(6)

إدارة التغيير كمدخل إستراتيجى لتعزيز الأمن السيبرانى وحماية الطفل في البيئة الرقمية "مراجعة سردية في ضوء التحول الرقمى"

د/ على محمد على محمد أحمد
دكتوراه الفلسفة فى التربية للطفولة المبكرة،قسم العلوم الاساسية
كلية التربية للطفولة المبكرة جامعةالإسكندرية
عضو وحدة التدريب الميدانى بالمعهد اللعالى للخدمة الاجتماعية بالاسكندرية

إدارة التغيير كمدخل إستراتيجي لتعزيز الأمن السيبراني وحماية الطفل في البيئة الرقمية "مراجعة سردية في ضوء التحول الرقمي "

د/ علي محمد علي محمد احمد[5]

ملخص:

يهدف هذا البحث إلى تقديم معالجة تكاملية تجمع بين المفاهيم الثلاثة (إدارة التغيير، الأمن السيبراني، حماية الطفل).

تتمحور إشكالية البحث حول الكيفية التي يمكن من خلالها توظيف إدارة التغيير كمدخل استراتيجي لتعزيز الأمن السيبراني وحماية الطفل في البيئة الرقمية، حيث تنتمي هذه الدراسة إلى المراجعات الأدبية السردية حيث تستند إلى تجميع وتحليل الأدبيات المتوفرة في مجالات إدارة التغيير، الأمن السيبراني، وحماية الطفل في البيئة الرقمية، وقد تم الاعتماد على المنهج الوصفي التحليلي في صورته السردية، وقد توصلت نتائج الدراسة على مستوى المفاهيم النظرية أن الأمن السيبراني لم يعد مقتصراً على الجوانب التقنية، بل بات يشمل أبعاداً اجتماعية وتربوية، وقصور السياسات الحالية التي تتسم غالباً بالطابع التفاعلي أكثر من الوقائي كما أظهرت النتائج أن دمج إدارة التغيير في استراتيجيات الأمن السيبراني يسهم في بناء ثقافة مؤسسية داعمة للأمن الرقمي، كما كشف المراجعة أن تبني نموذج تكاملي يدمج بين (إدارة التغيير – الأمن السيبراني – حماية الطفل) من شأنه أن يوفر أساساً عملياً لتطوير سياسات وقائية أكثر استدامة وفاعلية داخل مؤسسات رعاية الطفل.

الكلمات المفتاحية: إدارة التغيير، الأمن السيبراني، البيئة الرقمية، حماية الطفل.

---

(5) دكتوراه في التربية للطفولة المبكرة، كلية التربية للطفولة المبكرة، جامعة الإسكندرية، عضو وحدة التدريب الميداني بالمعهد العالي للخدمة الاجتماعية بالإسكندرية.

- تم التوثيق بنظام APA.

Change Management as a Strategic Approach to Enhancing Cybersecurity and Protecting Children in the Digital Environment :A Narrative Review in the Context of Digital Transformation

Abstract:

This study aims to provide an integrative approach that brings together three key concepts: change management, cybersecurity, and child protection. The research problem centers on how change management can be employed as a strategic approach to enhance cybersecurity and safeguard children in the digital environment. The study adopts a narrative literature review methodology, relying on the collection and analysis of existing literature in the fields of change management, cybersecurity, and child protection in digital contexts. Using a descriptive-analytical narrative approach, the findings reveal at the conceptual level that cybersecurity is no longer confined to technical aspects but also encompasses social and educational dimensions. The study highlights the limitations of current policies, which are often reactive rather than preventive. Moreover, the results indicate that integrating change management into cybersecurity strategies contributes to building an institutional culture that supports digital safety, The review further demonstrates that adopting a comprehensive model that integrates change management, cybersecurity, and child protection can provide a practical foundation for developing more sustainable and effective preventive policies within child care institutions.

Keywords:

Change Management, Cybersecurity, Digital Environment, Child Protection.

المقدمة:

يشهد العالم في العقدين الأخيرين تحولاً رقمياً متسارعاً أعاد تشكيل أنماط الحياة والتعليم والعمل والتواصل الاجتماعي، فقد أصبح الأطفال والمراهقون من أكثر الفئات استخداماً للتقنيات الرقمية، حيث تشير تقارير اليونيسف (2023) إلى أن ما يزيد عن 80% من الأطفال حول العالم يتصلون بالإنترنت بصورة يومية، الأمر الذي يفتح أمامهم فرصاً للتعلم والتطور، ولكنه في الوقت نفسه يعرضهم لمجموعة واسعة من المخاطر مثل التنمر الإلكتروني، الاستغلال، والإدمان على المحتوى الرقمي.

وقد بين تقرير الاتحاد الدولي للاتصالات (ITU, 2023) أن ما يقارب نصف الأطفال عالمياً تعرضوا لشكل من أشكال التهديد الرقمي، فيما أشار تقرير Cybersecurity Ventures (2022)إلى أن الجرائم الإلكترونية ضد الأطفال ارتفعت بنسبة تتجاوز 85% خلال جائحة كورونا .وعلى المستوى المحلي والإقليمي، أظهرت دراسة الشهري (2021) في السعودية أن 57%من الأطفال تعرّضوا لمضايقات عبر الشبكات الاجتماعية، بينما كشفت دراسة البدري (2020) أن برامج التثقيف الرقمي ساهمت في خفض التنمر الإلكتروني بنسبة 40% بين الأطفال المشاركين.

