلة H_1:** توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المركز الوظيفي، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$).

يتضح من الجدول أعلاه أن مستوى الدلالة أكبر من (0.05)، وعليه فإنه لا توجد اختلافات ذات دلالة إحصائية لأثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعود لاختلاف المركز الوظيفي في البنك محل الدراسة، حيث أن كل المراكز الوظيفية المختلفة التي تتكون منها عينة الدراسة تتفق على أن البنك محل الدراسة تتفق على أن تعزيز سلوك الأمن السيبراني يكون انطلاقا من القيادة الرقمية ، وعليه تقبل الفرضية الصفرية الموالية:

"لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير المركز الوظيفي، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$)."

3-الفرضية الفرعية الثالثة:

-**الفرضية الصفرية H_0:** لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير الخبرة المهنية، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة $(\propto \leq 0.05)$؛

-**الفرضية البديلة H_1:** توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير الخبرة المهنية، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة $(\propto \leq 0.05)$.

يتضح من الجدول أعلاه أن مستوى الدلالة أكبر من (0.05)، وعليه فإنه لا توجد اختلافات ذات دلالة إحصائية لأثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعود لاختلاف الخبرة المهنية في البنك محل الدراسة، حيث أن كل الفئات ذات الخبرات المختلفة التي تتكون منها عينة الدراسة في البنك محل الدراسة تتفق على أن تعزيز سلوك الأمن السيبراني يكون انطلاقا من القيادة الرقمية ، وعليه تقبل الفرضية الصفرية الموالية:

"لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى لمتغير الخبرة المهنية، ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة $(\propto \leq 0.05)$."

ثالثا: عرض وتحليل نتائج اختبار الفرضيات الرئيسية

من خلال هذا الفرع تم عرض وتحليل نتائج اختبار الفرضيتان الرئيسيتان واللتان تتعلقان بدراسة تأثير القيادة الرقمية على تعزيز الأمن السيبراني في البنك محل الدراسة، كما تم اختبار إذا كانت هناك فروق ذات دلالة إحصائية وفقا للبيانات الشخصية الوظيفية لعينة الدراسة.

1-اختبار الفرضية الرئيسية الأولى:

تم اختبار الفرضية الرئيسية الأولى من خلال الجدول التالي:[1]

[1]-أنظر الملحق رقم (04)، ص. 126

الجدول رقم (21): نتائج اختبار الفرضية الرئيسية الأولى

المتغير المستقل	المتغير التابع	ثابت الانحدار(β)	معامل الانحدار(α)	معامل الارتباط(R)	معامل التحديد(R^2)	قيمة(t)	القيمة المحسوبة(F)	مستوى الدلالة(sig)
القيادة الرقمية	سلوك الأمن السيبراني	0.082	0.976	0.801	0.642	6.132	37.602	0.000

المصدر:من إعداد الطالبين بناء على مخرجات نتائج التحليل الإحصائيSpss.

-**الفرضية الصفرية H_0**: لا يوجد أثر ذو دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$)؛

-**الفرضية البديلة H_1**: يوجد أثر ذو دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني ببنك الجزائر الخارجي BEA وكالة تبسة – 46- عند مستوى الدلالة ($\propto \leq 0.05$).

يوضح الجدول أعلاه نتائج تحليل الانحدار الخطي البسيط الذي أستخدم لمعرفة العلاقة بين القيادة الرقمية وتعزيز سلوك الأمن السيبراني في البنك محل الدراسة، وعليه تبين أن هناك أثر للقيادة الرقمية على تعزيز سلوك الأمن السيبراني في البنك محل الدراسة، حيث نجد:

-قيمة معامل الارتباط (R) بلغت 0.801 بين متغير القيادة الرقمية وتعزيز سلوك الأمن السيبراني، وهو ما يدل على وجود علاقة ارتباط قوي وايجابي بين المتغيرين.

-كما بلغ معامل التحديد (R^2) القيمة 0.642 وهذا يدل على أن متغير القيادة الرقمية يمكن أن يفسر ما قيمته 64.2% فقط من تباين المتغير التابع، أي أن ما نسبته 64.2% من التغيرات الحاصلة في سلوك الأمن السيبراني في البنك محل الدراسة ناتجة عن التغيرات في القيادة الرقمية، وأن الباقي يرجع لتأثير عوامل أخرى.

- أما قيمة (F) المحسوبة بلغت 37.602 بمستوى دلالة 0.000 وهو أقل من مستوى الدلالة الإحصائية المعتمد في هذه الدراسة (0.05)، وهو ما يؤكد معنوية القيادة الرقمية في تعزيز سلوك الأمن السيبراني في البنك محل الدراسة.

كما أن مستوى الدلالة بلغ (0.000) وهو أقل من مستوى المعنوية (0.05) وبهذه النتائج تقبل الفرضية البديلة الموالية:

"يوجد أثر ذو دلالة إحصائية بين القيادة الرقمية وسلوك الأمن السيبراني ببنك الجزائر الخارجي BEAوكالة تبسة - 46- عند مستوى الدلالة($\alpha \leq 0.05$)."

ويمكن كتابة العلاقة بين القيادة الرقمية وتعزيز سلوك الأمن السيبراني بالبنك محل الدراسة في شكلها الرياضي من خلال المعادلة الخطية للانحدار كما يلي:

$Y=0.976\ x+0.082$، حيث أن:

X : القيادة الرقمية؛

Y :سلوك الأمن السيبراني.

وبالتالي ومن خلال تحليل نتائج التحليل الإحصائي تم برهنة أن القيادة الرقمية لها دور في تعزيز سلوك الأمن السيبراني في البنك محل الدراسة.

2-اختبار الفرضية الرئيسية الثانية:

تم اختبار الفرضية الرئيسية الأولى من خلال الجدول التالي:[1]

-**الفرضية الصفرية H_0:** لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، ببنك الجزائر الخارجي BEA وكالة تبسة - 46- عند مستوى الدلالة ($\alpha \leq 0.05$)؛

-**الفرضية البديلة H_1:** توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، ببنك الجزائر الخارجي BEA وكالة تبسة -46-عند مستوى الدلالة ($\alpha \leq 0.05$).

وانطلاقا من نتائج الجدول رقم (20) أعلاه نلاحظ ما يلي:

أن كل من البيانات الشخصية الوظيفية لأفراد عينة الدراسة (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، بعد تحليل نتائج تحليل التباين الأحادي ANOVA تبين أنه لا توجد فروق ذات دلالة إحصائية ترجع إلى كل من (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)في البنك محل الدراسة، وبالتالي وفقا لهذه البيانات الشخصية الوظيفية يتم قبول الفرضية الصفرية الموالية:

"لا توجد فروق ذات دلالة إحصائية بين إجابات أفراد العينة لأثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، ببنك الجزائر الخارجي BEA وكالة تبسة - 46- عند مستوى الدلالة ($\alpha \leq 0.05$)."

[1]- أنظر الملحق رقم (04)، ص. 126

وعليه، تم في هذا المطلب اختبار فرضيات الدراسة باستخدام أسلوبي التوزيع الطبيعي والانحدار الخطي البسيط، من أجل التحقق من أثر أبعاد القيادة الرقمية على تعزيز سلوك الأمن السيبراني في البنك محل الدراسة. وقد أظهرت نتائج اختبار الفرضيات الفرعية أن لكل من الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، والمشاركة والتعاون أثر ذو دلالة إحصائية إيجابية على سلوك الأمن السيبراني، حيث كانت قيم الدلالة أقل من المستوى المعتمد (0.05). كما بينت نتائج الانحدار أن أقوى تأثير تحقق من خلال بعد المشاركة والتعاون، تليه الرؤية الرقمية، ثم الابتكار الرقمي، وأخيراً المعرفة الرقمية. أما بالنسبة للفرضيات المرتبطة بمتغيرات العينة (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، فقد أظهر تحليل التباين الأحادي عدم وجود فروق ذات دلالة إحصائية بين استجابات الأفراد بشأن أثر القيادة الرقمية على سلوك الأمن السيبراني تعزى لهذه المتغيرات. وهو ما يعزز من مصداقية النتائج ويؤكد تجانس آراء العينة حول دور القيادة الرقمية في دعم الأمن السيبراني.

