التوجه نحو تطبيق الإدارة الرقمية كآلية لتحقيق الأمن المعلوماتي بالمؤسسة –دراسة حالة مؤسسة اتصالات الجزائر وكالة خنشلة-

Orientation towards implementing digital management as a mechanism to achieve The information security in the institution – Case study: Algeria Telecom, Khenchela Agency

راضية عروف *

مخبر حاضنات المؤسسات والتنمية المحلية، جامعة خنشلة– الجزائر

Radiaarrouf@yahoo.com

تاريخ الإستلام: 2025/07/10 تاريخ القبول: 2025/09/10 تاريخ النشر: 2025/11/22

ملخص:

هدفت هذه الدراسة إلى التعرف على دور التوجه نحو تطبيق الإدارة الرقمية كآلية لتحقيق وتعزيز أمن المعلومات من خلال تطبيق سياسات، استراتيجيات وتقنيات متقدمة، ومنه فقد سعت وحتمية مختلف القطاعات الاقتصادية إلى رقمنة إداراتها ومنها قطاع الاتصالات الذي يعتبر من بين القطاعات الحساسة التي تحتاج طبيعة نشاطها إلى التحديث الدائم وفق التغيرات التكنولوجية، ولذلك فقد تمت الدراسة بمؤسسة اتصالات الجزائر وكالة خنشلة-، بحيث تكونت عينة الدراسة من (30) فرد، وأظهرت النتائج أن هناك علاقة قوية موجبة بين المتغيرين (الإدارة الرقمية وأمن المعلومات)، غير أن تعزيز هذه العلاقة يتطلب الاستثمار الفعال في التكنولوجيا وتوفير بنية تحتية داعمة وتوفير برامج تدريبية للموظفين من أجل تعزيز أمن المعلومات داخل المؤسسة.

الكلمات المفتاحية: الإدارة الرقمية، أمن المعلومات، التكنولوجيا، الاستثمار البشري، مؤسسة اتصالات الجزائر

تصنيف JEL: M15 ، L86، O33، L96 ، J24 .

Abstract: This study aimed to identify the role of the shift toward implementing digital management as a mechanism for achieving and enhancing information security through the application of advanced policies, strategies, and technologies. As a result, various economic sectors have found it necessary to digitize their administrative processes, including the telecommunications sector, which is considered one of the most sensitive sectors due to the nature of its operations that require constant updates in line with technological changes. Therefore, the study was conducted at the Algeria Telecom Company – Khenchela Agency, with a sample of 30 individuals. The results showed a strong positive relationship between the two variables (digital management and information security). However, strengthening this relationship requires effective investment in technology, the provision of supportive infrastructure, and the implementation of training programs for employees to enhance information security within the institution.

Keywords: Digital management, information security, technology, human investment, Algeria Telecom.

Jel Classification Codes: M15 ، L86 ، O33 ، L96،. J24.

* المؤلف المراسل.

1. مقدمة:

في ظل التطور السريع الذي يشهده العالم في عصر التكنولوجيا الرقمية، فقد عرف تقدما متسارعا نتيجة تراكم في الثروة المعلوماتية، مما أدى إلى تغييرات جذرية في طرق العمل والتواصل وتبادل المعلومات وظهور أساليب وتقنيات جديدة في كل القطاعات والمجالات خاصة مجال الإدارة الذي يعتبر المحرك الأساسي لسير مختلف العمليات والوظائف داخل المؤسسات. لأنها تساهم بدورها في تحسين أداء العاملين من خلال توفير تقنيات حديثة لتسهيل مختلف وظائفها الإدارية وتوفير بيئة عمل مريحة وداعمة تمتاز بالشفافية وروح الفريق، الأمر الذي فرض على المؤسسات إحداث تغييرات للتكيف مع التطورات المتلاحقة من أبرزها التخلي عن قوالب الإدارة النمطية وتبني أنماط إدارية حديثة وتطبيقها لمساعدتها على التأقلم والتعامل في الأوضاع الديناميكية سريعة التحول.

ومع تزايد الاعتماد على الأنظمة الرقمية، ساعدت التكنولوجيا الحديثة على تبسيط الإجراءات وتقليل استخدام الورق إلى أقل ما يمكن لكسب الوقت وتوفير الجهد والتكلفة، حيث أصبح أمن المعلومات من القضايا الحيوية التي تواجه المؤسسات على حد سواء وذلك لضمان سلامة البيانات والمعلومات خاصة الحساسة منها، إذ تبرز الحاجة الملحة إلى تطوير آليات فعالة لحمايتها من مختلف المخاطر والتهديدات. وهنا تلعب الإدارة الرقمية، دورا محوريا في تعزيز أمن المعلومات من خلال تطبيق استراتيجيات وسياسات أمنية متطورة مثل: تشفير البيانات الحساسة كأحد الأساليب الفعالة لحماية المعلومات أثناء النقل والتخزين، التحديثات الدورية للبرامج والتطبيقات، وتفعيل أنظمة للكشف عن التسلل، كما تلعب الإدارة الرقمية دور في تعزيز أمن المعلومات بين الموظفين، من خلال توفير التدريب والدعم مما يضمن تحقيق أعلى مستويات الأمان للبيانات داخل المؤسسة، حيث أن الإدارة تعمل على مراقبة الأنشطة المشبوهة واستخدام تقنيات الكشف عن الهجمات والتهديدات الخارجية المتزايدة.

كذلك فإن الإدارة الرقمية هي التي تستشرف مستقبل المؤسسة وبناء إستراتيجيتها بواسطة التكنولوجيا ومتابعة خططها، لتعزيز أمن وحماية مختلف بياناتها ومعلوماتها سواء كانت داخلية أم خارجية. بهدف خلق بيئة عمل آمنة لضمان سرية وسلامة وتوافر المعلومات عند الحاجة، لأن استخدامها وتطبيقها أمر لا غنى عنه في كافة المؤسسات لما تحققه من نتائج ايجابية فيما يخص زيادة إنتاجية المؤسسة أولا ثم أداء العاملين، وذلك لضمان بقائها واستمراريتها على المدى الطويل. ولهذا أصبح تبني فكرة الإدارة الرقمية أمرا حتميا لتعزيز أمن المعلومات داخل المؤسسات بسبب التطورات التكنولوجية السريعة، وتزايد وتعقيد التهديدات التي تستهدف البيانات الحساسة، مما يتوجب عليها الاستعانة بتقنيات حديثة وتطبيق إجراءات صارمة للحماية.

1-1- إشكالية الدراسة: على ضوء ما تقدم يمكن صياغة الإشكالية التالية:

كيف تساهم الإدارة الرقمية في تعزيز أمن المعلومات في مؤسسة اتصالات الجزائر وكالة خنشلة؟

ويتفرع على هذه الإشكالية الرئيسية مجموعة من الأسئلة الفرعية نوجزها فيما يلي:

- هل تؤثر الإدارة الرقمية في المؤسسات على تعزيز أمن المعلومات لديها؟
- هل استخدام تقنيات الإدارة الرقمية يساهم في تقليل حوادث اختراق أمن المعلومات؟
- هل تؤثر الإدارة الرقمية على تعزيز أمن المعلومات التي تعزى إلى المتغيرات الديموغرافية المستوى العلمي؟

1-2- فرضيات الدراسة: للإجابة على التساؤلات السابقة تم الاعتماد على مجموعة من الفرضيات في هذه الدراسة والمتمثلة فيما يلي:

- هناك علاقة ايجابية ذات دلالة إحصائية بين تطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات.
- استخدام تقنيات الإدارة الرقمية يساهم في تقليل حوادث اختراق أمن المعلومات.
- توجد فروق ذات دلالة إحصائية عند مستوى دلالة (0,05) بين متوسطات إجابات أفراد العينة حول أثر الإدارة الرقمية على تعزيز أمن المعلومات التي تعزى إلى المتغيرات الديموغرافية المستوى التعليمي.

1-3-**أهداف الدراسة:** تهدف هذه الدراسة إلى مجموعة من الأهداف نذكر منها:

- التعرف على مفهوم الإدارة الرقمية وأمن المعلومات.
- دور الإدارة الرقمية في تعزيز الوعي الأمني بين الموظفين داخل المؤسسات.
- إبراز أهمية أمن المعلومات كجزء أساسي من الإدارة الرقمية، مع التركيز على حماية سرية البيانات وسلامتها وتوافرها.
- معرفة مدى تطبيق الإدارة الرقمية في مؤسسة اتصالات الجزائر والتقنيات المستعملة لحماية المعلومات.

1-4-منهج الدراسة: من أجل دراسة الإشكالية التي طرحت سابقا واختبار صحة الفرضيات المقدمة تم الاعتماد على المنهج الوصفي والتحليلي، الذي يمكن من خلاله وصف خصائص هذه المشكلة وتحليل وتفسير نتائج الدراسة الميدانية، كما تم الاعتماد على منهج دراسة الحالة بالنسبة للجانب التطبيقي، باختيار مؤسسة اتصالات الجزائر كمحل للدراسة.