أما على المستوى الدولي، فقد وجدت دراسة Pew Research (Anderson & Jiang, 2018)أن 95%من المراهقين الأمريكيين يمتلكون هواتف ذكية، و 45%منهم متصلون بالإنترنت بشكل دائم تقريباً، في حين أوضح تقرير Ofcom (2023) أن 77%من الأطفال البريطانيين (5–15 سنة) يمتلكون جهازاً ذكياً شخصياً، وأن 62% من أولياء الأمور يشعرون بالقلق من تعرض أبنائهم لمحتوى ضار .وتؤكد نتائج المسح الأسترالي (Australian eSafety Commissioner, 2022) أن 67%من الأطفال والمراهقين واجهوا شكلاً من أشكال الإساءة أو التنمر عبر الإنترنت، و30% شاهدوا محتوى غير لائق خلال عام واحد فقط.

ورغم الجهود المبذولة عبر تشـــريعات دولية مثل اللائحة العامة لحماية البيـانـات الأوروبيـة (GDPR)، أو المبـادرات الأمميـة مثـل Child Online Protection الصـادرة عن الاتحاد الدولي للاتصـالات، إلا أن معظم هذه التدابير ما تزال ذات طبيعة تفاعلية (Reactive) تركز على التعامل مع المشـــكلات بعد وقوعها، أكثر من كونها وقائية واســـتباقية. وهنا تبرز أهمية إدارة التغيير كمدخل اســـتراتيجي، إذ يرى Kotter (1996) أن إدارة التغيير هي عملية قيادة التحول المؤســـســـي عبر رؤية واضـــحة وإشـــراك الأطراف المعنية، فيما أكد Burnes (2017)أن نجاح المؤســـســـات في البيئات المتغيرة مرهون بقدرتها على دمج استراتيجيات جديدة بشكل مستدام.

وتكمن أهمية هذا الموضـــوع في أنه يتناول فجوة بحثية قائمة بين ثلاثة مجالات عادة ما تُدرس بصـورة منفصـلة: إدارة التغيير، الأمن السـيبراني، وحماية الطفل في البيئة الرقمية، ومن هنا تأتي الدراســة الحالية لتقديم معالجة تكاملية تربط بين هذه المفاهيم، وتوضـــح كيف يمكن توظيف إدارة التغيير كمدخل اســـتراتيجي لتعزيز الأمن السيبراني وتطوير سياسات وقائية أكثر فاعلية لحماية الطفل.

وعليه، فإن دمج إدارة التغيير ضـــمن اســـتراتيجيات الأمن الســـيبراني يمثل مدخلاً عملياً لتطوير ســـياســـات حماية الطفل في البيئة الرقمية على نحو اســـتباقي وأكثر فاعلية، وذلك من خلال صـــياغة خطط واضـــحة، تدريب المعنيين، إشـــراك الأسر والمدارس، وبناء تحالفات مجتمعية ومؤسسية تعزز الأمن الرقمي للأطفال.

أولاً: مشكلة الدراسة:

يشـــهد العالم المعاصـــر طفرة غير مســـبوقة في وتيرة التحول الرقمي، حيث بـاتت التقنيـات الرقميـة والإنترنـت جزءاً لا يتجزأ من حيـاة الأطفـال والمراهقين. وتشـــير تقارير اليونيســـف (UNICEF, 2023) إلى أن ما يزيد عن 80% من الأطفال حول العالم يتصـلون بالإنترنت بشـكل يومي، وهو ما يفتح أمامهم فرصـاً واسـعة للتعلم والتواصـل، لكنه في الوقت ذاته يجعلهم عرضـة لمخاطر متعددة مثل الاستغلال، التنمر الإلكتروني، الإدمان، والوصول إلى محتويات غير مناسبة.

في المقابل، يوضح الاتحاد الدولي للاتصالات (ITU, 2023) أن نصف الأطفال تقريباً قد تعرضوا لشكل من أشكال التهديد أو الخطر الرقمي، وهو ما يعكس هشاشة أنظمة الحماية الحالية. وقد دعمت هذه النتائج تقارير Cybersecurity Ventures (2022)التي كشفت عن زيادة بنسبة 85% في الجرائم الإلكترونية الموجهة ضد الأطفال خلال جائحة كوفيد-19، مما يكشف قصور الأدوات والسياسات الأمنية التقليدية. ورغم وجود مبادرات تشريعية وتنظيمية مثل اللائحة الأوروبية العلمة لحماية البيانات (GDPR) أو برنامج Child Online Protectionالتابع للاتحاد الدولي للاتصالات، إلا أن معظم هذه المبادرات تظل ذات طابع تفاعلي Reactive أكثر من كونها استباقية .Proactive ومن هنا تبرز الحاجة إلى إطار استراتيجي يدمج بين إدارة التغيير- باعتبارها أداة مؤسسية فعالة لقيادة التحول- وبين الأمن السيبراني لتعزيز آليات حماية الطفل.