خلاصة القول، تم في هذا المبحث إبراز أهمية التحليل الإحصائي في تقييم دور القيادة الرقمية في تعزيز سلوك الأمن السيبراني داخل البنك محل الدراسة. من خلال تحليل البيانات الشخصية لعينة الدراسة، اتضح أن البنك يعتمد على كفاءات جامعية وخبرة مهنية معتبرة، مما يعزز من فعالية تبني القيادة الرقمية. أما نتائج الدراسة الميدانية فقد أظهرت أن أبعاد القيادة الرقمية تتمثل في الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، والمشاركة والتعاون، وهي أبعاد حققت مستويات تقييم مرتفعة من طرف أفراد العينة. كما برهنت اختبارات الفرضيات وجود علاقة تأثير إيجابية وذات دلالة إحصائية للقيادة الرقمية على سلوك الأمن السيبراني، مما يدل على أن الاستثمار في تطوير القدرات القيادية الرقمية داخل البنك يُسهم بشكل مباشر في تحسين الأمن السيبراني وضمان حماية البيانات والأنظمة المصرفية.

خلاصة الفصل الثاني

من خلال هذا الفصل التطبيقي تم التعرف على البنك محل الدراسة، وواقع تطبيق متغيرات الدراسة (القيادة الرقمية وسلوك الأمن السيبراني) في البنك، وذلك بالاعتماد على الاستبيان، والذي يتكون من محورين أساسيين ، يمثل المحور الأول البيانات الشخصية الوظيفية لعينة الدراسة، والمحور الثاني الخاص بعبارات الدراسة المقسم إلى جزأين، الجزء الأول الخاص بالمتغير المستقل "القيادة الرقمية " بـأبعاده، المخصص له 20 سؤال ، إلى العينة المتكونة من 23 موظف بالبنك ، أما الجزء الثاني والذي يتمثل في المتغير التابع وهو سلوك الأمن السيبراني، وتم توجيهه إلى نفس العينة من خلال 13 سؤال، ليتم بعد ذلك إخضاع البيانات المتحصل عليها إلى عملية التحليل الإحصائي باستخدام برنامج (SPSS V25)، حيث تم التوصل إلى مجموعة من النتائج أهمها:

-أن مستوى تطبيق القيادة الرقمية بمختلف أبعادها(الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون)، في البنك محل الدراسة مقبول جدا حيث كانت نتائج المتوسط الحسابي قدرها (4.021) وانحراف معياري قدره (0.520) بدرجة موافقة مرتفعة؛

-مستوى تعزيز الأمن السيبراني في البنك محل الدراسة مقبول حيث كانت نتائج المتوسط الحسابي قدرها (3.841) وانحراف معياري قدره (0.634) بدرجة موافقة مرتفعة؛

-يوجد أثر للقيادة الرقمية بمختلف أبعادها في تعزيز سلوك الأمن السيبراني في البنك محل الدراسة،إذ تساهم القيادة الرقمية بنسبة (64.2%) في التغيرات التي تعزز سلوك الأمن السيبراني وهي نسبة مساهمة جيدة، في حين أن باقي النسبة يعود لعوامل أخرى؛

-يعد بعد المشاركة والتعاون من أكثر أبعاد القيادة الرقمية إسهاما في تعزيز سلوك الأمن السيبراني ، إذ يساهم بعد المشاركة والتعاون بنسبة (63.9%) في التغيرات التي تعزز سلوك الأمن السيبراني في البنك محل الدراسة، وهذا يؤكد على أن الأمن السيبراني لا يمكن تحقيقه من خلال الجهود الفردية فقط، بل يتطلب التعاون والمشاركة بين الأفراد ، يليه بعدي الرؤية الرقمية والابتكار الرقمي في مرتبة الثانية والثالثة على التوالي بنسبة مساهمة متقاربة، حيث تقدر بـ (48.2%) وتقدر بـ (48.0%)، ثم عنصر المعرفة الرقمية في الرتبة الرابعة بنسبة مساهمة تقدر بـ (25.7%)، وهو أقل بعد في القيادة الرقمية مساهمة في تعزيز سلوك الأمن السيبراني.

-كما بينت نتائج الدراسة أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في إجابات أفراد العينة حول متغير القيادة الرقمية في تعزيز سلوك الأمن السيبراني تعزى للخصائص الشخصية الوظيفية (المستوى العلمي، المركز الوظيفي، الخبرة المهنية)، في البنك محل الدراسة.

خاتمة

خاتمة

ختاما، تناولت هذه الدراسة موضوعًا حديثًا في أدبيات الإدارة المعاصرة، يتمثل في أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني داخل المؤسسات المالية، مع التركيز على دراسة ميدانية ببنك الجزائر الخارجي BEA وكالة تبسة –46–. وقد سعت إلى تحليل كيف تُمكّن القيادة الرقمية من توجيه الموظفين نحو الاستخدام الأمن للتكنولوجيا، ليس من خلال الأدوات التقنية فقط، بل عبر أبعاد تتعلق بالابتكار، الرؤية، المعرفة، والمشاركة والتعاون.

وقد ساهمت الدراسة في إبراز أن القيادة الرقمية تُعد نمطًا متكاملًا يمكّن المؤسسات من مواجهة التحديات الرقمية، ويُرسّخ سلوكيات أمنية احترازية لدى الموظفين. كما بيّنت نتائج الدراسة التطبيقية وجود علاقة تأثير مباشرة بين القيادة الرقمية وسلوك الأمن السيبراني، وشمول هذا التأثير لمختلف فئات العينة، مما يعزّز من أهمية دمج مفاهيم القيادة الرقمية ضمن استراتيجيات الحماية السيبرانية للمؤسسات.

والجدير بالذكر أن هذه الدراسة تُضيف قيمة علمية من خلال تركيزها على السياق الجزائري، وتقديمها نموذجًا ميدانيًا واقعيًا يُسهم في سد فجوة قائمة في الدراسات المحلية التي تناولت العلاقة بين التحول الرقمي والأمن السيبراني داخل القطاع المالي.

ختامًا، تؤكد هذه الدراسة أن تبني القيادة الرقمية لم يعد خيارًا في المؤسسات المالية، بل ضرورة إستراتيجية لضمان أمنها الرقمي واستمراريتها في بيئة تتسم بالتحديات السيبرانية المتزايدة.

أولا: نتائج الدراسة

تُبرز هذه الدراسة من خلال جانبها النظري أن القيادة الرقمية تمثل استجابة حديثة لمتطلبات التحول الرقمي، وتهدف إلى تحسين الأداء المؤسسي عبر استغلال التكنولوجيا بفعالية. وتستند إلى أربعة أبعاد مركزية: الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، والمشاركة والتعاون. وقد تبين أن القائد الرقمي يسهم في ترسيخ ثقافة الأمن السيبراني من خلال التوجيه المستمر والتحفيز، مما يعزز وعي الموظفين بضرورة حماية البيانات والمعلومات الحساسة.

أما على المستوى التطبيقي، فقد أظهرت نتائج الدراسة الميدانية أن موظفي البنك محل الدراسة يتمتعون باتجاهات إيجابية نحو كل من القيادة الرقمية وسلوك الأمن السيبراني، وهو ما يشير على وجود وعي متزايد بأهمية هذه المفاهيم في بيئة العمل الرقمية.

كما دلّ التحليل الإحصائي على وجود علاقة تأثير إيجابية ذات دلالة معنوية بين القيادة الرقمية بجميع أبعادها وسلوك الأمن السيبراني. وبرز بُعد المشاركة والتعاون كأكثر الأبعاد تأثيرًا، متبوعًا بالرؤية والابتكار الرقمي ، في حين كان تأثير المعرفة الرقمية أقل نسبيًا، لكنه يظل ضمن المستوى المقبول.

من جهة أخرى، لم تُسجل فروق دالة في إدراك تأثير القيادة الرقمية على تعزيز سلوك الأمن السيبراني تعزى إلى المتغيرات الشخصية (المستوى العلمي، المركز الوظيفي، أو سنوات الخبرة)، مما يدل على أن هذا التأثير يمتد بشكل متجانس بين جميع فئات العينة.