2-ماهية الإدارة الرقمية: تعد الإدارة الرقمية جزءا أساسيا من التحول الرقمي الذي يشهده العالم، حيث تسعى المؤسسات إلى دمج الحلول الرقمية في جميع جوانب عملها لتحقيق التميز التنافسي وتحسين الإنتاجية واتخاذ قرارات أكثر استنادا إلى البيانات، ومع التقدم التكنولوجي السريع أصبح التحول الرقمي والإدارة الرقمية من الأمور الضرورية لتحقيق النمو المستدام في العديد من المجالات.

2-1- مفهوم الإدارة الرقمية:تعددت تعاريف الإدارة الرقمية وفق لتعدد توجهات الباحثين ومن أهم التعريف نذكر ما يلي:

✓ الإدارة الرقمية هي:"استخدام وسائل الاتصال التكنولوجية المتنوعة في تسيير سبل أداء الإدارات الحكومية لخدمتها العامة ذات القيمة والتواصل مع طالبي الانتفاع من خدمات المرفق العام بمزيد من الديموقراطية، من خلال تمكينهم من استخدام وسائل الاتصال الالكترونية عبر بوابة واحدة." (سامية، 2024)

✓ تعرف أيضا على أنها:"منهجية جديدة تقوم على الاستيعاب الشامل، والاستخدام الواعي، والاستثمار الايجابي لتقنيات المعلومات والاتصالات الحديثة، في ممارسة وظائف الأساسية للإدارة على مختلف المستويات التنظيمية في المنظمات المعاصرة." (الطاهر و دربيخ، 2024)

ومن هنا فإن الإدارة الرقمية هي استخدام التكنولوجيا والبرمجيات لتحسين وتنظيم العمل في الشركات والمؤسسات بهدف تسهيل إدارة العمليات اليومية مثل التواصل واتخاذ القرار وتنظيم الموارد باستخدام أدوات رقمية حديثة، مما يساعد على زيادة الكفاءة وتحقيق نتائج أفضل بشكل أسرع.

2-2- وسائل الإدارة الرقمية: تتكون الإدارة الرقمية من عدة وسائل أساسية والمتمثلة في:

✓ **صناع المعرفة (المورد البشري):** إذ يمثل القيادات الرقمية كل ما يشمل رأس المال الفكري، المدربون، والمحللون للموارد المعرفية، فدور هذه الأخيرة يكمن في محاولة خلق ثقافة معرفية جديدة تتبنى الإدارة الرقمية، عن طريق تغيير طرق التفكير، وترقية أساليب العمل الإداري، وفق ما يتعاملون به من خبرات ومعارف في مجال المعلوماتية الواسع.

- ✓ **الأجهزة:** تضم المكونات المادية للحاسوب، شبكاته، نظمه، وملحقاته، بحيث يجب أن يراعى من قبل المؤسسات اقتناء أحدث الأجهزة في العالم من أجل توفير تكاليف التطوير المستمر، وأيضا ملائمة عتاد الحاسوب لمختلف التطورات التكنولوجية.
- ✓ **الشبكيات:** وتتمثل في تلك الحزم من مختلف الوصلات الالكترونية الممتدة عبر نسيج اتصالي لشبكات الأنترنت.
- ✓ **البرمجيات:** وهي التعليمات المختلفة التي تتحكم بالحاسوب وتضم الأجزاء التالية: لغات البرمجة، الأنظمة التطبيقية، البرامج والبيانات، أدوات تدقيق البرمجة وتحقق الاستفادة من إمكانياته المختلفة. (ميمونة، 2024)

2-3-أبعاد الإدارة الرقمية: تتمثل أبعاد الإدارة الرقمية فيما يلي:

- ✓ **البعد التكنولوجي:** يتعلق هذا البعد بالبنية التحتية التكنولوجية التي تدعم الإدارة الرقمية، مثل أنظمة المعلومات، البرمجيات، الأجهزة، والحوسبة السحابية، يجب أن تكون التكنولوجيا المستخدمة متوافقة مع احتياجات المؤسسة وقابلة للتطوير لمواكبة التطورات التقنية.
- ✓ **البعد البشري:** يتناول هذا البعد تأثير الأفراد والعاملين في المؤسسة على تبني الإدارة الرقمية، حيث أن الأمر يتعلق بتدريب الموظفين على استخدام الأدوات الرقمية، وتطوير المهارات الرقمية، ودور القيادة في دعم التحول الرقمي.
- ✓ **البعد التنظيمي:** يشمل هذا البعد تصميم العمليات الداخلية والهياكل التنظيمية لدعم آليات الإدارة الرقمية، قد يتطلب التحول الرقمي إعادة هندسة العمليات لضمان مرونة وكفاءة أكبر.
- ✓ **البعد القانوني والأمني:** يتعلق هذا البعد بالاعتبارات القانونية والأمنية المرتبطة بالإدارة الرقمية، يشمل ذلك الامتثال للقوانين والتشريعات، وحماية البيانات الشخصية، وأمن المعلومات لضمان سلامة الأنظمة الرقمية.
- ✓ **البعد البيئي:** يرتبط هذا البعد بتأثير التكنولوجيا الرقمية على البيئة، حيث تسعى المؤسسات غلى تطبيق آليات الإدارة الرقمية بطريقة تقلل من التأثير السلبي على البيئة، مثل تحسين استهلاك الطاقة وتقليل للنفايات الالكترونية.
- ✓ **الأتمته والتحليلات:** تعتمد الإدارة الرقمية على أتمتة المهام الروتينية وتحليل البيانات الضخمة لتحسين الكفاءة واتخاذ القرارات المستنيرة، الأدوات الرقمية مثل الروبوتات البرمجية وأنظمة التحليلات الذكية تساعد على تقليل الأخطاء البشرية، وزيادة سرعة العمليات.
- ✓ **المرونة الرقمية:** المرونة هي واحدة من السمات الأساسية للإدارة الرقمية، حيث تتيح التكنولوجيا مثل الحوسبة السحابية والاتصال عن بعد للموظفين العمل من أي مكان، مما يحسن توازن الحياة العملية والشخصية ويزيد من إنتاجيتهم. (زكريا، عبد النبي، و محمد جمال، 2025)

3-الإطار النظري لأمن المعلومات: أصبح أمن المعلومات أمرا ضروريا لحماية البيانات الحساسة من التهديدات المتزايدة، يشمل ذلك تأمين المعلومات الشخصية والتجارية وضمان سلامتها وسريتها وتوافرها، حيث يركز أمن المعلومات على حماية الأنظمة والشبكات من الاختراقات الإلكترونية والبرامج الضارة، مما يتطلب استراتيجيات فعالة وسياسات أمنية متكاملة لمواجهة هذه التحديات المختلفة.

1-3-مفهوم أمن المعلومات: أمن المعلومات ليس مجرد مجموعة من الإجراءات التقنية أو البرمجيات بل هو نهج شامل يهدف إلى حماية هذه المعلومات من أي تهديد قد يعرضها للخطر، لذلك سنتطرق لعدة تعريفات أهمها:

- ✓ "هو العلم الذي يبحث في نظريات واستراتيجيات توفر الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء". (حفصي و حليمي، 2022)
- ✓ "هو عبارة عن مجموعة من الإجراءات الإدارية والتقنية التي تم اتخاذها لضمان توفير الحماية اللازمة للمعلومات من التهديدات الداخلية والخارجية". (الغثير و محمد بن عبد الله، 2009)

ومنه يمكن القول أن: أمن المعلومات هو مجموعة من الممارسات والعمليات لحماية المعلومات من المخاطر والتهديدات الخارجية، حيث يهدف إلى تأمين المعلومات المتداولة عبر الانترنت ويوفر مختلف الأدوات والوسائل لحمايتها من المخاطر سواء كانت داخلية أم خارجية.