وبناءً عليه، تتحدد مشكلة الدراسة في السؤال الرئيس الآتي:

كيف يمكن توظيف إدارة التغيير كمدخل استراتيجي لتعزيز الأمن السيبراني بما يضمن حماية أكثر فاعلية للأطفال في البيئة الرقمية؟

أسئلة الدراسة:

تتمحور مشكلة الدراسة حول الكيفية التي يمكن من خلالها توظيف إدارة التغيير كمدخل استراتيجي لتعزيز الأمن السيبراني وحماية الطفل في البيئة الرقمية. وانطلاقًا من ذلك، تسعى الدراسة للإجابة عن الأسئلة الرئيسة الآتية:

1- ما المفاهيم النظرية الأساسية التي تناولتها الأدبيات السابقة في مجالات: إدارة التغيير، الأمن السيبراني، وحماية الطفل في البيئة الرقمية؟
2- ما اهم المخاطر والتحديات الرقمية التي تواجه الأطفال في ظل التحول الرقمي، وما الآليات الحالية لحمايتهم؟
3- كيف يمكن توظيف **إدارة التغيير كمدخل استراتيجي** لتعزيز فعالية سياسات وإجراءات الأمن السيبراني الخاصة بحماية الأطفال؟

4- ما ملامح **التصور التكاملـــــي المقترح** الذي يمكن أن يدمج بين إدارة التغيير والأمن السيبراني وحماية الطفل، ويسهم في صياغة سياسات وقائية واستباقية أكثر فاعلية في ظل التحول الرقمي؟

أهداف الدراسة:

تهدف هذه الدراسة إلى تقديم معالجة تكاملية تجمع بين المفاهيم الثلاثة (إدارة التغيير، الأمن السيبراني، حماية الطفل)، وذلك من خلال الأهداف التالية:

1- التعرف على المفاهيم النظرية الأســاســية التي تناولتها الأدبيات الســابقة في مجالات: إدارة التغيير، الأمن السيبراني، وحماية الطفل في البيئة الرقمية؟
2- التعرف على اهم المخاطر والتحديات الرقمية التي تواجه الأطفال في ظل التحول الرقمي، وما الآليات الحالية لحمايتهم؟
3- توضيح طبيعة دور إدارة التغيير كمدخل استراتيجي لتعزيز فعالية سياسات وإجراءات الأمن السيبراني الخاصة بحماية الأطفال؟
4- صياغة **تصور تكاملـــــي مقترح** يدمج بين إدارة التغيير والأمن السيبراني وحماية الطفل، ويسهم في صياغة سياسات وقائية واستباقية أكثر فاعلية في ظل التحول الرقمي؟

اهمية الدراسة:

تنبع أهمية هذه الدراسة من تلاقي ثلاثة محاور أساسية في بناء مستقبل أكثر أماناً للأطفال في العصــر الرقمي، وهي :مؤســســات رعاية الطفل، إدارة التغيير، والأمن السيبراني.

ففي الوقت الذي تتزايد فيه التحديات المرتبطة بالمخاطر الرقمية كالتنمر الإلكتروني، والاســتغلال، والاختراقات الأمنية، تصــبح الحاجة ملحة إلى تطوير آليات شمولية تستند إلى ممارسات إدارية مرنة واستراتيجيات تغيير فعالة قادرة على حماية الأطفال وضمان رفاههم (UNICEF, 2021).

تسهم هذه الدراسة في:

1- سد فجوة معرفية من خلال تقديم تصور متكامل يجمع بين إدارة التغيير والأمن السيبراني في سياق حماية الطفل، وهو منظور لم يُتناول بترابط واضح في الأدبيات السابقة.
2- تزويد صناع القرار والعاملين بمؤسسات رعاية الطفل برؤية عملية لصياغة سياسات وإجراءات أكثر فاعلية في مواجهة التحديات الرقمية.
3- دعم السياسات العامة الرامية إلى تعزيز الأمن السيبراني المجتمعي عبر دمجه في استراتيجيات حماية الطفولة.
4- تعزيز الوعي المجتمعي والمؤسسي بأهمية تبني سياسات وقائية واستباقية لمواجهة مخاطر الفضاء السيبراني.

وبذلك، تكتسب الدراسة أهميتها في كونها لا تقتصر على الجانب النظري، بل تطرح إطاراً عملياً مقترحاً يمكن لمؤسسات رعاية الطفولة الاسترشاد به لحماية الأطفال في ظل التحولات الرقمية المتسارعة.

الإطار النظري:

مفاهيم الدراسة:

[1] مفهوم مؤسسات رعاية الطفل:

تشير مؤسسات رعاية الطفل إلى "المنظمات الرسمية وغير الرسمية التي تُعنى بحماية الأطفال وتوفير بيئة آمنة لنموهم الجسدي، النفسي، والاجتماعي. وتشمل هذه المؤسسات دور الحضانة، المدارس، المراكز المجتمعية، والمبادرات الحكومية أو غير الحكومية التي تعمل على تلبية احتياجات الأطفال في ظل التغيرات الاجتماعية والتكنولوجية" (UNICEF, 2021). "وتُعد هذه المؤسسات خط الدفاع الأول في تعزيز ثقافة الاستخدام الآمن للتكنولوجيا الرقمية، وذلك من خلال التوعية، وضع السياسات للداخلية، وتطبيق أدوات الرقابة الرقمية" (Livingstone et al., 2017).

[2] مفهوم حماية الطفل:

"حماية الطفل تعني مجموع السياسات والإجراءات التي تهدف إلى وقاية الأطفال من جميع أشكال الإساءة والاستغلال والإهمال والعنف، سواء في البيئات التقليدية أو في البيئة الرقمية" (Council of Europe, 2020).