ثالثا: التوصيات

في ضوء النتائج التي تم التوصل إليها من خلال الدراسة النظرية والتطبيقية، تقترح هذه الدراسة مجموعة من التوصيات العملية التي من شأنها دعم تفعيل القيادة الرقمية وتعزيز سلوك الأمن السيبراني داخل البنك محل الدراسة، وتتمثل فيما يلي:

- ✓ ضرورة تكوين العاملين داخل المؤسسة البنكية في مجال القيادة الرقمية، لما لها من دور فعّال في تحسين الأداء وتوجيه السلوك الوظيفي في ظل البيئة الرقمية؛
- ✓ الحرص على تنفيذ برامج تدريبية وتنسيق مهارات القيادة الرقمية بما يسمح بترقية الكفاءات الداخلية وتحقيق الانسجام مع متطلبات العصر الرقمي؛
- ✓ ضرورة توعية العاملين بأهمية القيادة الرقمية، وزيادة معرفتهم بمفاهيمها ومجالات تطبيقها داخل المؤسسة؛
- ✓ العمل على استغلال أبعاد القيادة الرقمية (الابتكار الرقمي ، الرؤية الرقمية ، المعرفة الرقمية ، المشاركة والتعاون)، بطريقة عملية تُعزز من سلوك الأمن السيبراني لدى الموظفين؛
- ✓ تشجيع الانفتاح على استخدام التكنولوجيا الرقمية الحديثة ضمن بيئة العمل، بما يساهم في رفع جاهزية المؤسسة لمواجهة تحديات الأمن السيبراني.

رابعا: أفاق الدراسة

في ضوء معالجة إشكالية هذه الدراسة، برزت مجموعة من الآفاق البحثية المستقبلية التي يمكن التوسع فيها، ومن أبرزها:

- إجراء دراسات مقارنة دولية بين مؤسسات مالية في دول مختلفة، بهدف تقييم مستويات تبني القيادة الرقمية وأثرها على السلوكيات السيبرانية؛
- استكشاف دور القيادة الرقمية في المؤسسات الحكومية غير المالية، مثل قطاعات الصحة، التعليم، والعدالة، لقياس مدى فعاليتها في ترسيخ ممارسات الأمن الرقمي؛
- دراسة أدوار القادة الرقميين في إدارة الأزمات السيبرانية داخل بيئات معقدة أو عالية المخاطر، لتحديد مهارات القيادة المطلوبة في مواجهة التحديات الرقمية المعاصرة.

قائمة المراجع

قائمة المراجع

أولا: المراجع باللغة العربية

I.الكتب

1. الأشقر منى جبور، **السيبرانية هاجس العصر**، مجلة المكتبات والمعلومات والتوثيق في العالم العربي، جامعة الدول العربية، قطاع الأعمال والاتصال-إدارة المعلومات والتوثيق والترجمة، بيروت -لبنان-، 2016؛
2. بوقلقول الهادي، **تحليل البيانات باستخدام SPSS**، ندوة علمية، جامعة باجي مختار، عنابة، 2013؛
3. الحديدي أيمن احمد، **الأمن السيبراني في ظل الانفجار المعرفي**، ط1،دار اليازوري للنشر والتوزيع، عمان، الأردن، 2023؛
4. حلاق بطرس، **القيادة الإدارية**، منشورات الجامعة الافتراضية السورية،سوريا، 2020؛
5. خالد محمد السواعي، **مدخل إلى تحليل البيانات باستخدام SPSS**، ط1، عالم الكتب الحديث، 2011؛
6. ذوقان عبيدات، عبد الرحمن عدس، محمد عبد الحق ، **البحث العلمي: مفهومه، أدواته، وأساليبه**، ط3، دار الفكر للنشر والتوزيع، عمان، 1998؛
7. سالدر فيليب، ترجمة هدى فؤاد، **القيادة**، ط1، مجموعة النيل العربي، القاهرة، مصر، 2008؛
8. السكارنة بلال خلف، **القيادة الإدارية الفعالة**، ط2، دار الميسرة للنشر والتوزيع، عمان، الأردن، 2014؛
9. الطجم عبد الله بن عبد الغني، طلق بن عوض الله السواط، **السلوك التنظيمي**، ط4، دار حافظ للنشر والتوزيع، المملكة العربية السعودية، 2003؛
10. العتبي محمود مهدي، **تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي SPSS**، دار حامد، الأردن، 2005؛
11. العلاق بشير، **القيادة الإدارية**، دار اليازوري العلمية للنشر والتوزيع،عمان، الأردن، 2009؛
12. اللقاني عبد الله، **دور الأمن السيبراني في تعزيز أمن المعلومات المالية والإلكترونية**، دار اليازوري العلمية للنشر والتوزيع، عمان، الأردن، 2023؛

II.المذكرات والأطروحات الجامعية

13. الجريان أسماء عوض نهار، "**القيادة الرقمية وعلاقتها بالأداء الوظيفي في المدارس الحكومية** "، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2024؛

14. الجيوسي سيرين عزيز حسن حسني، **"القيادة الرقمية وعلاقتها بالاحتراق الرقمي لدى معلمي المدارس الخاصة الأردنية"**، رسالة ماجستير، جامعة الشرق الأوسط، عمان، الأردن، 2024؛

15. المهنّديّ منى عبد عليّ، " **دور القيادة العليا في تبني حالة التغيير وتضمين إستراتيجية التحول الرقميّ** دراسة حالة: الهيئة العامة لشؤون القاصرين بدولة قطر"، رسالة ماجستير ،جامعة قطر، 2023؛

16. دحبج سالم حمد، **"دور الأتمته في تحسين قيادة المؤسسات الاجتماعية"**، رسالة ماجستير، جامعة قطر، 2023؛

17. دوح التجاني، " **سلوكيات القيادة التحويلية وأثرها على الإبداع التنظيمي** –دراسة حالة – جامعة غرداية"، أطروحة دكتوراه، جامعة غرداية، 2020؛

18. صيتي عبد اللطيف، " **دور أنماط القيادة الإدارية في تدعيم سلوك المواطنة التنظيمية في الجامعات الجزائرية** – دراسة ميدانية على عينة من جامعات قسنطينة، ورقلة، تلمسان –"، أطروحة دكتوراه، جامعة قاصي مرباح، ورقلة، 2021؛

III. المجلات والدوريات العربية

19. البدري كمال حنان، حنان عبد الستار محمود، **"القيادة الرقمية كمدخل لتعزيز المرونة التنظيمية لدى القيادات الأكاديمية بجامعة أسوان"** ، المجلة التربوية كلية التربية، العدد 100، المجلد 01، 2022؛

20. أحمد الحسيني مجاهد فايزة، **" الوعي بالأمن السيبراني ترف أم ضرورة في عصر المعلوماتية"**، مجلة بحث وتربية المعهد الوطني للبحث في التربية، العدد 02، المجلد 13، 2023؛

21. إدريس عطية، " **مكانة الأمن السيبراني في منظومة الأمن الوطني الجزائري"** ، العدد 01، المجلد 01، 2019؛

22. العتيبي مها بنت غزاي عبد الله، **"تطبيقات قاعدة "الضرر يزال" في مجال الأمن السيبراني،** مجلة الإبراهيمي للآداب والعلوم الإنسانية، جامعة برج بوعريريج، العدد 02، المجلد 05، 2023؛

23. المرداس ندى بنت خالد، " **الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)**"، المجلة الدولية لنشر البحوث والدراسات، العدد 49، المجلد 05، 2023؛

24. بارة سمير، **"الأمن السيبراني (Cyper Security) في الجزائر: السياسات والمؤسسات"** ، المجلة الجزائرية للأمن الإنساني، العدد 04، بدون مجلد، 2017؛

25. بن فهم حسن العتيبي عفاف، **"دور القيادة في الحد من الجرائم المعلوماتية"** ، مجلة الدراسات الجامعية للبحوث الشاملة، العدد 05، المجلد 01، 2022؛

26. بوقرص ساعد، **"الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة"**، مجلة الأبحاث في الحماية الاجتماعية، العدد 01، المجلد 03، 2022؛

27. جبريل بصيلي أماني، "**واقع تطبيق القيادة الرقمية بمدارس التعليم العام بمنطقة أبها الحضرية من وجهة نظر القيادات التربوية**"، مجلة العلوم التربوية والنفسية، العدد 42، المجلد 6، 2022؛

28. حداوي أميرة هاتف، وآخرون، **"القيادة الرقمية ودورها في تعزيز سلوك الأمن السيبراني في الالمؤسسات"**، مجلة العلوم الإنسانية والطبيعية، العدد 01، المجلد 05، 2024؛

29. زمورة جمال، بن عيسى ليلى، "**دور القيادة الرقمية في نجاح التحول الرقمي للخدمات العمومية في الجزائر**"، مجلة الاقتصاديات المالية البنكية وإدارة الأعمال، العدد 02، المجلد 11، 2022؛

30. قطاف سليمان، بوقرين عبد الحليم، **"الأمن السيبراني والمضامين المفاهيمية المرتبطة به"** ، مجلة طبنة للدراسات العلمية الأكاديمية، العدد 02، المجلد 05، 2022؛

31. مها فهد الشمراني، **"أثر القيادة الرقمية على تحقيق التميز المؤسسي"**، المجلة العربية للنشر العلمي، العدد 58، المجلد 06، 2023؛