2-3-أبعاد أمن المعلومات: لأمن المعلومات مجموعة من الأبعاد التي يتم تطبيقها للحفاظ على سلامة وجودة وتوافر المعلومات، وتتمثل فيما يلي:

- ✓ **سرية المعلومات:** بمعنى عدم إطلاع أو تغيير المعلومات المخزنة على أجهزة الحاسوب أو المنقولة على الشبكة إلا من قبل الأشخاص المخول لهم بذلك.
- ✓ **سلامة المعلومات:** يتمثل ذلك في عدم تغيير المعلومات المخزنة على أجهزة الحاسوب أو المنقولة عبر الشبكة.
- ✓ **جودة المعلومات:** وذلك يتمثل في عدم حذف المعلومات المخزنة على أجهزة الحاسوب إلا من قبل الأشخاص المخولين لهم بذلك. (قذايفية، 2016)

3-3-مخاطر وتهديدات أمن المعلومات: تتزايد مخاطر وتهديدات أمن المعلومات بشكل ملحوظ في ظل التطورات التكنولوجية السريعة، تشمل هذه المخاطر الهجمات السيبيرانية التي تستهدف البيانات الحساسة والأنظمة الحيوية مما يؤدي إلى خسائر مالية كبير، حيث يصبح الاستثمار في استراتيجيات أمن المعلومات أمرا ضروريا لحماية المؤسسات من هذه التهديدات المتزايدة وضمان سلامة بياناتها. وصنفت مخاطر أمن المعلومات كما يلي: (شوابكة، 2019)

أ. **مخاطر داخلية:** هي المصادر التي تحدث بسبب أحد مكونات النظام وهي كما يلي:

- ✓ **المخاطر البشرية:** تعد المخاطر التي يتسبب فيها الأفراد العاملون في النظام من أخطر التهديدات وأكثرها تأثيرا وتشمل الأفعال المقصودة والغير المقصودة من قبل الأشخاص المسموح لهم وغير المسموح لهم باستخدام النظام.
- ✓ **الخلل في المعدات:** يتضمن تعطل أجهزة الحاسوب والتجهيزات الشبكية المرتبطة بالنظام، وهذا النوع من الأعطال يتسبب في توقف النظام عن العمل وحجب الخدمة عن المستفيدين.
- ✓ **أخطاء البرمجيات:** تعاني الكثير من البرمجيات المستخدمة في النظام من احتوائها على الأخطاء، الأمر الذي ينعكس على دقة المخرجات وصحة المعالجة التي يقوم بها النظام.
- ✓ **أخطاء البيانات:** هي الأخطاء الناشئة عن عملية إدخال البيانات بحيث يتم إدخال بيانات غير صحيحة مما ينعكس على دقة المخرجات، وكلما زادت نسبة الخطأ في البيانات المدخلة كلما زاد حجم الخطر.

ب. **مخاطر خارجية:** هذا النوع من المخاطر يكون مصدره أسباب من خارج النظام، أي يمكن أن يكون نتيجة أشخاص غير مخولين باستخدام النظام أو من أسباب بيئية أو طبيعية، ومن هذه المخاطر ما يلي:

- ✓ **الهجوم الأمني:** يقصد به المحاولات المختلفة التي ينفذها الأشخاص غير المخولين بقصد الوصول غير الشرعي للنظام أو إحداث الخطر فيه.

- ✓ **خطر الاختراق:** يقصد به القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، ويتحقق ذلك بدخول شخص غير مصرح له إلى النظام والقيام بأنشطة غير مصرح له كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات.
- ✓ **الاصطياد الإلكتروني:** يقصد به قيام المهاجم بإرسال رسائل بريد إلكترونية خادعة إلى المستخدمين تتضمن روابط إلكترونية مزيفة تشابه الموقع الإلكتروني للمنظمة أو تكون مواقع إلكترونية مزيفة تدعي أنها بنوك وتقدم خدمات بنكية، وعند دخول المستخدم لهذه المواقع فإنها تطلب منه معلومات كمعلومات حسابه البنكي أو معلومات بطاقته الائتمانية وهذه المواقع تكون مصممة بطريقة تشبه فيها المواقع الإلكترونية الحقيقية.
- ✓ **البرامج الخبيثة:** عبارة عن برنامج صغير معد لتخريب البيانات، يتم إدخاله إلى الحاسوب من غير علم المستخدم بغرض نسخ أو إزالة البيانات المسجلة عليه، ومن الأمثلة عليه الفيروسات الحاسوبية وبرامج الديدان وحصان طروادة والقنابل الموقوتة.
- ✓ **مخاطر بيئية:** تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق فضلا عن المشاكل القائمة عن تعطل أنظمة التكييف والتبريد وغيرها ودرجة الحرارة والرطوبة كلها تؤدي إلى توقف هذه التجهيزات لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات. (منصور، 2018)

4-إجراءات الدراسة التطبيقية والوسائل المعتمدة: بعد التطرق في الجانب النظري إلى المفاهيم المتعلقة بالإدارة الرقمية وأمن المعلومات، تم إسقاط ما تم التوصل إليه نظريا على ما هو موجود في الواقع، ومن ثم إبراز دور الإدارة الرقمية في تحقيق أمن المعلومات داخل المؤسسات، لذلك تم إجراء دراسة ميدانية **بمؤسسة" اتصالات الجزائر"** بولاية خنشلة. وذلك من وجهة نظر مجموعة من المهنيين والإداريين ذوي الصلة بمجال تكنولوجيا المعلومات والإدارة، وقدرت عينة الدراسة ب 30 مفردة،

4-1-بناء أداة الدراسة: تم تصميم الاستبيان بطريقة علمية منظمة، واحتوى على مقدمة تعريفية تهدف إلى توضيح طبيعة الموضوع للمستجيب، واحتوى على **21سؤالا** موزعة على جزئين رئيسيين: جزء خاص بالبيانات الديمغرافية المتعلقة بأفراد العينة، تعنى بالجنس، الفئة العمرية، والمؤهل العلمي، وهي بيانات من شأنها أن تساعد في تفسير النتائج وتحليلها. أما الجزء الثاني فتعلق باختبار فروض الدراسة، ويتضمن **18سؤالا** وُزعت على ثلاثة محاور رئيسية: الإدارة الرقمية أمن المعلومات العلاقة بين الإدارة الرقمية وأمن المعلومات. وقد تم بناء عبارات الاستبيان باستخدام مقياس ليكارت الخماسي الذي يوفر خمس بدائل للإجابة، مما يتيح إمكانية قياس مستوى موافقة المستجيبين بدقة، كما يسهل ترميز البيانات وتحليلها إحصائيا.

4-2-صدق و ثبات أداة الدراسة:

4-2-1-الاتساق الداخلي للمحور الأول الإدارة الرقمية: يهدف استخدامه إلى قياس الارتباط بين الدرجة الكلية لكل عنصر والدرجة الكلية للمحور الذي يتبع له، بالإضافة إلى ارتباط الدرجة الكلية لكل محور مع الدرجة الكلية للأداة الاستبيانية بأكملها التي يتبع لها. وإحصائيا نعبر عن الصدق من خلال حساب معامل الارتباط بيرسون، والجدول التالي تبين نتائج حساب الصدق الاتساق الداخلي لفقرات الإدارة الرقمية، كما هو موضح في الجدول.

فتظهر النتائج أن معظم العبارات (من 02 إلى 06) حققت معاملات ارتباط مرتفعة ودالة إحصائيا عند مستوى الدلالة 0.001(**$p < 0.01$**) ، حيث تراوحت قيم معاملات الارتباط بين **0.668** و**0.866**، وهي دلالات قوية تشير إلى وجود علاقة

ارتباط إيجابية قوية بين العبارات والدرجة الكلية للمحور. هذه النتائج تدل على أن العبارات من 02 إلى 06 تتسق بشكل جيد مع المفهوم العام لمحور الإدارة الرقمية، مما يدعم صدق المحور ومصداقية عباراته.

الجدول رقم (01): مصفوفة الارتباط للمحور الأول الإدارة الرقمية

العبارات	معامل الارتباط	مستوى الدلالة
01	0.51	0.788
02	**0.850	0.001
03	**0.697	0.001
04	**0.866	0.001
05	**0.736	0.001
06	**0.668	0.001

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

(**) الارتباط عالي عند مستوى الدلالة (0.01)

(*) الارتباط عالي عند مستوى الدلالة (0.05)

من ناحية أخرى، تسجّل العبارة الأولى (01) معامل ارتباط ضعيف نسبيا قدره **0.51**، وهو غير دال إحصائيا (**p** = **0.788**)، ما قد يشير إلى اختلاف إيجابي في فهم أو تفسير المستجيبين للعبارة، وهو مؤشر إيجابي على ضرورة التنوع في الفهم الثقافي. بشكل عام، تعد نتائج هذا الجدول مؤشرا إيجابيا على قوة وصدق مكونات محور **"الإدارة الرقمية"**، مع ملاحظة أن العبارة الأولى تمثل استثناء.

الجدول رقم (02): مصفوفة الارتباط للمحور الثاني أمن المعلومات

العبارات	معامل الارتباط	مستوى الدلالة
07	**0.750	0.001
08	**0.802	0.001
09	**0.908	0.001
10	**0.885	0.001
11	**0.786	0.001
12	**0.911	0.001

المصدر: من إعداد الباحث بالاعتماد على مخرجات SPSSV27

(**) الارتباط عالي عند مستوى الدلالة (0.01)

(*) الارتباط عالي عند مستوى الدلالة (0.05)

تشير النتائج إلى أن جميع العبارات (من 07 إلى 12) قد سجلت **معاملات ارتباط مرتفعة ودالة إحصائيا** عند مستوى دلالة 0.001(**p** < **0.01**) ، وهو ما يعكس قوة العلاقة بين كل عبارة والمجموع الكلي للمحور. فقد تراوحت معاملات الارتباط بين **0.750**و**0.911**، وهي قيم تدل على **درجة عالية من الاتساق الداخلي** بين الفقرات، مما يعزز من صدق هذا المحور.