– آليات حماية الطفل:

"تتضمن آليات الحماية برامج الرقابة الأبوية، التشفير، سياسات الخصوصية، التدريب على مهارات الوعي السيبراني، إضافة إلى التعاون بين المؤسسات التعليمية والأسر والمجتمع المدني" (ITU, 2023) وتشير الدراسات إلى "أن الحماية الأكثر فاعلية هي التي تمزج بين الحلول التقنية(Technical Solutions) والتدخلات التربوية والاجتماعية"(Livingstone & Stoilova, 2021) .

[3] إدارة التغيير:

تُعرّف إدارة التغيير بأنها "عملية منهجية تهدف إلى الانتقال من الوضع الحالي إلى الوضع المستقبلي المرغوب من خلال التخطيط، التنفيذ، ومتابعة التحول داخل المؤسسات" (Kotter, 1996) وترى الأدبيات أن إدارة التغيير لا تقتصر على إدخال أدوات جديدة، بل تشمل بناء ثقافة تنظيمية قادرة على التكيف والاستجابة للتغيرات (Burnes, 2017) أما استراتيجيات إدارة التغيير فتتضمن:

- **الرؤية والقيادة:** صياغة رؤية واضحة وتوجيه المنظمة نحوها.
- **إشراك الأطراف المعنية:** تعزيز المشاركة بين الموظفين، الأسر، والمجتمع.
- **بناء القدرات:** تدريب الموارد البشرية على المهارات الرقمية والأمنية.
- **التقييم المستمر:** متابعة النتائج وتعديل الخطط بناءً على التغذية الراجعة (Hiatt, 2006).

تُعد إدارة التغيير (Change Management) مجموعة من العمليات والأدوات والمنهجيات المصممة لدعم الانتقال من حالة راهنة إلى حالة مستقبلية مرغوبة داخل أي منظومة، سواء كانت مؤسسة، أو نظاماً، أو حتى مجتمعاً بأكمله.

ويكمن الهدف الأساسي لها في تقليل مقاومة الأفراد، ضمان تبنّي الممارسات والسياسات الجديدة، وتحقيق أهداف استراتيجية مستدامة (Cameron & Green, 2020).

ومن أبرز النماذج المستخدمة عالميًا في هذا المجال:

1) **نموذج كوتر ذو الخطوات الثمانية:** طوّره جون كوتر (Kotter, 2012) ويُستخدم لقيادة التغيير على المستوى المؤسسي. يقوم على ثماني خطوات متسلسلة:
   - خلق إحساس بالإلحاح.
   - بناء قيادة ميسرة للتغيير.
   - صياغة رؤية واستراتيجية واضحة.
   - التواصل المستمر مع أصحاب المصلحة.
   - تمكين الأفراد من العمل وتذليل العقبات.
   - تحقيق مكاسب قصيرة المدى.
   - البناء على النجاحات لتعزيز التغيير.
   - ترسيخ التغيير في الثقافة المؤسسية.

   هذا النموذج يساعد المؤسسات التعليمية ومؤسسات رعاية الأطفال على غرس ثقافة الأمن الرقمي وتبني سياسات مستدامة لحماية الطفل.

2) **نموذج أدكار (ADKAR Model):** طورته مؤسسة Prosci (Hiatt, 2006)، ويركز على التغيير على مستوى الأفراد من خلال خمس مراحل:
   - **(الوعي) Awareness:** إدراك الحاجة للتغيير.
   - **(الرغبة) Desire:** وجود دافع شخصي لتبني التغيير.
   - **(المعرفة) Knowledge:** توفير المعلومات والمهارات اللازمة.
   - **(القدرة) Ability:** تمكين الأفراد من تطبيق السلوكيات الجديدة.
   - **(التعزيز) Reinforcement:** ترسيخ التغيير وضمان استمراره.

يُعد هذا النموذج مهمًا جداً في ســـياق حملية الطفل في البيئة الرقمية، إذ يضمن مشاركة وتبنّي الأفراد (المعلمين، أولياء الأمور، الأطفال) للسياسات الأمنية بشكل تدريجي ومستدام.

وعليه، فإن تبنّي هذين النموذجين يسهم في صياغة مدخل استراتيجي متكامل يدمج بين إدارة التغيير والأمن السيبراني لحماية الأطفال في البيئة الرقمية.

أهمية إدارة التغيير:

لقد اخترقت مفاهيم ومداخل التغيير كل جانب من جوانب السلوك التنظيمي، حيث أصـــبحت الفكرة المهيمنة لنظرية الإدارة الحديثة تتمثل في فهم وخلق التغيير والتكيف معه، وأصبح ينظر إلى التغيير على أنه المفتاح الأساسي لنجاح المنظمات وتميزها (دافيد ويلسون، 2001، 20).

حيث يعد تبني فكرة أو ســـلوك جديد من قبل المنظمة بمثابة تأكيد على ضـرورة التغيير التنظيمي في إعادة هيكلة الموارد والإمكانيات لزيادة القدرات وخلق قيمة وتحسين العوائد والنتائج لأصحاب المصالح في المنظمة (غسان اللامي، 2007، 94).