IV. الجرائد الرسمية

32. المرسوم التنفيذي رقم 05/20، **الجريدة الرسمية للجمهورية الجزائرية** ، العدد 6904، الصادرة بتاريخ 30 يوليو 2020م؛

ثانيا: مراجع باللغة الأجنبية

I. المجلات والدوريات الأجنبية

33. Anderson, Ashley, et al, **"Case-Based Learning for Cyber security Leaders: A Systematic Review and Research Agenda."**Information & Management, vol. 61, 2024, p. 104015. DOI : 10.1016/j.im.2024.104015, P1;

34. Barada Abd rrezzaq, Dahmani Fatima, **" The Level of Cyber security Awareness and Cybercrime Response among Internet Users in Algeria: A Field Study on Students of the Faculty of Humanities and Social Sciences at the University of Djilali Bounaam in Khamis Miliana"**, The journal of El-Ryssala for media studies,Issue03, volume 08, 2024;

35. Bounfour Ahmed, **digital futures, digital transformation**, Springer international publishing, edition 01, switzerland, 2016 ;

36. Dehimat Amina, Baroudi Mohammed, **"Reviewing the literature on the link between Digital Leadership characteristics and Digital Transformation Based on Dynamic Capabilities**", Journal of Economic Growth and Entrepreneurship JEGE Spatial and entrepreneurial development studies laboratory, Issue 03, volume 05, 2022;

37. Fetty poerwita sary**, digital leadership and organizational communication toward millennial Employees in A telecommunication company,** corporate governance and organizational behavior review**,** vol: 06, N°:04, university of Telkom, 2022;
38. Mihret Sheleme, Rajesh Sharma Rajendran, **"Cyber-attack and Measuring its Risk,** IRO Journal on Sustainable Wireless Systems, Issue 04, volume 03, 2021;
39. Mohsen Al- Faris Mubarak, Merei Hassan Hamad Bani Khaled, **" Impact of Digital Leadership on Kuwaiti Hospitals' Employees' Performance"**, Journal of Economic, Administrative and Legal Sciences **,** Issue 19, volume 06, 2022;
40. Ms.Karitika ,**"Leadership in the Cyber Age : Technology Integration for Excellence "**, Journal of Arts Humanities and Social Sciences (GASJAHSS), Issue 01, volume 01 , 2023;
41. Parashu Ram Pal,**"A Recent Study over Cyber Security and its Elements "**, International Journal of Advanced Reseearch in Computer Science, Issue 03, volume 08, 2022;
42. Regner Sabillon, Jeimy J. Cano M . , Jordi Serra-Ruiz, Victor Cavaller, **" Cybercrime and Cybercriminals : A Comprehensive Study,** International Journal of Computer Networks and Communications Security, Issue 06, volume 04 , 2016;
43. RiteshVerma, **"Cyber Security Challenges In The Era of Digital Transformation ",** In Trans disciplinary Threads: Crafting the Future Through Multidisciplinary Research, Volume 01, 2024;
44. Sereir El Hirtsi Hayet**, " An In-Depth Study For A Proposed National Cyber Strategy For Digital Economy In Algeria"**, Journal Of Economics And Management**,** Issue 01, volume 23, 2023;
45. Titiana Ertiö et al , **"The Role of Digital Leaders' Emotional Intelligence in Mitigating Employee Techno stress",** Business Horizons, Issue 03, volume 67, 2024;
46. Uche Mbanaso , Emmanuel s.Dandaura , **"The Cyberspace : Redefining A New World ",**IOSR Journal of Computer Engineering (IOSR- JCE), Issue03, volume 17 , 2015;
47. Vaman Ashqi Saeed, Renas Rajab Asaad, **"Cyber Security Threats, Vulnerability, Challenges With Proposed Solution"**, Applied Computing Journal, Issue 04, volume 02, 2022;
48. Yogesh P . Surwade, Hitendra J Patil, **" Information Security"**, SSRN (Social Science Research Network), 2024;
49. Yousfi Rihab, El Bachir El Ibrahimi Mohamed**, " Cybersecurity Challenges and International Cooperation",** Journal of law and humanities Sciences,Issue03, volume 17, 2024;

II.مواقع إلكترونية

50. Omar Alobthany,**" Cybersecurity Career", https://cyberhub.sa/posts/4223**.

قائمة الملاحق

الملحق رقم (01): قائمة الأساتذة المحكمين

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي – تبسة–

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم علوم التسيير

استمارة مقدمة للأساتذة الذين قاموا بتحكيم الاستبيان الخاص بمذكرة ماستر

تخصص إدارة أعمال

تحت عنوان: أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني في المؤسسات المالية

دراسة حالة: بنك الجزائر الخارجي BEA وكالة تبسة–46–

الرقم	الاسم واللقب	جهة التدريس	الجامعة
01	أ.د دريس يحي	كلية العلوم الاقتصادية والتجارية وعلوم التسيير	جامعة الشهيد الشيخ العربي التبسي
02	د. وداد بن قيراط	كلية العلوم الاقتصادية والتجارية وعلوم التسيير	جامعة الشهيد الشيخ العربي التبسي
03	د. عايب فاطمة الزهرة	كلية العلوم الاقتصادية والتجارية وعلوم التسيير	جامعة قسنطينة 2
04	د. جوال مروى	كلية العلوم الاقتصادية والتجارية وعلوم التسيير	جامعة قسنطينة 2

من إعداد الطلبة :

–إيمان زيطاري

–سمير دوالي

تحت إشراف الدكتورة:

–هيبة الله أوريسي

السنة الجامعية: 2025/2024

الملحق رقم (02): استمارة الاستبيان

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي – تبسة–

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

قسم علوم التسيير

استمارة الاستبيان حول:

أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني في المؤسسات المالية
دراسة حالة: بنك الجزائر الخارجي BEA وكالة تبسة–46–

مذكرة لنيل شهادة ماستر في علوم التسيير تخصص: إدارة أعمال

من إعداد الطلبة :

–إيمان زيطاري

–سمير دوالي

تحت إشراف الدكتورة:

–هيبة الله أوريسي

إلى موظفي بنك الجزائر الخارجي – BEA فرع تبسة–

في إطار التحضير لنيل شهادة الماستر تحت عنوان "أثر القيادة الرقمية في تعزيز سلوك الأمن السيبراني في المؤسسات المالية، دراسة حالة بنك الجزائر الخارجي BEA وكالة تبسة –46–"، نضع بين أيديكم هذا الاستبيان للمساعدة على إتمام هذه الدراسة عن طريق الإجابة على الأسئلة المرفقة. حيث أن صحة النتائج تعتمد بدرجة كبيرة على إجابتكم، مع العلم أن إجاباتكم ستُعامل بسرية تامة ولن يتم استخدامها إلا لأغراض البحث العلمي.

وفي الأخير، لكم منا جزيل الشكر على مساهمتكم القيّمة ومشاركتكم الفعالة في إثراء هذا الموضوع من خلال إجاباتكم على أسئلة هذا الاستبيان.

السنة الجامعية: 2025/2024

المحور الأول: الخصائص الشخصية

1. المستوى العلمي:

☐ ثانوي أو أقل ☐ شهادات جامعية

☐ شهادات أخرى (حدد): ----------

2. المركز الوظيفي:

☐ قائد رئيس مصلحة رئيس مصل☐

☐ مكلف بالزبائن ☐ وظيفة أخرى

3. الخبرة المهنية:

☐ أقل من 05 سنوات ☐ من 05 إلى 10 سنوات

☐ من 11 إلى 15 سنة ☐ أكثر من 15 سنة

المحور الثاني: العبارات الخاصة بالدراسة

الجزء الأول: القيادة الرقمية

الإشارة إلى بعض المفاهيم:

- **القيادة الرقمية:** هي نهج إداري يعتمد على استخدام التكنولوجيا الرقمية لتمكين الفرق، تحسين الأداء، وتعزيز الابتكار، من أجل تحقيق أهداف المؤسسة.
- **الرؤية الرقمية:** هي تصور استراتيجي يحدد كيفية استخدام التكنولوجيا الرقمية لتحقيق الأهداف المستقبلية للمؤسسة، من خلال الابتكار، التحول الرقمي، وتحسين الكفاءة والخدمات.
- **المعرفة الرقمية:** هي القدرة على فهم واستخدام وتقييم التكنولوجيا والبيانات الرقمية بفعالية وأمان.