بشكل خاص، نلاحظ أن العبارة (12) سجلت أعلى معامل ارتباط بلغ **0.911**، تليها العبارة (09) بـ **0.908**، وهو ما يشير إلى أن هاتين العبارتين تعدان الأكثر تمثيلًا لمضمون محور أمن المعلومات. كما أن بقية العبارات تتبع نفس النمط من الاتساق المرتفع، مما يعكس أن جميع العبارات تشكل وحدة متماسكة تقيس بعدا مفاهيميا واحدًا بشكل دقيق ومنسجم.

وتظهر هذه النتائج أن محور **"أمن المعلومات"** يتمتع **بمصداقية عالية** ويمكن الاعتماد عليه في القياس، كما تعكس جودة تصميم فقرات الاستبيان المتعلقة بهذا المحور، سواء من حيث الصياغة أو الارتباط النظري بالمفهوم العام.

الجدول رقم (03): مصفوفة الارتباط للمحور الثالث الإدارة الرقمية وأمن المعلومات

العبارات	معامل الارتباط	مستوى الدلالة
13	**0.767	0.001
14	**0.900	0.001
15	**0.864	0.001
16	**0.851	0.001
17	**0.839	0.001
18	**0.707	0.001

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

(**) الارتباط عالي عند مستوى الدلالة (0.01)

(*) الارتباط عالي عند مستوى الدلالة (0.05)

تشير القيم إلى أن جميع العبارات من (13) إلى (18) قد حققت **معاملات ارتباط مرتفعة ودالة إحصائيا** عند مستوى دلالة 0.001(**p < 0.01**) ، وهو ما يعكس اتساقا قويا بين كل عبارة والمجموع الكلي للمحور.

تراوحت معاملات الارتباط بين **0.707**(العبارة 18) و**0.900** (العبارة 14)، وهي مؤشرات قوية تدل على أن جميع الفقرات تقيس نفس البعد المفاهيمي بدرجة عالية من الدقة. تعتبر العبارة (14) الأعلى من حيث معامل الارتباط، ما يشير إلى تمثيلها الجيد لهذا البعد المركب الذي يجمع بين مفهومي الإدارة الرقمية وأمن المعلومات. وتؤكد هذه النتائج على أن المحور يتمتع **بدرجة عالية من الصدق الداخلي**، مما يدل على **فعالية بناء الاستبيان** من حيث صياغة الفقرات وتوافقها النظري مع أهداف الدراسة. كما تعكس النتائج قدرة العبارات على قياس مفهوم "التكامل بين الإدارة الرقمية وأمن المعلومات" بشكل مترابط ومنسجم.

4-2-2-ثبات أداة الدراسة: وفي إطار هذه الدراسة، تم **التحقق من ثبات محاور الاستبيان** عبر استخدام أحد أكثر الأساليب الإحصائية شيوعا، وهو **معامل ألفا كرونباخ (Cronbach's Alpha)** ، والذي يستخدم لتحديد مدى تجانس العبارات الداخلة ضمن كل محور من محاور الدراسة، ومدى قدرتها على قياس نفس البعد.

الجدول رقم (04): معامل ألفا كرونباخ لأداة الدراسة

المحاور	عدد العبارات	معامل ألفا كرونباخ
المحور الأول: الإدارة الرقمية	06	0.786
المحور الثاني: أمن المعلومات	**06**	**0.918**
المحور الثالث: الإدارة الرقمية وامن المعلومات	06	0.900
جميع محاور الاستبانة	18	0.940

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

يتضح من خلال النتائج الواردة في **الجدول (04)**:أن قيم معامل ألفا كرونباخ لجميع المحاور قد تجاوزت القيمة المقبولة إحصائيًا (0.70)، وهو ما يعكس تمتع أداة الاستبيان بدرجة عالية من الاتساق الداخلي. وتُعد هذه النتائج مؤشرا قويا على موثوقية الأداة المستخدمة في الدراسة، وقدرتها على قياس الأبعاد المتعلقة بالإدارة الرقمية وأمن المعلومات بجودة

ودقة. كما أن القيمة الكلية المرتفعة (0.940) تعزز من مصداقية النتائج المستخلصة من التحليل الإحصائي، مما يضفي مصداقية على الاستنتاجات النهائية للدراسة.

ومن أجل مزيد من الثبات تم استخدام طريقة التجزئة النصفية كطريقة أخرى لاختيار ثبات الاستبيان لمحاوره الإجمالية وحتى لأبعاد كل محور، وذلك عن طريق تقسيم فقرات الاستبيان إلى جزئين، حيث الجزء الأول مخصص للأسئلة الفردية (س،1 س،3 س...،5الخ) والجزء الثاني مخصص للأسئلة الزوجية (س،2 س،4 س،6 ....الخ)، حيث يتم حساب معامل ألفا كرونباخ لكل جزء مستقل، ثم حساب معامل الارتباط بين الأسئلة الفردية والزوجية، ثم إجراء عملية تصحيح هذا المعامل وذلك باستخدام معامل سبيرمان براون المعدل للمعامل الأول .Half Split والجدول الموالي يبين ذلك:

الجدول رقم (05): التجزئة النصفية لأداة الدراسة

المحاور	معادل الارتباط قبل التصحيح	تصحيح المعامل بمعادلة سبيرمان براون
المحور الأول:الإدارة الرقمية	0.766	0.867
المحور الثاني: أمن المعلومات	**0.865**	**0.927**
المحور الثالث: الإدارة الرقمية وامن المعلومات	0.828	0.906
جميع محاور الاستبانة	0.935	0.967

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

تشير نتائج التجزئة النصفية لأداة الدراسة إلى درجة عالية من الثبات والاتساق الداخلي بين فقرات الاستبيان، وهو ما يعد مؤشرا مهما على جودة الأداة ومصداقيتها في قياس المتغيرات المستهدفة بالدراسة.

فمن خلال معامل الارتباط قبل التصحيح، نلاحظ أن جميع المحاور سجلت قيمًا مرتفعة (أعلى من 0.75)، مما يدل على وجود درجة جيدة من الاتساق بين نصفي كل محور. وبعد تطبيق معامل **سبيرمان-براون** لتصحيح معامل الارتباط الناتج عن تقسيم العبارات إلى نصفين، ارتفعت القيم إلى مستويات أعلى، حيث تجاوزت جميعها 0.86، وهو ما يعكس مستوى ثبات مرتفع جدا.

فعلى سبيل المثال، بلغ معامل الثبات المعدل لمحور "الإدارة الرقمية" 0.867، بينما سجل محور "أمن المعلومات" قيمة 0.927، ومحور "الإدارة الرقمية وأمن المعلومات" قيمة 0.906. أما بالنسبة لكامل محاور الاستبيان مجتمعة، فقد بلغ معامل التصحيح النهائي 0.967، وهي قيمة ممتازة وتشير إلى اتساق داخلي مرتفع جدا.

وبناء عليه، يمكن القول إن نتائج التجزئة النصفية تعزز من صلاحية أداة الدراسة كمؤشر كمي موثوق يسمح للباحث بإجراء تحليلات إحصائية دقيقة تستند إلى بيانات ذات جودة عالية.

4-3-اختبار التوزيع الطبيعي: لاختبار الأدوات الإحصائية المناسبة من اجل تحليل إجابات أفراد العينة الدراسة واختبار صحة الفرضيات يجب أولا أن معرفة طبيعة توزيع بيانات العينة وهو اختبار ضروري في حالة اختبار الفرضيات. وعليه ومن اجل اختبار طبيعة التوزيع نحتاج إلى وضع فرضيتين هما فرضية العدم والفرضية البديلة، على اعتبار أن فرضية العدم خاضعة للاختبار أي أنها قد تكون غير صحيحة، مما يتطلب وضع الفرضية البديلة H_1 الفرضية الصفرية H_0 كما يلي:

- ✓ **H_0: بيانات تتبع التوزيع الطبيعي**
- ✓ **H_1: بيانات لا تتبع التوزيع**

يعتبر اختبار **كولموغوروف-سميرنوف** أحد الأساليب الشائعة المستخدمة لفحص الانحراف عن التوزيع الطبيعي، إذ يمكن أن يكون للبيانات توزيعات أخرى مختلفة مثل التوزيع غير الطبيعي أو التوزيع ذو الذيل الثقيل وغيرها.