أهمية إدارة التغيير في السياقات التقنية والحماية الرقمية:

- **الربط بين التقنية والإنسان:** تغييرات تقنية (نُظم/ منصات) تفشل غالبًا بسبب مقاومة البشـــر أو غياب تدريب مناســـب؛ إدارة التغيير تقلّل الفجوة بين التقنية والممارسات.
- **ترسيخ السياسات:** تحويل التشريعات والسياسات إلى ممارسات يومية يتطلب خطة تغيير محكمة (تواصل، تدريب، حوافز، متابعة).
- **المرونة والاســـتدامة:** من خلال قياس الأثر وتعزيز التعلم، تضـــمن الإدارة استدامة التغيير وليس مجرد تنفيذ عمليات مؤقتةDiscovered+1 .

استراتيجيات إدارة التغيير التربوي:

أشـــار "بربخ" إلى أبرز اســـتراتيجيات إدارة التغيير (فرحان بربخ، 2012، ص. 104)، فيما يلي:

أ- **اســـتراتيجية الإقناع والإغراء:** وتعني ضـــرورة إشـــراك كل العاملين في حقل التعليم أو الذين سـيمسـهم التغيير، وإلا سـتكون اسـتجابتهم للتغير مجرد موافقة وليس التزامات وبالتالي تكون نتائج التغيير سطحية بدلاً من كونها جوهرية.

ب- **اسـتراتيجية السـلطة:** تشـتمل هذه الاسـتراتيجية على التدرج الهرمي الإداري الواضـــح لاتخاذ القرار واســـتخدام الموجهات والقوانين والقواعد واللوائح التنفيذية والمشاركة والتوجيه في جانب القيادة السياسية العليا.

ج- **اسـتراتيجية المدخل المفتوح:** وتشـمل التحديد الواسـع للأهداف، وإعادة تحديد الأهداف والإجراءات، والاسـتخدام الكبير للموارد المحلية والإقليمية والفردية، والبحث عن أفكار جديدة من أكبر عدد ممكن من أفراد المجتمع والهيئات والمراكز البحثية.

د- **اســـتراتيجية التجديد التنظيمي:** وتقوم على إحداث تغيير في الحالة الراهنة أو الوضـع القائم الذي يؤثر في أهداف التغيير أو بيئته أو التكنولوجيا المسـتخدمة فيه أو الأفراد العاملين فيه، وهذه الاســـتراتيجية قد تســـببها قوى داخلية في النظام العلمي نفســـه وقوى خارجية، وقد نبدأ من قمة النظام أو من أســـفله (فرحان حسن بربخ، 2012، 104).

استراتيجيات ومنهجيات عملية لإدارة التغيير في حماية الطفل.

تشـــير الأدبيات إلى أن تطبيق إدارة التغيير في ســـياق حماية الطفل والأمن السـيبراني يتطلب مزيجاً من الاسـتراتيجيات المنهجية والأدوات العملية التي تعزز من فاعلية التغيير وتضـمن اسـتدامته (Kotter, 1996; Hiatt, 2006; ISACA, 2020) , .و يمكن تبسيط هذه الاستراتيجيات في الخطوات التالية:

1- تقييم الاستعداد للتغيير(Readiness Assessment):

- يتضمن استخدام أدوات مثل خرائط أصحاب المصلحة (Stakeholder Maps)لتحديد القوى الداعمة والمعارضة للتغيير.
- تحليل مقاومة التغيير (Resistance Analysis) وتحديد الحوافز التي تشجع على تبني السلوكيات الجديدة (Burnes, 2017).

2- اختيار نموذج مناسب للتغيير (Change Model Selection):

- نموذج Kotter's 8-Step Model (من جامعة هارفارد) مناسب للمبادرات الاستراتيجية واسعة النطاق.
- نموذج ADKAR (Awareness, Desire, Knowledge, Ability, Reinforcement)من تطوير Prosci، ملائم لإدارة التغيير على مستوى الأفراد والمهام (Hiatt, 2006).

3- خطة تواصل متدرجة (Communication Plan):

- تصميم رسائل توعوية واضحة تناسب مختلف الفئات (الأسر، الأطفال، العاملين).
- استخدام قنوات متعددة (اجتماعات، منصات رقمية، حملات توعية).
- توفير آليات تغذية راجعة مستمرة لضمان تحسين التواصل (Kotter, 1996).

4- بناء القدرات (Capacity Building):

- إعداد برامج تدريبية تفاعلية للعاملين في مؤسسات رعاية الطفل.
- إدماج عمليات محاكاة (Simulations) لاختبار سيناريوهات الاستجابة للأخطار الرقمية(PubMed Central, 2021) .

5- إدماج مؤشرات الأداء(KPIs) :

- KPIs = Key Performance Indicators (مؤشرات الأداء الرئيسة).
- تشمل: معدلات الامتثال، عدد الحوادث الناتجة عن السلوك البشري، معدل استخدام الأدوات الرقمية الآمنة.(ISACA, 2020)

ملاحظة عملية:

في سياق حماية الطفل والأمن الرقمي، لا يمكن أن تُسند إدارة التغيير إلى قسم واحد فقط. بل يجب أن تكون عملية تكاملية تضم فرقًا متعددة الاختصاصات (الأمن، الحماية، التقنية، التعليم، الشؤون القانونية) تعمل وفق خطة موحدة ومنسقة (ISACA, 2020).