الرجاء الإجابة على العبارات الآتية بوضع علامة (x) في الخانة المراد اختيارها:

	الرقم	العبارات	درجة الموافقة				
			موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
بعد الابتكار الرقمي	01	يساهم الابتكار الرقمي في تحسين جودة الخدمات الرقمية التي يقدمها البنك لعملائه؛					
	02	تعد التقنيات الحديثة ضرورية لدعم الابتكار الرقمي في القطاع البنكي؛					
	03	تعزز البرمجيات الحديثة قدرة البنك على المنافسة في السوق؛					
	04	يسمح البنك للموظفين بتقديم اقتراحات لتطوير تقنيات حديثة وحلول بنكية جديدة؛					
	05	يدعم البنك الابتكار الرقمي بتخصيص الموارد اللازمة له؛					
بعد الرؤية الرقمية	06	يحرص البنك على مواكبة الابتكارات الرقمية لضمان تحقيق رؤيته المستقبلية لتعزيز موقعه التنافسي في السوق؛					
	07	تلتزم قيادة البنك بتطوير استراتيجيات رقمية تتماشى مع متطلبات السوق البنكي الحديث؛					

	08	يحرص قادة البنك على توظيف البيانات وتحليلها رقمياً لدعم اتخاذ القرارات الإستراتيجية التي تتماشى مع الرؤية الرقمية للبنك؛						
	09	يستخدم البنك تقنيات وبرمجيات رقمية حديثة من أجل التكيف مع التحديات الرقمية؛						
	10	يركز البنك على تحسين تجربة العملاء من خلال استخدام التقنيات والبرمجيات الرقمية المبتكرة؛						
بعد المعرفة الرقمية	11	يستقطب البنك أشخاص بكفاءات عالية متمكنة من استخدام التقنيات والبرمجيات الحديثة؛						
	12	توفر قيادة البنك برامج تدريبية لتعزيز المعرفة الرقمية لدى الموظفين؛						
	13	يتمتع قادة البنك بالمعرفة الرقمية الكافية لتوجيه عمليات التحول الرقمي بفعالية؛						
	14	تحرص قيادة البنك على تطوير مهاراتها الرقمية لمواكبة التطورات في القطاع البنكي؛						
	15	تستند استراتيجيات البنك إلى المعرفة الرقمية لتوجيه الابتكار وتحقيق أهداف التحول الرقمي؛						
بعد المشاركة والتعاون	16	توفر القيادة الرقمية في البنك قنوات اتصال فعالة لتعزيز تبادل المعارف الرقمية بين أصحاب المصلحة؛						
	17	يدعم البنك بيئة عمل تعاونية تعتمد على الأدوات الرقمية لزيادة الإنتاجية وتحسين الأداء؛						
	18	تساهم ثقافة المشاركة الرقمية في تحسين جودة الخدمات البنكية المقدمة للعملاء؛						
	19	يعمل البنك على تعزيز الشراكات مع المؤسسات التكنولوجية لتطوير حلول رقمية مبتكرة؛						
	20	يشجع البنك موظفيه على تبادل الخبرات الرقمية والمساهمة في مبادرات التحول الرقمي.						

الجزء الثاني: الأمن السيبراني

هو مجموعة من الممارسات والتقنيات المصممة لحماية الأنظمة، والشبكات، والبرمجيات، والبيانات من الهجمات الإلكترونية أو الاختراقات غير المصرح بها. يهدف الأمن السيبراني إلى ضمان سرية المعلومات وسلامتها وتوافرها، مما يحمي المؤسسات والأفراد من التهديدات الرقمية مثل الفيروسات، والبرمجيات الخبيثة، وهجمات التصيد الاحتيالي، والاختراقات.

الرجاء الإجابة على العبارات الآتية بوضع علامة (x) في الخانة المراد اختيارها:

الرقم	العبارات	درجة الموافقة				
		موافق تماما	موافق	محايد	غير موافق	غير موافق تماما
21	يمتلك البنك الوعي الكافي بالمخاطر السيبرانية التي قد تهدد أنظمته؛					
22	يتبع البنك إجراءات وقائية فعالة لمواجهة الهجمات السيبرانية؛					
23	يطبق البنك سياسات واضحة ومحدثة للأمن السيبراني؛					
24	يعتمد البنك على آليات رصد وسياسات أمنية فعالة للحد من التهديدات السيبرانية؛					
25	يعتمد البنك تقنيات تشفير معترف بها عالمياً لحماية بيانات العملاء؛					
26	يتم تطبيق التحقق المزدوج، مثل رموز التحقق لضمان الوصول الأمن إلى الأنظمة البنكية؛					
27	تقلل سياسات الأمان الرقمي، مثل التشفير والمراقبة، من مخاطر الاختراقات وتسريب البيانات؛ مما يعزز ثقة العملاء؛					
28	تساهم استراتيجيات الأمن السيبراني في تعزيز مكانة البنك في السوق المالية وتحقيق الاستدامة المالية؛					
29	تساهم الاستثمارات المستمرة في الأمن السيبراني في تحسين كفاءة العمليات المصرفية وضمان استمراريتها؛					

30	يمثل الانتقال إلى البنية الرقمية تحدياً رئيسياً للبنك بسبب صعوبة تحديث الأنظمة التقليدية لمواكبة التطورات الأمنية؛					
31	يعاني البنك من نقص في الموارد البشرية المؤهلة لتنفيذ استراتيجيات الأمن السيبراني؛					
32	يواجه البنك مشكلة عدم ثقة العملاء وتخوفهم من الهجمات السيبرانية؛					
33	يعاني البنك من مشاكل بسبب ضعف الأنظمة القانونية التي توفرها الدولة في مجال الأمن السيبراني؛					
34	يواجه البنك تحدياً في الموازنة بين تعزيز الأمن السيبراني وتسهيل الخدمات الرقمية المقدمة.					

الملحق رقم (03): مقابلة مع موظف إطار ببنك الجزائر الخارجي BEA وكالة تبسة -46-

س1: كيف تقيّمون مستوى القيادة الرقمية داخل الوكالة؟

ج1: القيادة الرقمية في الوكالة لا تزال في مراحلها الأولى، مع وجود بعض المبادرات لتحديث أساليب التسيير باستخدام التكنولوجيا، لكنها تحتاج إلى مزيد من الدعم والانتشار.

س2: هل ترون أن الإدارة تعتمد على أدوات رقمية في التسيير واتخاذ القرار؟

ج2: نعم، هناك استخدام لبعض الأدوات الرقمية خاصة في التقارير الداخلية ومتابعة الأداء، لكن الاعتماد الكلي لا يزال محدودًا.

س3: ما هي أبرز التحديات التي تواجه القادة عند استخدام الحلول الرقمية؟

ج3: من أبرز التحديات ضعف التكوين في المجال الرقمي، ومقاومة بعض الموظفين للتغيير، إضافة إلى نقص التجهيزات التقنية.

س4: هل توفر الإدارة تكوينات رقمية للعاملين؟ وما مضمونها؟

ج4: نعم، يتم تقديم دورات في الأمن السيبراني والتعامل مع الأنظمة الرقمية، لكن بوتيرة غير منتظمة وبحاجة للتحديث المستمر.

س5: ما مدى تأثير القيادة الرقمية في تحسين الأداء الوظيفي للموظفين؟

ج5: لها تأثير إيجابي من حيث تسهيل إنجاز المهام وتقليل الأخطاء، لكنها تحتاج إلى متابعة وتقييم فعّال من طرف الإدارة.

س6: هل يتم إشراك الموظفين في قرارات تتعلق بالتحول الرقمي داخل الوكالة؟

ج6: المشاركة محدودة، وغالبًا ما تكون القرارات مركزية، مما يحد من تفاعل الموظفين مع التغييرات الرقمية

س7: ما هي السياسات المعتمدة لتعزيز ثقافة الأمن السيبراني داخل الوكالة؟

ج7: توجد تعليمات دورية، مع وجود إجراءات أمنية تخص كلمات المرور والدخول للأنظمة، لكن لا توجد سياسة موحدة ومكتوبة بوضوح.

س8: كيف يتم توعية العاملين بمخاطر الهجمات السيبرانية؟

ج8: من خلال بعض النشرات الداخلية والدورات التكوينية، لكن الوعي لا يزال غير كافٍ لدى الجميع.

س9: هل هناك دور واضح للقيادة في تعزيز الالتزام بالممارسات الآمنة رقمياً؟

ج9: نعم، هناك محاولات من طرف المسؤولين لتشجيع الالتزام، لكن ذلك يتفاوت بين قسم وآخر حسب وعي المسؤول.