الجدول رقم (06): القيمة الإحصائية لاختبار التوزيع الطبيعي Kolmogorove-simirnov

	محاور الاستبانة	Kolmogorov-Smirnov		النتيجة
		القيمة الإحصائية	مستوى الدلالة	
1	الإدارة الرقمية	0.144	0.114	يتبع التوزيع الطبيعي
2	امن المعلومات	0.050	0.200*	يتبع التوزيع الطبيعي
3	الادارة الرقمية وامن المعلومات	0.044	0.200*	يتبع التوزيع الطبيعي
	جميع محاور الاستبانة	0.963	0.200*	يتبع التوزيع الطبيعي

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

حسب النتائج المبينة في **الجدول رقم (06):** فإن جميع محاور الاستبيان قد سجلت **قيمًا دلالية (Sig) أكبر من 0.05**، مما يشير إلى **عدم وجود فروق ذات دلالة إحصائية بين التوزيع الفعلي والتوزيع الطبيعي المفترض** .وبذلك يمكن القول إن:

- ✓ **محور الإدارة الرقمية** سجل قيمة دلالة **0.114**، وهي تدل على أن البيانات تتبع التوزيع الطبيعي.
- ✓ **محور أمن المعلومات** أظهر قيمة دلالة**0.200** الحد الأقصى، ما يعزز افتراض التوزيع الطبيعي للبيانات الخاصة به.
- ✓ **محور الإدارة الرقمية وأمن المعلومات معا** أظهر كذلك قيمة دلالة **0.200**، وهو ما يعكس انسجام البيانات مع التوزيع الطبيعي المفترض.
- ✓ وأخيرا، **جميع محاور الاستبيان مجتمعة** سجلت قيمة دلالة **0.200**، وقيمة إحصائية **0.963**، وهي نتيجة قوية تؤكد تجانس البيانات مع التوزيع الطبيعي.

بناءا على هذه النتائج، يمكن اعتماد **الأساليب الإحصائية** في تحليل بيانات هذه الدراسة، مما يعزز من **المصداقية الإحصائية** ويسمح باستخدام أدوات تحليلية دقيقة مثل **اختبارT** ، تحليل التباينANOVA ، ومعاملات الارتباط والانحدار، وغيرها.

3-4-عينة الدراسة: تم تحديد عينة الدراسة بشكل مسبق قبل توزيع استمارة الاستبيان، حيث تم إعداد الاستبيان وتوزيعه على الأشخاص المحددين حيث تم توزيع 30 استمارة وتم استرجاعها كلها عن الطريق التسليم والاستلام المباشر.

4-4-1-خصائص العينة:

✓ **حسب الجنس:**

الجدول رقم (07): خصائص العينة حسب الجنس

الجنس	التكرارت	النسبة المئوية
ذكر	16	53,3%
أنثى	14	46,7%
المجموع	30	100%

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

✓ **حسب الفئة العمرية:**

يظهر الجدول رقم (08): أن الفئة العمرية **من 31 إلى 40 سنة** تمثل النسبة الأكبر من أفراد العينة بنسبة **43%**، تليها الفئة **من 25 إلى 30 سنة** بنسبة **27%**، ثم الفئة **من 51 سنة فأكثر** بنسبة **20%**، وأخيراً الفئة **من 41 إلى 50 سنة**

بنسبة .**10%** وهذا يشير إلى أن غالبية المشاركين هم من الفئة النشطة مهنياً، مما يعزز من دقة الإدراك والتحليل حول موضوع **الإدارة الرقمية وأمن المعلومات** داخل المؤسسات.

الجدول رقم (08): خصائص العينة حسب الفئة العمرية

الفئة العمرية	التكرارت	النسبة المئوية%
من 25 إلى 30 سنة	8	26,7%
من 31 إلى 40 سنة	13	43,3%
من 41 سنة إلى 50 سنة	3	10%
من 51 سنة فأكثر	6	20%
المجموع	30	100%

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

✓ **حسب المستوى العلمي:**

الجدول رقم (09): خصائص العينة حسب المستوى العلمي

المستوى	التكرارت	النسبة المئوية%
ليسانس	9	30%
ماستر	13	43,3%
دكتوراه	5	16,7%
تقني سام	2	6,7%
مؤهل جامعي	1	3,3%
المجموع	30	100%

المصدر: من إعداد الباحثة بالاعتماد على مخرجات SPSSV27

يتضح من الجدول: أن النسبة الأكبر من أفراد العينة يحملون شهادة **الماستر** بنسبة **43 %**، تليها شهادة **الليسانس** بنسبة **30%**، ثم شهادة **الدكتوراه** بنسبة **17%**، في حين أن الفئات الأخرى تمثل نسبا أقل. وهذا يدل على أن غالبية المشاركين يتمتعون بمستوى علمي عال، مما يعزز من جودة البيانات المحصلة ويضفي مصداقية على الآراء المتعلقة بتأثير الإدارة الرقمية على أمن المعلومات داخل المؤسسات.

4-4-2-عرض وتحليل نتائج الدراسة: تتضمن الدراسة مجموعة من النتائج يتم وصفها وتحليلها كما يلي:

يشير تحليل إجابات أفراد العينة على عبارات محور **الإدارة الرقمية** إلى تفاوت في درجة الاتفاق حول مدى تطبيق المؤسسة للمفاهيم الرقمية. فقد حققت العبارة الأولى، التي تنص على أن "المؤسسة تعتمد بشكل كبير على الأنظمة الرقمية في إدارة العمليات اليومية"، أعلى متوسط حسابي بلغ **(4.86)** مع انحراف معياري منخفض **(0.345)**، ما يدل على وجود **إجماع قوي بين أفراد العينة** على أن الرقمنة أصبحت جزءًا أساسيًا من عمل المؤسسة اليومي، وأن الآراء كانت متقاربة جدًا حول هذه النقطة.

في المقابل، جاءت العبارة الثانية حول امتلاك الموظفين للمهارات الرقمية بمتوسط حسابي منخفض نسبيًا بلغ **(2.86)**، وهو ما يعكس **ضعفًا في مدى تأهيل الكادر البشري** لاستخدام التكنولوجيا بشكل فعّال. كما أن الانحراف المعياري المرتفع **(1.252)**يظهر وجود **اختلاف كبير بين آراء المجيبين**، مما قد يُعزى إلى تفاوت المستويات المهارية بين الموظفين أو اختلاف طبيعة المهام التي يؤدونها.

أما فيما يتعلق بتأثير الإدارة الرقمية على جودة الخدمات، فقد حققت العبارة الثالثة متوسطًا بلغ **(3.03)**، مما يعكس **اتفاقًا محدودًا أو موافقة ضعيفة** على هذا الأثر. ويعزز ذلك الانحراف المعياري **(1.129)**، والذي يشير بدوره إلى وجود **تباين ملحوظ في وجهات النظر**، ما قد يُفهم على أنه ناتج عن اختلاف في مستويات رضا المتعاملين أو مدى تطبيق الرقمنة عبر مختلف الوحدات الإدارية.

الجدول رقم (10): نتائج تحليل إجابات أفراد العينة على عبارات المحور الاول الادارة الرقمية

الرقم	العبارات		التكرارات والنسب المئوية					المتوسط الحسابي	الانحراف المعياري	الاتجاه العام
			أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة			
01	تعتمد المؤسسة بشكل كبير على الانظمة الرقمية في ادارة العمليات اليومية.	ت	26	4	0	0	0	4.86	0.345	موافقة بشدة
		ن	86,7 %	13,3 %	/	/	/			
02	الموظفون في المؤسسة يمتلكون المهارات الكافية لاستخدام التقنيات الرقمية بفعالية	ت	3	6	11	4	06	2.86	1.252	محايدة
		ن	10 %	20 %	36 %	13.3 %	20 %			
03	الادارة الرقمية ساعدت في تحسين جودة الخدمات المقدمة للعملاء	ت	4	4	14	5	3	3.03	1.129	موافقة
		ن	13,3 %	13,3 %	46,7 %	16,7 %	10 %			
04	البينة التحتية في المؤسسة تلبي احتياجاتها بشكل جيد	ت	06	08	2	12	2	3.13	1.332	موافقة
		ن	20 %	26,7 %	6,70 %	40 %	6,7 %			
05	هناك مقاومة داخل المؤسسة عند تطبيق التقنيات الرقمية الجديدة	ت	6	8	4	9	3	3.16	1.341	موافقة
		ن	20 %	26,7 %	13,3 %	30 %	10 %			
06	الادارة الرقمية توفر الوقت والجهد مقارنة بالطرق التقليدية	ت	4	15	4	7	0	3.53	1.008	موافقة
		ن	13,3 %	50 %	13,3 %	23,3 %	/			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

بالنسبة للبنية التحتية الرقمية، فقد حصلت على متوسط **(3.13)**مع انحراف معياري مرتفع **(1.332)**، ما يدل على أن هناك **اتجاهًا نحو الموافقة، ولكن دون إجماع**، ويُحتمل أن تكون هناك **تفاوتات حقيقية في مستوى التجهيزات التقنية** من قسم إلى آخر داخل المؤسسة. ومن جهة أخرى تدل العبارة (05) على المقاومة داخل المؤسسة حيث بلغت متوسطًا بلغ **(3.16)**، وهو ما يعكس نوعًا من **الحياد المائل إلى الموافقة**، مما يدل على أن المقاومة موجودة لكنها **ليست مهيمنة** .ومع ذلك، فإن الانحراف المعياري المرتفع **(1.341)** يؤكد وجود **تباين ملحوظ** في المواقف الفردية تجاه التغيير الرقمي.