الأمن السيبراني (Cybersecurity) مفهومه، أنواعه، أدواته، وآليات التطبيق:

[4] الأمن السيبراني: المفهوم والأدوات:

الأمن السيبراني هو مجموعة الممارسات والأدوات التي تهدف إلى حماية الأنظمة الرقمية والشبكات والبيانات من الهجمات أو الاستخدام غير المصرح به (NIST, 2018)تتضمن أدواته أنظمة الحماية من الفيروسات، جدران الحماية، تقنيات التشفير، حلول إدارة الهوية، ونظم كشف التسلل.

أما أنواعه فيمكن تصنيفها إلى:

- أمن الشبكات (Network Security).
- أمن التطبيقات (Application Security).
- أمن البيانات (Data Security).
- أمن الهوية والوصول (Identity & Access Management).
- الأمن السحابي (Sharma & Gupta, 2020) (Cloud Security).

ويُطبَّق الأمن السيبراني على مستوى المؤسسات من خلال تطوير سياسات واضحة، تدريب العاملين، وتبني حلول تقنية متقدمة، إلى جانب إشراك المستخدم النهائي (خصوصاً الأطفال والأسر) في تعزيز الوعي الرقمي.

مفهوم الأمن السيبراني:

الأمن السيبراني يعني مجموعة الضوابط الفنية والإدارية والتقنية لحماية الأنظمة والمعلومات والمستخدمين من التهديدات الإلكترونية. يغطي مجالات متعددة: أمن الشبكات، أمن التطبيقات، أمن نقاط النهاية، إدارة الهوية والتحكم في الوصول، حماية البيانات، المراقبة والاستجابة للحوادث، والتعافي من الكوارث. الإطار العملي الشائع هو إطار NIST CSF: Identify – Protect – Detect – Respond – Recover. NIST Publications.

أنواع الأدوات والسياسات التقنية لحماية الأطفال في البيئة الرقمية

تشير الأدبيات الحديثة والتقارير للدولية إلى أن حماية الطفل في البيئة الرقمية لا يمكن أن تتحقق عبر السياسات الاجتماعية أو التوعوية فقط، بل تتطلب منظومة أدوات تقنية متكاملة تولكب معايير الأمن السيبراني العالمية (ISO, 2022; OWASP Foundation, 2023; UNICEF, 2023).

وفيما يلي عرض مبسط لأهم هذه الأدوات:

1- أدوات الوقاية والتقليل(Prevention and Mitigation Tools)

- **(الجدران النارية) Firewalls**: أنظمة تمنع محاولات الدخول غير المصرح به إلى الشبكات.
- **(إدارة الهوية والوصول) IAM = Identity and Access Management**: سياسات للتحكم في من يمكنه الوصول إلى المعلومات والأنظمة.
- **(تشفير البيانات) Data Encryption**: ضمان أن البيانات لا يمكن قراءتها إلا من قبل الأشخاص المخوّلين.

- **(سياسات كلمات المرور) Password Policies**: إلزامية تعقيد كلمات المرور وتغييرها دورياً.
- **(المصادقة متعددة العوامل) MFA = Multi-Factor Authentication**: إضافة طبقات أمان إضافية عبر التحقق من الهوية باستخدام أكثر من وسيلة (مثل الهاتف والبريد الإلكتروني).
- توصي معايير ISO/IEC 27001 بهذه الإجراءات كأساس لحماية البيانات والمعلومات(ISO, 2022) .

2- حماية التطبيقات والويب (Application and Web Security):

- **(جدار حماية تطبيقات الويب) WAF = Web Application Firewall**: أداة تراقب حركة المرور على التطبيقات وتحجب الهجمات الشائعة.
- **(مراجعة الشيفرة) Code Review**: فحص الكود البرمجي لاكتشاف الثغرات الأمنية.
- **(إدارة الثغرات) Vulnerability Management**: تحديد ومعالجة نقاط الضعف في الأنظمة بشكل دوري.
- **OWASP Principles** مجموعة من أفضل الممارسات لحماية التطبيقات والويب صادرة عن OWASP Foundation (مثل معالجة هجمات SQL Injectionأو XSS).

3- حماية نقاط النهاية والمراقبة (Endpoint & Monitoring Security):

- **(الكشف والاستجابة لنقاط النهاية) EDR = Endpoint Detection and Response**: أنظمة لرصد الأنشطة المشبوهة على الأجهزة (حاسوب، هاتف، جهاز لوحي).
- **(مكافحة الفيروسات) AV = Antivirus**: أدوات أساسية لمنع البرمجيات الخبيثة.

- **(إدارة معلومات وأحداث الأمان)** SIEM= Security Information and Event Management: تجميع وتحليل السجلات والتنبيه بالحوادث الأمنية.
- **(أنظمة كشف التسلل) IDS = Intrusion Detection System** و**(أنظمة منع التسلل) IPS = Intrusion Prevention System**: لرصد ومنع محاولات الهجوم على الشبكات(OWASP Foundation, 2023).

4- حماية المحتوى وخصوصية الأطفال (Content & Privacy Protection):

- **(فلترة المحتوى) Content Filtering**: منع وصول الأطفال إلى المواقع أو التطبيقات غير المناسبة.
- **(أدوات الرقابة الأبوية) Parental Control Tools**: تمكّن الأهل من متابعة سلوك الأطفال الرقمي.
- **(إعدادات خصوصية افتراضية للأطفال) Default Privacy Settings for Children**: ضبط الحسابات لتكون آمنة بشكل تلقائي.
- **(سياسات مشاركة محدودة) Limited Sharing Policies**: الحد من مشاركة البيانات الشخصية للأطفال على المنصات الرقمية (UNICEF, 2023).