س10: ما مدى التزام العاملين بإجراءات الأمن السيبراني (كلمات مرور، برامج حماية، الخ)؟

ج10: الالتزام جيد نسبيًا، لكن بعض التصرفات الفردية مثل مشاركة كلمات المرور لا تزال تحدث أحيانًا.

س11: برأيكم، هل توجد علاقة مباشرة بين جودة القيادة الرقمية ومستوى الأمن السيبراني؟

ج11: نعم، فكلما كانت القيادة واعية ومدعومة رقمياً، ساهم ذلك في رفع مستوى الوعي والانضباط في المجال السيبراني.

س12: ما أهم الآليات المقترحة لتعزيز هذا الارتباط بين القيادة الرقمية والأمن السيبراني؟

ج12: تكثيف التكوينات، اعتماد سياسات رقمية واضحة، وتحفيز الموظفين على تبني السلوكيات الرقمية الآمنة.

س13: هل لديكم توصيات لتطوير القيادة الرقمية بما يخدم حماية نظم المعلومات؟

ج13: نعم، من الضروري اعتماد خطة رقمية إستراتيجية، وتكوين قادة رقميين في كل قسم، إضافة إلى تخصيص ميزانية لتحديث البنية التحتية الرقمية.

الملحق رقم (04): مخرجات برنامج Spss

أولا: التحليل الإحصائي للبيانات الشخصية

المستوى_العلمي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	ثانوي أو أقل	4	17,4	17,4	17,4
	شهادات جامعية	15	65,2	65,2	82,6
	شهادات أخرى	4	17,4	17,4	100,0
	Total	23	100,0	100,0	

المركز_الوظيفي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	قائد	4	17,4	17,4	17,4
	رئيس مصلحة	3	13,0	13,0	30,4
	مكلف بالزبائن	7	30,4	30,4	60,9
	وظيفة أخرى	9	39,1	39,1	100,0
	Total	23	100,0	100,0	

الخبرة_المهنية

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	أقلمن 5 سنوات	6	26,1	26,1	26,1
	من 5 إلى 10 سنوات	6	26,1	26,1	52,2
	من 11 سنة إلى 15 سنة	4	17,4	17,4	69,6
	أكثر من 15 سنة	7	30,4	30,4	100,0
	Total	23	100,0	100,0	

ثانيا: التحليل الوصفي لمتغيرات الدراسة

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
يساهم الابتكار الرقمي في تحسين جودة الخدمات الرقمية التي يقدمها البنك لعملائه؛	23	4,00	5,00	4,3478	,48698
تعد التقنيات الحديثة ضرورية لدعم الابتكار الرقمي في القطاع البنكي؛	23	1,00	5,00	4,3043	1,01957
تعزز البرمجيات الحديثة قدرة البنك على المنافسة في السوق؛	23	2,00	5,00	4,3478	,83168

يسمح البنك للموظفين بتقديم اقتراحات لتطوير تقنيات حديثة وحلول بنكية جديدة؛	23	2,00	5,00	3,6957	,87567
يدعم البنك الابتكار الرقمي بتخصيص الموارد اللازمة له؛	23	2,00	5,00	3,8261	,83406
يحرص البنك على مواكبة الابتكارات الرقمية لضمان تحقيق رؤيته المستقبلية لتعزيز موقعه التنافسي في السوق؛	23	2,00	5,00	4,2609	,81002
تلتزم قيادة البنك بتطوير استراتيجيات رقمية تتماشى مع متطلبات السوق البنكي الحديث؛	23	2,00	5,00	3,8696	,54808
يحرص قادة البنك على توظيف البيانات وتحليلها رقمياً لدعم اتخاذ القرارات الإستراتيجية التي تتماشى مع الرؤية الرقمية للبنك؛	23	1,00	5,00	3,7391	,86431
يستخدم البنك تقنيات وبرمجيات رقمية حديثة من أجل التكيف مع التحديات الرقمية؛	23	2,00	5,00	3,9130	1,08347
يركز البنك على تحسين تجربة العملاء من خلال استخدام التقنيات والبرمجيات الرقمية المبتكرة؛	23	1,00	5,00	3,8696	,91970
يستقطب البنك أشخاص بكفاءات عالية متمكنة من استخدام التقنيات والبرمجيات الحديثة؛	23	2,00	5,00	4,0000	,79772
يستقطب البنك أشخاص بكفاءات عالية متمكنة من استخدام التقنيات والبرمجيات الحديثة؛	23	2,00	5,00	4,0435	,92826
توفر قيادة البنك برامج تدريبية لتعزيز المعرفة الرقمية لدى الموظفين؛	23	3,00	5,00	4,2609	,81002
تحرص قيادة البنك على تطوير مهاراتها الرقمية لمواكبة التطورات في القطاع البنكي؛	23	1,00	5,00	3,9565	,92826
تستند استراتيجيات البنك إلى المعرفة الرقمية لتوجيه الابتكار وتحقيق أهداف التحول الرقمي؛	23	2,00	5,00	4,2174	,95139
توفر القيادة الرقمية في البنك قنوات اتصال فعالة لتعزيز تبادل المعارف الرقمية بين أصحاب المصلحة؛	23	2,00	5,00	3,9130	,90015
يدعم البنك بيئة عمل تعاونية تعتمد على الأدوات الرقمية لزيادة الإنتاجية وتحسين الأداء؛	23	3,00	5,00	4,0435	,70571
تساهم ثقافة المشاركة الرقمية في تحسين جودة الخدمات البنكية المقدمة للعملاء؛	23	3,00	5,00	4,1304	,69442
يعمل البنك على تعزيز الشراكات مع المؤسسات التكنولوجية لتطوير حلول رقمية مبتكرة؛	23	1,00	5,00	3,7826	,99802
يشجع البنك موظفيه على تبادل الخبرات الرقمية والمساهمة في مبادرات التحول الرقمي.	23	1,00	5,00	3,9130	1,16436
الابتكار_الرقمي	23	3,20	5,00	4,1043	,50043
الرؤية_الرقمية	23	2,40	5,00	3,9304	,60785
المعرفة_الرقمية	23	2,80	5,00	4,0957	,62920
المشاركة_والتعاون	23	2,40	5,00	3,9565	,72603
القيادة_الرقمية	23	3,00	5,00	4,0217	,52067
N valide (liste)	23				

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
يمتلك البنك الوعي الكافي بالمخاطر السيبرانية التي قد تهدد أنظمته؛	23	3,00	5,00	4,3478	,71406
يتبع البنك إجراءات وقائية فعالة لمواجهة الهجمات السيبرانية؛	23	3,00	5,00	4,0435	,87792
يطبق البنك سياسات واضحة ومحدثة للأمن السيبراني؛	23	2,00	5,00	3,8696	1,05763
يعتمد البنك على آليات رصد وسياسات أمنية فعالة للحد من التهديدات السيبرانية؛	23	2,00	5,00	4,0870	,94931
يعتمد البنك تقنيات تشفير معترف بها عالمياً لحماية بيانات العملاء؛	23	1,00	5,00	3,8261	1,26678
يتم تطبيق التحقق المزدوج، مثل رموز التحقق لضمان الوصول الأمن إلى الأنظمة البنكية؛	23	2,00	5,00	3,8696	,91970
تقلل سياسات الأمان الرقمي، مثل التشفير والمراقبة، من مخاطر الاختراقات وتسريب البيانات؛ مما يعزز ثقة العملاء؛	23	3,00	5,00	4,0435	,76742
تساهم استراتيجيات الأمن السيبراني في تعزيز مكانة البنك في السوق المالية وتحقيق الاستدامة المالية؛	23	2,00	5,00	3,9565	,82453
تساهم الاستثمارات المستمرة في الأمن السيبراني في تحسين كفاءة العمليات المصرفية وضمان استمراريتها؛	23	2,00	5,00	3,6522	,83168
يمثل الانتقال إلى البنية الرقمية تحدياً رئيسياً للبنك بسبب صعوبة تحديث الأنظمة التقليدية لمواكبة التطورات الأمنية؛	23	3,00	5,00	4,1739	,65033
يعاني البنك من نقص في الموارد البشرية المؤهلة لتنفيذ استراتيجيات الأمن السيبراني؛	23	2,00	5,00	3,4348	1,07982
يواجه البنك مشكلة عدم ثقة العملاء وتخوفهم من الهجمات السيبرانية؛	23	2,00	5,00	3,4348	1,16096
يعاني البنك من مشاكل بسبب ضعف الأنظمة القانونية التي توفرها الدولة في مجال الأمن السيبراني؛	23	1,00	5,00	3,3043	1,32921
يواجه البنك تحدياً في الموازنة بين تعزيز الأمن السيبراني وتسهيل الخدمات الرقمية المقدمة.	23	2,00	5,00	3,7391	,91539
الأمن_السيبراني	23	2,71	5,00	3,8416	,63412
N valide (liste)	23				