وأخيرًا، نلاحظ أن أفراد العينة قد أبدوا **موافقة معتدلة** على العبارة السادسة التي تفيد بأن الإدارة الرقمية توفر الوقت والجهد، حيث بلغ المتوسط الحسابي **(3.53)**، وهو قريب من الحد الأعلى لفئة "موافقة قليلة"، بينما بلغ الانحراف المعياري **(1.008)**، وهو مؤشر على أن **الآراء متفاوتة ولكنها تميل نحو الإيجاب**.

بناءً على هذه النتائج، يمكن القول إن المؤسسة قد قطعت شوطًا معتبرًا في التحول نحو الإدارة الرقمية، إلا أن **نجاح هذا التحول ما يزال يواجه تحديات بشرية وتقنية** تتطلب تعزيز البنية التحتية الرقمية وتكثيف برامج التكوين المستمر للموظفين.

الجدول رقم (11): نتائج تحليل إجابات أفراد العينة على عبارات المحور الثاني أمن المعلومات

الرقم	العبارات		التكرارات والنسب المئوية					المتوسط الحسابي	الانحراف المعياري	الاتجاه العام
			أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة			
07	تستخدم المؤسسة برامج مكافحة الفايروسات	ت	4	8	9	8	1	3.20	1.095	موافقة
		ن	13,3 %	26,7 %	30 %	26,7 %	3,3 %			
08	يتم تحديث برامج فحص أنظمة المؤسسة بشكل دوري للتأكد من أمانها	ت	7	15	7	1	0	3.66	1.184	محايدة
		ن	23,3 %	50 %	23,3 %	3,3 %	/			
09	يتم استخدام جدار الحماية في المؤسسة والمكاتب	ت	10	9	6	2	3	3.70	1.290	موافقة
		ن	33,3 %	30 %	20 %	6,7 %	10 %			
10	يتم تدريب الموظفين على ممارسة أمن المعلومات	ت	06	10	7	5	2	3.43	1.194	موافقة
		ن	20 %	33,3 %	23,3 %	16,7 %	6,7 %			
11	يتم حماية البيانات عند نقلها بين الموظفين او الى خارج المؤسسة	ت	8	10	7	3	2	3.63	1.188	موافقة
		ن	26,7 %	33,3 %	23,3 %	10 %	6,7 %			
12	تتبع المؤسسة ارشادات امان البريد الالكتروني	ت	7	12	7	1	3	3.63	1.188	موافقة
		ن	23,3 %	40 %	23,3 %	3,3 %	10 %			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

تشير نتائج تحليل إجابات أفراد العينة حول محور أمن المعلومات إلى وجود توجه عام نحو الموافقة على تطبيق المؤسسة لإجراءات الحماية الرقمية، وإن بدرجات متفاوتة. فقد حصلت العبارة السابعة، التي تشير إلى استخدام برامج مكافحة الفيروسات، على متوسط حسابي بلغ (3.20)، ما يعكس موافقة معتدلة من طرف المجيبين، بينما يُظهر الانحراف المعياري (1.095)قدرًا من التباين في الآراء، مما قد يُعزى إلى اختلاف مستويات المعرفة أو الممارسات اليومية بين الموظفين.

فيما يتعلق بعملية تحديث برامج فحص الأنظمة بشكل دوري (العبارة 08)، فقد جاءت النتائج إيجابية نسبيًا بمتوسط حسابي (3.66)، وهو ما يعكس اتفاقًا أعلى على تطبيق هذه الممارسة، مع انحراف معياري (1.184)، مما يدل على

أن معظم المشاركين لديهم وجهة نظر متقاربة في هذا السياق، ويعتبرون أن المؤسسة تقوم بجهود واضحة للحفاظ على أنظمة آمنة ومحدثة.

أما استخدام جدار الحماية، فقد حصل على أعلى متوسط ضمن هذا المحور تقريبًا، بقيمة (3.70)، مما يشير إلى مستوى جيد من الموافقة على وجود بنية أمنية تحمي الشبكات المؤسسية. إلا أن الانحراف المعياري المرتفع نسبيًا (1.290)يعكس تفاوتًا في الإدراك أو الخبرة بين أفراد العينة، وقد يكون ذلك بسبب عدم اطلاع بعض الموظفين على الجوانب التقنية للبنية التحتية الأمنية.

وفيما يتعلق بجهود تدريب الموظفين على أمن المعلومات (العبارة 10)، فقد بلغ متوسط التقديرات (3.43)، ما يدل على موافقة مقبولة، مع انحراف معياري (1.194)، ما يشير إلى وجود فروقات ملحوظة بين تقييمات الأفراد، مما يمكن أن يُفهم على أنه وجود برامج تدريبية غير منتظمة أو متفاوتة في فعاليتها.

بالنسبة للعبارتين المتعلقتين بحماية البيانات أثناء النقل (العبارة 11) وإتباع إرشادات أمان البريد الإلكتروني (العبارة 12)، فقد سجلتا متوسطًا متساويًا بلغ (3.63)لكل منهما، وهو ما يعكس مستوى موافقة جيد من قبل أفراد العينة على الإجراءات الأمنية المتعلقة بالبيانات والبريد الإلكتروني. ويلاحظ أن الانحراف المعياري (1.188) في كلا الحالتين يشير إلى درجة متوسطة من التباين في الآراء، مما قد يعكس اختلاف مستويات الالتزام بين الأقسام أو غموض السياسات المعتمدة.

الجدول رقم (12) : نتائج تحليل إجابات أفراد العينة على عبارات المحور الثالث الإدارة الرقمية وامن المعلومات

الرقم	العبارات		التكرارات والنسب المئوية					المتوسط الحسابي	الانحراف المعياري	الاتجاه العام
			أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة			
13	تعتمد المؤسسة على الادارة لرقمية لتحسين حماية المعلومات وسرية البيانات	ت	16	7	3	4	0	4.03	1.376	موافقة
		ن	,353 %	23,3 %	10 %	13,3 %	/			
14	توفر الادارة الرقمية في المؤسسة آليا فعالة لضمان أمن المعلومات ضد التهديدات الخارجية	ت	18	5	4	1	2	4.20	1.214	موافقة
		ن	60 %	16.7 %	13.3 %	3.3 %	6.7 %			
15	تساهم الإدارة الرقمية في تعزيز وعي الموظفين بأهمية امن المعلومات	ت	12	9	4	3	2	3.86	1.252	موافقة
		ن	40 %	30 %	13,3 %	10 %	6,7 %			
16	تشجع الإدارة الرقمية في المؤسسة على التعاون والمشاركة بين الموظفين لتعزيز امن المعلومات	ت	5	5	14	5	1	3.26	1.048	موافقة
		ن	16,7 %	16,7 %	46,7 %	16,7 %	3,3 %			
17	يلتزم جميع الموظفين بإتباع إجراءات أمنية عند استخدام الأدوات الرقمية لضمان حماية المعلومات	ت	7	10	9	3	1	3.63	1.066	موافقة
		ن	23,3 %	33,3 %	30 %	10 %	3,3 %			
18	يتم تطبيق سياسات أم المعلومات صارمة ومتوافقة مع الإدارة الرقمية لضمان سلامتها وسرية الوصول إليها	ت	4	16	2	7	1	3.50	1.106	موافقة
		ن	13,3 %	53,3 %	6,7 %	23,3 %	13,3 %			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

وبوجه عام، تكشف هذه النتائج أن المؤسسة تولي اهتماما واضحا بجوانب أمن المعلومات، وتطبق عددا من الممارسات الجيدة في هذا المجال، إلا أن هناك مؤشرات تدل على ضرورة تعزيز التكوين الداخلي وتحسين وضوح السياسات الأمنية، من أجل تقليص التباين بين الموظفين وزيادة فعالية تطبيق نظم الحماية الرقمية.

تشير نتائج تحليل إجابات أفراد العينة حول محور "الإدارة الرقمية وأمن المعلومات"إلى وجود إدراك إيجابي ووعي واضح لدى المشاركين بأهمية التكامل بين هذين الجانبين داخل المؤسسة. فقد جاءت جميع العبارات ضمن نطاق "موافقة"، مما يدل على أن أفراد العينة يعترفون بدور الإدارة الرقمية في تعزيز أمن المعلومات.

أظهرت العبارة رقم (13) التي تنص على أن المؤسسة تعتمد على الإدارة الرقمية لتحسين حماية المعلومات وسرية البيانات متوسطًا حسابيًا بلغ (4.03)، ما يعكس موافقة قوية نسبيا من طرف المشاركين، على الرغم من وجود انحراف معياري مرتفع نوعًا ما(1.376) ، وهو ما قد يشير إلى تباين في تطبيق هذه الممارسة أو تفاوت في الإدراك بين الموظفين باختلاف أقسامهم أو مسؤولياتهم.