كيفية التطبيق داخل مؤسسات رعاية الطفل:

1- **تقييم المخاطر الرقميّة (Digital Risk Assessment)**: تحديد بيانات الطفل المخزنة، نقاط الوصول، الموردين الخارجيين، واحتمالات التعرض NIST . Publications

2- **تصميم ISMS**: نظام إدارة أمن المعلومات مطابق لمعايير ISO 27001 أو مبادئ NIST لضمان إدارة المخاطر واستمرارية الأعمالISO .

3- **تطبيق ضوابط تقنية وبشرية متكاملة**: من التقنيات (تشفير، مراقبة، تحديثات) إلى حوكمة الموظفين (تدريب، وصول مبني على الأدوار، سياسات استخدام الأجهزة)1+ISMS.online .

4- اســـتجابة للحوادث **(Incident Response)** وعمليات الإبلاغ: وجود خطة لستجابة لحوادث تعرض بيانات طفل أو إساءة عبر منصة، مع خطوط اتصال واضحة وإجراءات إشعار السلطات والأهلNIST Publications .

5- **مؤشـرات قياس الأداء:** نسـبة تحديث الأنظمة، زمن الاسـتجابة للحوادث، عدد حوادث التعرض، نســـبة الالتزام بتدريبات الأمن، وعدد محاولات الاختراق المحظورة. هذه المؤشـــرات تســـاعد على رصـــد أثر التدابير وتغذية حلقات التحسين NIST Publications.

كيفية الاستفادة من إدارة التغيير لتعزيز الأمن السيبراني لحماية الطفل:

سبل تعزيز إدارة التغيير للأمن السيبراني:

إدارة التغيير تعمل كجســـر تنظيمي بين الاســـتراتيجية (الســـياســـات الوطنية/المؤسسية لحماية الطفل) والتنفيذ التقني (ضوابط أمنية، إعدادات منصات).

عندما تُطبَّق مبادئ إدارة التغيير على برامج الأمن السـيبراني، فإنها تسـاعد على: إشـراك الأطراف المعنية (الموظفين، الأطفال، الأهالي، مقدمي التقنية)، وذلك يغرض تكييف الممارسات مع سياقات العمل، وضمان تبنّي الضوابط على مستوى السلوك اليومي، وليس فقط إدخال تقنيات جديدة جسديةISACA+1 .

[5] التكامل بين إدارة التغيير والأمن السيبراني لحماية الطفل:

يمثل الجمع بين المحاور الســـابقة مدخلاً متكاملاً لحملية الطفل في البيئة الرقمية. إذ يمكن لإدارة التغيير أن تهيئ مؤسسات رعاية الطفل لتبني استراتيجيات أمن سيبراني أكثر فاعلية واستدامة عبر:

- تغيير الثقافة التنظيمية نحو وعي رقمي استباقي.
- إدماج الأسر والمعلمين ضمن خطط التغيير المؤسسي.
- تخصيص الموارد لتبني حلول أمنية متقدمة.

- تطوير سياسات حماية الطفل بما ينسجم مع التحولات الرقمية.

وبذلك يصبح الأمن السيبراني ليس مجرد استجابة تقنية، بل جزءاً من تحول مؤسسي أشمل تقوده إدارة التغيير لتعزيز حماية الأطفال في العصر الرقمي (Snyder, 2019).

قائمة الاختصارات

الاختصار	الاسم الكامل بالإنجليزية	الترجمة العربية	كيفية الاستفادة في الدراسة
Kotter	**Kotter's 8-Step Model for Change**	نموذج كوتر ذو الخطوات الثمانية لإدارة التغيير	يساعد على قيادة التغيير الاستراتيجي على مستوى المؤسسات، عبر خطوات منظمة (من خلق الإحساس بالحاجة للتغيير حتى تثبيت التغيير في الثقافة المؤسسية).
ADKAR	**Awareness, Desire, Knowledge, Ability, Reinforcement**	نموذج "أدكار" (الوعي، الرغبة، المعرفة، القدرة، التعزيز)	يركز على التغيير على مستوى الأفراد، ما يدعم تبني الأطفال والمعلمين والموظفين لسياسات الأمن الرقمي خطوة بخطوة.
KPIs	**Key Performance Indicators**	مؤشرات الأداء الرئيسية	تستخدم لقياس مدى نجاح تنفيذ التغيير الرقمي، مثل: معدلات الامتثال للسياسات، أو معدل استخدام أدوات الأمان من قبل الأطفال والموظفين.
IAM	**Identity and Access Management**	إدارة الهوية والوصول	يضمن التحكم في من يستطيع الوصول إلى بيانات الأطفال أو أنظمة

الاختصار	الاسم الكامل بالإنجليزية	الترجمة العربية	كيفية الاستفادة في الدراسة
			المؤسسات، مما يقلل من مخاطر الاختراق أو التسريب.
MFA	**Multi-Factor Authentication**	المصادقة متعددة العوامل	توفر طبقة إضافية من الأمان عبر طلب أكثر من وسيلة تحقق (كلمة مرور + رمز عبر الهاتف) لحماية بيانات الأطفال.
WAF	**Web Application Firewall**	جدار حماية تطبيقات الويب	يحمي تطبيقات ومنصات التعليم والرعاية الرقمية من الهجمات الشائعة مثل الحقن البرمجي (**SQL Injection**).
OWASP	**Open Web Application Security Project**	مشروع أواسب للأمن المفتوح لتطبيقات الويب	يقدم أفضل الممارسات لتأمين تطبيقات ومواقع المؤسسات، بما يحمي الأطفال من ثغرات الويب.
EDR	**Endpoint Detection and Response**	الكشف والاستجابة لنقاط النهاية	يساعد في رصد الهجمات على أجهزة المستخدمين (مثل حواسيب الأطفال أو أجهزة الإدارة) والتعامل معها بسرعة.
AV	**Antivirus**	برامج مكافحة الفيروسات	خط دفاع أساسي ضد البرمجيات الخبيثة التي قد تهدد بيانات الأطفال.