ثالثا: نتائج الارتباط بيرسون

Corrélations

		الابتكار_الرقمي	الرؤية_الرقمية	المعرفة_الرقمية	المشاركة_والتعاون	القيادة_الرقمية
الابتكار_الرقمي	Corrélation de Pearson	1	,694**	,596**	,664**	,854**
	Sig. (bilatérale)		,000	,003	,001	,000
	N	23	23	23	23	23
الرؤية_الرقمية	Corrélation de Pearson	,694**	1	,593**	,776**	,908**
	Sig. (bilatérale)	,000		,003	,000	,000
	N	23	23	23	23	23
المعرفة_الرقمية	Corrélation de Pearson	,596**	,593**	1	,412	,762**
	Sig. (bilatérale)	,003	,003		,051	,000
	N	23	23	23	23	23
المشاركة_والتعاون	Corrélation de Pearson	,664**	,776**	,412	1	,859**
	Sig. (bilatérale)	,001	,000	,051		,000
	N	23	23	23	23	23
القيادة_الرقمية	Corrélation de Pearson	,854**	,908**	,762**	,859**	1
	Sig. (bilatérale)	,000	,000	,000	,000	
	N	23	23	23	23	23

**. La corrélation est significative au niveau 0.01 (bilatéral).

Corrélations

		القيادة_الرقمية	الأمن	الاستبيان_ككل
القيادة_الرقمية	Corrélation de Pearson	1	,801**	,938**
	Sig. (bilatérale)		,000	,000
	N	23	23	23
الأمن_السيبراني	Corrélation de Pearson	,801**	1	,959**
	Sig. (bilatérale)	,000		,000
	N	23	23	23
الاستبيان_ككل	Corrélation de Pearson	,938**	,959**	1
	Sig. (bilatérale)	,000	,000	
	N	23	23	23

**. La corrélation est significative au niveau 0.01 (bilatéral).

رابعا: نتائج ألفا كرونباج

للاستبيان ككل

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,943	34

الابتكار الرقمي

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,565	5

الرؤية الرقمية

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,746	5

المعرفة الرقمية

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,755	5

المشاركة والتعاون

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,857	5

القيادة الرقمية

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,905	20

الأمن السيبراني

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
,896	14

خامسا: اعتدالية التوزيع (توزيع طبيعي)

Test Kolmogorov-Smirnov pour un échantillon

		الأمن_السيبراني	القيادة_الرقمية	الاستبيان_ككل
N		23	23	23
Paramètres normaux[a,b]	Moyenne	3,8416	4,0217	3,9317
	Ecart type	,63412	,52067	,54822
Différences les plus extrêmes	Absolue	,125	,163	,115
	Positif	,125	,112	,111
	Négatif	-,116	-,163	-,115
Statistiques de test		,125	,163	,115
Sig. asymptotique (bilatérale)		,200[c,d]	,118[c]	,200[c,d]

a. La distribution du test est Normale.

b. Calculée à partir des données.

c. Correction de signification de Lilliefors.

d. Il s'agit de la borne inférieure de la vraie signification.

سادسا: اختبار فرضيات الدراسة

اختبار الفرضيات الفرعية للفرضية الرئيسية الأولى

اختبار الفرضية الفرعية الأولى

Variables introduites/éliminées[a]

Modèle	Variables introduites	Variables éliminées	Méthode
1	الابتكار_الرقمي[b]	.	Introduire

a. Variable dépendante : الأمن

b. Toutes les variables demandées ont été introduites.

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,693[a]	,480	,455	,46800

a. Prédicteurs : (Constante), الرقمي_الابتكار

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	4,247	1	4,247	19,391	,000[b]
	de Student	4,599	21	,219		
	Total	8,846	22			

a. Variable dépendante : الأمن

b. Prédicteurs : (Constante), الرقمي_الابتكار

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés		
		B	Erreur standard	Bêta	t	Sig.
1	(Constante)	,238	,824		,289	,775
	الرقمي_الابتكار	,878	,199	,693	4,403	,000

a. Variable dépendante : الأمن

اختبار الفرضية الفرعية الثانية

Variables introduites/éliminées[a]

Modèle	Variables introduites	Variables éliminées	Méthode
1	الرقمية_الرؤية[b]	.	Introduire

a. Variable dépendante : الأمن

b. Toutes les variables demandées ont été introduites.

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,695[a]	,482	,458	,46698

a. Prédicteurs : (Constante), الرقمية_الرؤية

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	4,267	1	4,267	19,567	,000[b]
	de Student	4,579	21	,218		
	Total	8,846	22			

a. Variable dépendante : الأمن

b. Prédicteurs : (Constante), الرقمية_الرؤية

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés		
		B	Erreur standard	Bêta	t	Sig.
1	(Constante)	,994	,651		1,527	,142
	الرقمية_الرؤية	,725	,164	,695	4,424	,000

a. Variable dépendante : الأمن

اختبار الفرضية الفرعية الثالثة

Variables introduites/éliminées[a]

Modèle	Variables introduites	Variables éliminées	Méthode
1	الرقمية_المعرفة[b]	.	Introduire

a. Variable dépendante : الأمن

b. Toutes les variables demandées ont été introduites.

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,507[a]	,257	,221	,55952

a. Prédicteurs : (Constante), الرقمية_المعرفة

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	2,272	1	2,272	7,257	,014[b]
	de Student	6,574	21	,313		
	Total	8,846	22			

a. Variable dépendante : الأمن

b. Prédicteurs : (Constante), الرقمية_المعرفة

Coefficients[a]

Modèle		Coefficients non standardisés		Coefficients standardisés	t	Sig.
		B	Erreur standard	Bêta		
1	(Constante)	1,750	,785		2,228	,037
	الرقمية_المعرفة	,511	,190	,507	2,694	,014

a. Variable dépendante : الأمن

اختبار الفرضية الفرعية الرابعة

Variables introduites/éliminées[a]

Modèle	Variables introduites	Variables éliminées	Méthode
1	والتعاون_المشاركة[b]	.	Introduire

a. Variable dépendante : الأمن

b. Toutes les variables demandées ont été introduites.

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,800[a]	,639	,622	,38978

a. Prédicteurs : (Constante), والتعاون_المشاركة

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	5,656	1	5,656	37,228	,000[b]
	de Student	3,190	21	,152		
	Total	8,846	22			

a. Variable dépendante : الأمن

b. Prédicteurs : (Constante), والتعاون_المشاركة

Coefficients[a]

Modèle		Coefficients non standardisés B	Erreur standard	Coefficients standardisés Bêta	t	Sig.
1	(Constante)	1,078	,460		2,344	,029
	والتعاون_المشاركة	,698	,114	,800	6,101	,000

a. Variable dépendante : الأمن

اختبار الفرضية الفرعية للفرضية الرئيسية الثانية

اختبار الفرضية الفرعية الأولى

ANOVA

المستوى_التعليمي

	Somme des carrés	ddl	Carré moyen	F	Sig.
Intergroupes	1,192	2	,596	2,199	,137
Intragroupes	5,420	20	,271		
Total	6,612	22			

اختبار الفرضية الفرعية الثانية

ANOVA

المركز_الوظيفي

	Somme des carrés	ddl	Carré moyen	F	Sig.
Intergroupes	,461	3	,154	,474	,704
Intragroupes	6,151	19	,324		
Total	6,612	22			

اختبار الفرضية الفرعية الثالثة

ANOVA

الخبرة_المهنية

	Somme des carrés	ddl	Carré moyen	F	Sig.
Intergroupes	1,232	3	,411	1,450	,260
Intragroupes	5,380	19	,283		
Total	6,612	22			

اختبار الفرضية الرئيسية الأولى والثانية

Variables introduites/éliminées[a]

Modèle	Variables introduites	Variables éliminées	Méthode
1	القيادة_الرقمية[b]	.	Introduire

a. Variable dépendante : الأمن

b. Toutes les variables demandées ont été introduites.