أما العبارة رقم (14) فقد حصلت على أعلى متوسط حسابي في هذا المحور(4.20) ، مما يشير إلى ثقة قوية لدى أفراد العينة في قدرة الإدارة الرقمية على توفير آليات فعالة لحماية المعلومات من التهديدات الخارجية، وقد دعم ذلك انحراف معياري معتدل نسبيًا (1.214)، وهو ما يدل على اتفاق نسبي بين المجيبين حول هذه النقطة.

وفيما يخص مساهمة الإدارة الرقمية في تعزيز وعي الموظفين بأهمية أمن المعلومات (العبارة 15)، فقد بلغ المتوسط الحسابي (3.86)، ما يدل على موافقة واسعة، مع انحراف معياري (1.252)يعكس وجود تفاوت متوسط في تقييم الأفراد، ربما ناتج عن اختلاف مستويات التكوين أو وعي الموظفين داخل المؤسسة.

كما تؤكد العبارة رقم (16) على أن الإدارة الرقمية تشجع على التعاون والمشاركة بين الموظفين لتعزيز أمن المعلومات، وقد سجلت متوسطًا قدره (3.26)، وهو أقل من المتوسطات السابقة، مما يدل على موافقة أقل نسبيا، بالرغم من الانحراف المعياري المنخفض نسبيًا (1.048)، مما يشير إلى أن هناك اتفاقًا عامًا حول هذا الرأي، ولكن بدرجة أقل حماسة مقارنة بالعبارات السابقة.

وبالنسبة للعبارة (17)، التي تطرقت إلى التزام الموظفين بإتباع الإجراءات الأمنية عند استخدام الأدوات الرقمية، فقد حصلت على متوسط (3.63) مع انحراف معياري (1.066)، ما يدل على توجه إيجابي جيد ومستقر نسبيا، مع ملاحظة أن هذا الالتزام قد لا يكون موحدا بين جميع الموظفين.

أخيرا، أظهرت العبارة رقم (18) حول تطبيق سياسات أمن معلومات صارمة ومتوافقة مع الإدارة الرقمية متوسطا حسابيا (3.50)، مع انحراف معياري (1.106)، ما يعكس موافقة معتدلة من طرف العينة، ويشير إلى إمكانية وجود ثغرات أو اختلاف في مستوى الصرامة والوضوح في السياسات الأمنية المطبقة.

بوجه عام، تُظهر النتائج أن هناك ترابطا واضحا بين الإدارة الرقمية وأمن المعلومات في المؤسسة المدروسة، إلا أن التطبيق العملي لهذه العلاقة قد يختلف بين الأقسام والموظفين، مما يستوجب تعزيز التكوين والتوعية، وتوحيد السياسات والإجراءات الأمنية لتكون أكثر فعالية واتساقا.

4-5-اختبار فرضيات الدراسة.

- ✓ **الفرضية الأولى: بوجد تأثير ايجابي لتطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات لديه عند مستوى الدلالة 0.05**

-الفرضية الصفرية (H_0):

✓ لا يوجد تأثير ايجابي لتطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات لديه عند مستوى الدلالة 0.05

-الفرضية البديلة (H_1)

✓ يوجد تأثير ايجابي لتطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات لديه عند مستوى الدلالة 0.05

الجدول رقم (13): نتائج تحليل المنحنى لاختبار تأثير ايجابي لتطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات لديه عند مستوى الدلالة 0.05

المتغير التابع تطبيق الإدارة الرقمية	المتغير المستقل: مستوى تعزيز أمن المعلومات			
	معامل الارتباط	معامل الانحدار	معامل التحديد	مستوى المعنوية
	0.730	0.533	0.516	0.000

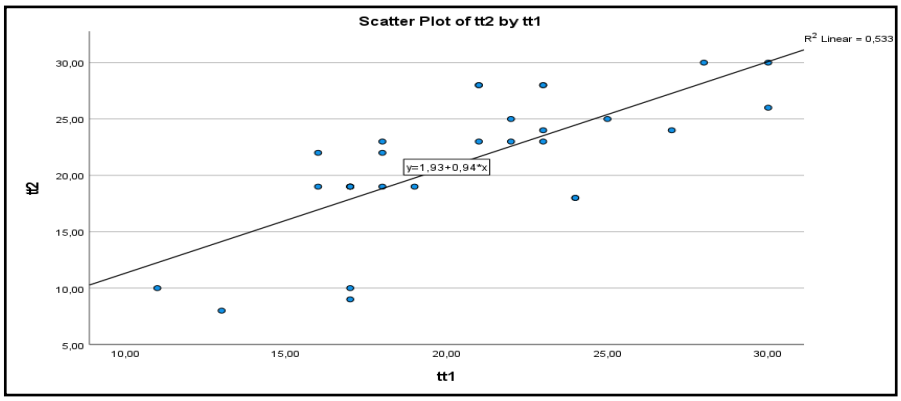
المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج (SPSS).

الجدول(14): تحليل التباين لاختبار تأثير ايجابي لتطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات لديه عند مستوى الدلالة 0.05

المتغير التابع	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	مستوى المعنوية
بين المجموعات	559.595	1	559.595	31.959	0.000
داخل المجموعات	490.272	28	17.510		
المجموع	1049.867	29			

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

الشكل رقم(01):منحنى العلاقة بين المتغير التابع والمتغير المستقل



المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

✓ **حيث tt1 تمثل الإدارة الرقمية**

✓ **حيث 2tt تمثل تعزيز أمن المعلومات**

في ضوء نتائج تحليل الانحدار وتحليل التباين (ANOVA) باستخدام برنامجSPSS ، تبين وجود علاقة ذات دلالة إحصائية بين تطبيق الإدارة الرقمية في المؤسسات ومستوى تعزيز أمن المعلومات. إذ أظهر معامل الارتباط (0.730) وجود علاقة ارتباط إيجابية قوية بين المتغيرين، في حين أن معامل التحديد ($R^2 = 0.516$) يشير إلى أن ما نسبته 51.6% من التغير في مستوى أمن المعلومات يمكن تفسيره من خلال تطبيق الإدارة الرقمية. كما كشفت نتائج تحليل التباين عن قيمة (F = 31.959)ودلالة إحصائية عالية(Sig. = 0.000) ، وهي أقل من مستوى الدلالة المعتمد (0.05)، مما يدل على معنوية النموذج

الاحصائي المستخدم. وعليه، يمكن رفض الفرضية الصفرية وقبول الفرضية البديلة التي تنص على وجود تأثير إيجابي لتطبيق الإدارة الرقمية في المؤسسات على مستوى تعزيز أمن المعلومات. وتؤكد هذه النتائج أهمية التحول الرقمي كأداة فعالة في دعم البنية الأمنية للمعلومات داخل المؤسسات وتعزيز قدرتها على حماية البيانات ومجابهة التهديدات السيبرانية.

✓ **الفرضية الثانية:**

-الفرضية الصفرية(H_0) :"استخدام تقنيات الإدارة الرقمية لا يساهم في تقليل حوادث اختراق أمن المعلومات بنسبة ملحوظة". عند مستوى الدلالة 0.05.

-الفرضية البديلة:(H_1) "استخدام تقنيات الإدارة الرقمية يساهم في تقليل حوادث اختراق أمن المعلومات بنسبة ملحوظة". عند مستوى الدلالة 0.05.

4-5-1-اختبار T-Student

الجدول رقم (15): الفروق بين المتوسط الحسابي لإجابات أفراد العينة على إجمالي عبارات المحور الأول والمتوسط الفرضي.

T	مستوى المعنوية Sig	مستوى الدلالة	المتوسط الفرضي	المتوسط الحسابي	الانحراف المعياري	درجة الحرية
4.250	0.001	0.05	18	22.50	5.79	29

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

أظهرت نتائج **اختبار (T)** الواردة في **الجدول رقم (15)** أن المتوسط الحسابي لإجابات أفراد العينة بلغ (22.50)، وهو أعلى من المتوسط الفرضي (18)، بانحراف معياري قدره (5.79). كما بلغت قيمة (T) المحسوبة (4.250)، بينما كان مستوى الدلالة (Sig) يساوي (0.001)، وهو أقل بكثير من مستوى الدلالة المعتمد.(0.05)

بناء على هذه النتائج، نلاحظ وجود فرق دال إحصائيًا بين المتوسط الفرضي والمتوسط الفعلي، مما يعني أن استخدام تقنيات الإدارة الرقمية ساهم بشكل ملحوظ في تقليل حوادث اختراق أمن المعلومات داخل المؤسسات. بالتالي، **نرفض الفرضية الصفرية** ونقبل الفرضية البديلة التي تنص على أن استخدام تقنيات الإدارة الرقمية يساهم فعلاً في الحد من حوادث الاختراق، وهو ما يعكس الدور الإيجابي الذي تلعبه الإدارة الرقمية في تعزيز أمن المعلومات.

✓ **الفرضية الثالثة:** لا توجد فروق ذات دلالة إحصائية عند مستوى (0.05) بين متوسطات إجابات أفراد العينة حول أثر الإدارة الرقمية على تعزيز أمن المعلومات تُعزى إلى المستوى التعليمي

-الفرضية البديلة (H_1): توجد فروق ذات دلالة إحصائية عند مستوى (0.05) بين متوسطات إجابات أفراد العينة حول أثر الإدارة الرقمية على تعزيز أمن المعلومات تعزى إلى المستوى التعليمي

الجدول (16): اختبار فرضية توجد فروق ذات دلالة إحصائية عند مستوى (0.05) بين متوسطات إجابات أفراد العينة حول أثر الإدارة الرقمية على تعزيز أمن المعلومات تُعزى إلى المستوى التعليمي

المتغير التابع	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة F	مستوى المعنوية
بين المجموعات	94.300	4	23.575	0.669	0.620
داخل المجموعات	881.200	25	35.248		

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS.V27

✓ بلغت قيمة Fالمحسوبة (0.669)، وهي قيمة صغيرة.

- ✓ مستوى الدلالة (**Sig = 0.620**) أكبر من مستوى الدلالة المعتمد.(**0.05**)

وبناءً على ذلك، وبما أن قيمة (Sig) أكبر من 0.05، فإننا **نقبل الفرضية الصفرية(H0)** التي تنص على أنه **لا توجد فروق ذات دلالة إحصائية** بين متوسطات إجابات الأفراد حول أثر الإدارة الرقمية على تعزيز أمن المعلومات تُعزى إلى المستوى التعليمي. **بمعنى آخر:** اختلاف المستوى التعليمي لأفراد العينة لم يؤثر بشكل معنوي على تقييمهم لدور الإدارة الرقمية في تعزيز أمن المعلومات

5-خاتمة: على ضوء ما سبق ونظرا لما تم التوصل إليه من الجانب النظري والتطبيقي وما أضفت إليه الدراسات السابقة، حيث تعد الإدارة الرقمية توجها معاصرا هاما ونهجا حديثا تسعى المؤسسات إلى اعتماده وتطويره، لمواكبة التغيرات السريعة في بيئة الأعمال من خلال تحسين كفاءتها وزيادة فعاليتها باستخدام التكنولوجيا الحديثة وتحليل البيانات مما تساهم في القضاء على الفساد الإداري وتعزيز الوعي الأمني بين الموظفين من خلال التدريب المستمر وتطوير ثقافة أمنية تركز على أهمية حماية المعلومات داخل المؤسسات، كما تشجع على تبني الحلول التقنية المبتكرة. أما بالنسبة لأمن المعلومات يعتبر من الركائز الأساسية في العصر الرقمي، نظرا لما يشهده العالم من تطور تقني متسارع وتزايد الاعتماد على الأنظمة الرقمية في مختلف مجالات الحياة حيث تكمن أهمية أمن المعلومات في حماية المعلومات والبيانات من السرقة سواء كانت بيانات شخصية أو مالية أو بيانات تخص المؤسسة، كما يساهم في تعزيز ثقة العملاء والمستخدمين من خلال المراقبة المستمرة للأنظمة بصفة دورية.

في الختام يمكن القول أن الإدارة الرقمية ليست فقط أداة للرفع من الأداء الإداري، بل تعتبر عنصر جوهري لا يمكن الاستغناء عنه بسهولة في تبني منظومة محمية أمنيا، لأنها بدورها تحمي المعلومات للحفاظ على استمرارية المؤسسة واستقرارها في عصر التكنولوجيات الحديثة.

5-1- نتائج الدراسة: وبالاعتماد على التحليل النظري لدور الإدارة الرقمية في تعزيز أمن المعلومات بمؤسسة اتصالات الجزائر من خلال التحليل الميداني للعلاقة بين المتغيرين لاختبار الفرضيات المطروحة تم استخلاص مجموعة من النتائج والمتمثلة في:

- ✓ تلعب الإدارة الرقمية دورا كبيرا في تسهيل الحصول على الوثائق وتعزيز أمن المعلومات داخل المؤسسات، من خلال الاعتماد على تطبيق تقنيات حديثة توفر الوقت والتكلفة والجهد.
- ✓ تعزز الإدارة الرقمية الرقابة الداخلية وتعمل على التقليل من المخاطر ومختلف الانتهاكات الأمنية.
- ✓ تساعد الإدارة الرقمية في تقييم المخاطر المحتملة ووضع استراتيجيات مناسبة للتصدي لها.
- ✓ يقوم أمن المعلومات على ثلاثة أبعاد رئيسية: السرية، السلامة، وتوافر المعلومات للمستخدمين المصرح لهم عند الحاجة.
- ✓ تعتمد الإدارة الرقمية على مجموعة من التقنيات لحماية المعلومات داخل المؤسسة من خلال الاعتماد على برامج مكافحة البرمجيات الخبيثة.
- ✓ أثبتت الدراسة تأثير تطبيق الإدارة الرقمية في مؤسسة اتصالات الجزائر عند مستوى دلالة 0,05 تم حسابها باختبار T-student حيث قدر المتوسط الحسابي ب(50 ,22) والانحراف المعياري ب (5,59)، أي أن الإدارة الرقمية تساهم بدرجة

كبيرة في تعزيز أمن المعلومات، حيث بلغت قيمة الاحتمال 0,001) أي أقل من مستوى دلالة (0,05) وبالتالي هذا مؤشر قوي لتأثير الإدارة الرقمية على تعزيز أمن المعلومات داخل المؤسسة.

5-2- اقتراحات الدراسة: بناءا على النتائج المتحصل عليها من الجانبين النظري والتطبيقي، تم وضع مجموعة من الاقتراحات والمتمثلة في:

- ✓ تعزيز الثقافة الرقمية داخل المؤسسة للتشجيع على الابتكار والتحسن المستمر.
- ✓ تفعيل نظام رقمي لإدارة شؤون الموظفين مثل حالات الحضور والغياب.
- ✓ تنظيم برامج تدريبية لتعزيز مهارات الموظفين في استخدام التكنولوجيات الرقمية الحديثة.
- ✓ حفظ نسخ احتياطية من البيانات بصفة دورية لضمان استعادها في حال حدوث أي فقدان للمعلومات.

5-3- أفاق الدراسة:

- ✓ النظام الرقمي في المؤسسة يعمل على تحسين جودة الخدمات والرفع من كفاءة الموظفين.
- ✓ فتح أفاق للسهر على تحديث البرمجيات.
- ✓ البرامج التدريبية تساهم في تقليل حوادث الاختراق داخل المؤسسات.

6- المصادر والمراجع:

1-أحلام منصور، الحلول الحديثة لأمن المعلومات لمواجهة المخاطر الالكترونية. مجلة دراسات في الاقتصاد والتجارة المالية ، المجلد 07 ، العدد 01، 2018، ص312.

2-أمنة قذايفية، إستراتيجية أمن المعلومات. مجلة أبعاد اقتصادية ، المجلد 06، العدد 01، 2016، ص166.

3-خالد بن سليمان الغثير، القحطاني محمد بن عبد الله، أمن المعلومات بلغة ميسرة. مكتبة فهد الملك الوطنية، 2009، ص 20،

4-رشيد حفصي، نبيل حليمي، أهمية الأمن المعلوماتي بالمؤسسة الاقتصادية -دراسة حالة مديرية توزيع الطهرباء والغاز. المجلة الجزائرية للدراسات الاقتصادية والإدارية، المجلد 2، العدد 01، 2022، ص 45.

5-عدنان عواد شوابكة.، دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، المجلد 11، العدد 04، 2019، ص ص 169-170.

6-عيواج سامية، دور الإدارة الرقمية في تحسين الخدمة العمومية -دراسة ميدانية ببريد الجزائر بولاية برج بوعريريج. مجلة بحوث ودراسات في الميديا الجديدة ، المجلد 5 ، العدد 01، 2024، ص 07.

7-كباش الطاهر، نبيل دربيخ، الادارة الرقمية للمصالح البيداغوجية بالجامعات الجزائرية -دراسة نموذجية لنظام SCOL بكلية العلوم بجامعة المدية. مجلة البحوث والدراسات العلمية ، المجلد 18، العدد 01، 2024، ص05.

8-مقبي ميمونة، الإدارة الرقمية في تحسين مستوى الخدمات الصحية من وجهة نظر إداري المؤسسة الاستشفائية محمد بوضياف. مجلة الأصيل للبحوث الاقتصادية والإدارية ، المجلد 8، العدد 01، 2024، ص 383.

9-وليد زكريا، أبو بكر عبد النبي، محمد عبد البارئ محمد جمال، إطار مقترح للعلاقة بين تطبيق آليات الإدارة الرقمية وتحسين بيئة العمل. مجلة العلوم التجارية والبيئية ، المجلد 4، العدد 01، 2025، ص ص 175-176.