Récapitulatif des modèles

Modèle	R	R-deux	R-deux ajusté	Erreur standard de l'estimation
1	,801[a]	,642	,625	,38853

a. Prédicteurs : (Constante), الرقمية_القيادة

ANOVA[a]

Modèle		Somme des carrés	ddl	Carré moyen	F	Sig.
1	Régression	5,676	1	5,676	37,602	,000[b]
	de Student	3,170	21	,151		
	Total	8,846	22			

a. Variable dépendante : الأمن

b. Prédicteurs : (Constante), الرقمية_القيادة

Coefficients[a]

Modèle		Coefficients non standardisés B	Erreur standard	Coefficients standardisés Bêta	t	Sig.
1	(Constante)	,082	,645		,127	,900
	الرقمية_القيادة	,976	,159	,801	6,132	,000

a. Variable dépendante : الأمن

الملحق رقم (05): اتفاقية التربص

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتنظيم

إتفاقية التربص

الرقم...../2024

المادة الاولى: هذه الاتفاقية تضبط علاقة جامعة الشهيد الشيخ العربي التبسي -تبسة- ممثلة من طرف عميد كلية العلوم الاقتصادية العلوم التجارية وعلوم التسيير.

مع المؤسسة: بنك الجزائر الخارجي BEA - ف تبسة -

مقرها: - تبسة -

ممثلة من طرف: Mr. MOSLEM Noureddine Directeur Agence BEA Tébéssa 046 الوظيفة:

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسماؤهم:

1- دوالي سمير 2- زيطاري ايمان

ماستر التخصص إدارة أعمال

عنوان المذكرة: أثر القيادة الرقمية على تعزيز سلوك الأمن السيبراني في المؤسسات المالية

الاستاذ المشرف: أويسي هبة الله

هذه الاتفاقية تهدف الى تنظيم تربص تطبيقي للطلبة الاتية أسماؤهم

1-.....2-.....3

4.....5-.....

ليسانس التخصص .....

عنوان تقرير التربص: .....

الاستاذ المشرف: .....

وذلك طبقا للمرسوم رقم: 88-90 المؤرخ في: 1988/05/03 القرار الوزاري المؤرخ في ماي 1989.

المادة الثانية : يهدف هذا التربص الى ضمان تطبيق الدراسات المعطاة في القسم والمطابقة للبرنامج والمخططات التعليمية في تخصص الطلبة المعنيين

المادة الثالثة :التربص التطبيقي يجرى في مصلحة

.....

الفترة من 2025/04/17 الى 2025/03/16

المادة الرابعة : برنامج التربص المعد من طرف الكلية مراقب عند تنفيذه من طرف جامعة تبسة والمؤسسة المعنية.

المادة الخامسة :

وعلى غرار ذلك تتكفل المؤسسة بتعيين عون أو أكثر بمتابعة تنفيذ التربص التطبيقي هؤلاء الاشخاص مكلفون أيضا بالحصول على المسابقات الضرورية للتنفيذ الامثل للتنفيذ الامثل للبرنامج وكل غياب للمتربص ينبغي أن يكون على استمارة السيرة الذاتية المسلمة من طرف الكلية.

المادة السادسة:خلال التربص التطبيقي والمحدد بثلاثين يوما يتبع المتربص مجموع الموظفين في وحداته المحددة في النظام الداخلي وعليه يحسب على المؤسسة أن توضع للطلبة عند وصولهم أماكن تربصهم مجموع التدابير المتعلقة بالنظام الداخلي في مجال الامن والنظافة وتبين لهم الاخطاء الممكنة.

المادة السابعة: في حالة الاخلال بهذه القواعد فالمؤسسة لها الحق في انهاء تربص الطالب بعد إعلام القسم عن طريق رسالة مسجلة ومؤمنة الوصول.

المادة الثامنة: تأخذ المؤسسة كل التدابير لحماية المتربص ضد مجموع مخاطر حوادث العمل وتسهر بالخصوص على تنفيذ كل تدابير النظافة والأمن المتعلقة بمكان العمل المعين لتنفيذ التربص.

المادة التاسعة: في حالة حادث ما على المتربصين بمكان التوجيه يجب على المؤسسة أن تلجأ الى العلاج الضروري كما يجب أن ترسل تقريرا مفصلا مباشرة الى القسم.

المادة العاشرة :تتحمل المؤسسة التكفل بالطلبة في حدود إمكانياتها وحسب محمل الاتفاقية الموقعة بين الطرفين عند الوجوب وإلا فإن الطلبة يتكفلون بأنفسهم من ناحية النقل ، المسكن ، المطعم.

ادارة القسم

رئيس قسم علوم التسيير

جدي شوقي

ادارة المؤسسة المستقبلة

Mr. MOSLEM Noureddine
Directeur Agence
BEA Tébessa 046

الملحق رقم (06): إذن بالطبع لمذكرة التخرج ماستر

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي -تبسة-

كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير
نيابة عمادة الكلية مكلفة بالدراسات والمسائل المرتبطة بالطلبة
مصلحة التعليم والتقييم

إذن بالطبع لمذكرة التخرج ماستر /تقارير التربص ليسانس

أنا الممضي أسفله الاستاذ (ة) :...حبيبة الأخضر تريسي....

المشرف على مذكرة التخرج: ماستر / تقرير تربص لسانس للسنة الجامعية : 2025/2024

فئة ليسانس

فريق العمل	الاختصاص	عنوان التقرير بالتفصيل
-1*		
-2*		
-3*		
-4*		
-5*		

فئة الماستر

فريق العمل	الاختصاص	عنوان المذكرة بالتفصيل
-1* إيمان زيطاري	علوم التسيير	أثر القيادة الرحيمة على تعزيز سلوك الأمن السيبراني في المؤسسات المالية
-2* سمير دوالي		

أوافق على تقديم المذكرة أو تقرير التربص وهذا بعد المراجعة الكاملة .

اللقب والاسم للاستاذ المشرف	الامضاء	تاريخ الامضاء
حبيبة الأخضر تريسي		2025/05/14

الادارة

ملخص الدراسة

ملخص

هدفت هذه الدراسة إلى تحليل أثر القيادة الرقمية بأبعادها المختلفة (الابتكار الرقمي، الرؤية الرقمية، المعرفة الرقمية، المشاركة والتعاون)، على تعزيز سلوك الأمن السيبراني لدى موظفي بنك الجزائر الخارجي BEA وكالة تبسة -46-. وقد اعتمدت الدراسة على المنهج الوصفي في الفصل النظري، ومنهج دراسة الحالة مستعيني ن بالمنهج التحليلي في فصل الدراسة الميدانية ، وتم جمع البيانات باستخدام أداة الاستبيان من عينة شملت 23 موظفًا من مختلف المستويات الإدارية . تم تحليل البيانات باستخدام برنامج SPSS بالاعتماد على أساليب الإحصاء الوصفي والانحدار البسيط لاختبار الفرضيات. وأظهرت نتائج التحليل الإحصائي وجود علاقة تأثير إيجابية ذات دلالة إحصائية بين القيادة الرقمية بجميع أبعادها وسلوك الأمن السيبراني . كما كشفت الدراسة عن وجود فروق ذات دلالة إحصائية في إدراك الموظفين لأثر القيادة الرقمية على الأمن السيبراني تعزى لمتغيرات كالمؤهل العلمي والمنصب الوظيفي والخبرة المهنية.

وفي ختام الدراسة، تم تقديم مجموعة من النتائج النظرية والتطبيقية، بالإضافة إلى توصيات تهدف إلى تعزيز أنماط القيادة الرقمية وترسيخ سلوك الأمن السيبراني في المؤسسات المالية.

الكلمات المفتاحية: القيادة الرقمية، الأمن السيبراني، المشاركة الرقمية، الرؤية الرقمية، المعرفة الرقمية، الابتكار الرقمي، المؤسسة المالية.

Abstract

This study aimed to analyze the impact of digital leadership and its various dimensions (digital innovation, digital vision, digital knowledge, and collaboration), on enhancing cybersecurity behavior among employees of the Banque Extérieure d'Algérie (BEA) Tebessa Branch -46-. The study adopted a descriptive approach in the theoretical chapter, a case study method, and an analytical approach in the field study chapter. Data were collected through a questionnaire administered to a sample of 23 employees from various administrative levels. The data were analyzed using the SPSS software, employing descriptive statistics and simple linear regression to test the hypotheses. The results of the statistical analysis revealed a positive and statistically significant relationship between digital leadership in all its dimensions and cybersecurity behavior. The study also found statistically significant differences in employees' perceptions of the impact of digital leadership on cybersecurity behavior, which were attributed to factors such as educational qualification, job position, and professional experience. In conclusion, the study presented a set of theoretical and practical findings, along with recommendations aimed at promoting digital leadership styles and strengthening cybersecurity behavior within financial institutions.

Keywords: Digital Leadership, Cybersecurity, Digital Collaboration, Digital Vision, Digital Knowledge, Digital Innovation, Financial Institution.