الاختصار	الاسم الكامل بالإنجليزية	الترجمة العربية	كيفية الاستفادة في الدراسة
SIEM	**Security Information and Event Management**	إدارة معلومات وأحداث الأمان	يجمع السجلات الأمنية ويحللها للتنبيه عن حوادث محتملة تخص أنظمة حماية الطفل.
IDS	**Intrusion Detection System**	أنظمة كشف التسلل	ترصد محاولات الدخول غير المصرح به إلى الشبكات التي تستخدمها مؤسسات رعاية الطفل
IPS	**Intrusion Prevention System**	أنظمة منع التسلل	تمنع الهجمات المكتشفة فوراً، ما يعزز حماية الأنظمة الحساسة للأطفال.
ISO	**International Organization for Standardization**	المنظمة الدولية للمعايير	**ISO/IEC** تقدم معايير مثل التي توفر إطاراً **27001** عالمياً لإدارة أمن المعلومات في مؤسسات رعاية الطفل.

هذه الاختصارات تم الاستعانة بها في الدراسة ويجد الباحث ضرورة فهم هذه الاختصارات خاصا أنهاتساعدفي اليات التطبيق والتنفيذ: وهي في أدوات للتغيير للتنظيمي (Kotter, ADKAR, KPIs) وأدوات الأمن السيبرلني,IAM) (MFA,WAF,OWASP,EDR, AV, SIEM, IDS, IPS, ISO.

- الأولىمن خلال(نماذجالتغيير) تساعد في قيادة التغيير السلوكي والثقافي داخل مؤسسات رعاية الطفل.
- والثانية من خلال (الأدوات التقنية للامن السيبراني) التي تضمن تأمين البيئة الرقمية من الأخطار، وبالتالي حماية الأطفال أثناء استخدام التكنولوجيا.

الدراسات السابقة:

- دراســـة (العســـاف، 2022): "التربية الرقمية ودورها في الوقاية من مخاطر الإنترنت لدى الأطفال".

أظهرت الدراسة أن 65% من الأطفال السعوديين في العينة يقضون أكثر من 4 ســـاعات يومياً على الإنترنت، مع وجود علاقة طردية بين طول الاســـتخدام وزيادة احتمالية التعرض لمخاطر سيبرانية (تنمر، محتوى غير لائق).

وتؤكد هذه الدراسة أن المؤسسات التعليمية والرعوية بحاجة لتغيير استراتيجياتها نحو تعزيز التوعية الرقمية المبكرة (العساف، 2022).

- دراسة (اليونيسف، 2021): "محو الأمية الرقمية للأطفال: استكشاف التعريفات والأطر".

أوضـــحت الدراســـة أن واحد من كل ثلاثة مســـتخدمين للإنترنت هو طفل، وأن الأطفال في المنطقة العربية يواجهون تهديدات متزليدة مثل التنمر الإلكتروني والاســـتغلال، كما أظهرت أن 70% من أولياء الأمور لا يمتلكون الوعي الكافي بطرق حماية أبنائهم رقمياً.

كما تشير هذه الدراسة إلى الحاجة لبرامج تغيير داخل مؤسسات رعاية الطفل لتأهيل المربين على استراتيجيات الأمن السيبراني (UNICEF, 2021).

- دراسة (Council of Europe, 2021): "رسم خرائط الاستجابات للاستغلال والاعتداء الجنسي على الأطفال عبر الإنترنت: مجلس أوروبا".

أفادت الدراســـة أن 80% من الأطفال في 25 دولة يشـــعرون بأنهم معرضـــون للاســـتغلال عبر الإنترنت، فيما أكدت الدول الأعضـــاء أن الاســـتجابة ما زالت تفتقر للتكامل بين المؤسسات التعليمية والأمنية.

وتوضـــح هذه الدراســـة أهمية وجود إطار تكاملي قائم على التغيير المؤســـســـي لتعزيز الأمن السيبراني (Council of Europe, 2021).

- دراســـة (الشـــهري، 2021): "مخاطر الشـــبكات الاجتماعية على الأطفال والمراهقين في المملكة العربية السعودية".

توصـــلت الدراســـة إلى أن 57% من الأطفال في العينة (ن=500) تعرضـــوا لمضـــايقات أو محاولات اســـتغلال عبر الإنترنت، وأن 45%من أولياء الأمور غير مدركين لطبيعة هذه المخاطر.

تبرز هذه الدراسة الحاجة لتغيير استراتيجيات التوعية الرقمية داخل مؤسسات رعاية الطفل (الشهري، 2021).

- دراســـة (البدري، 2020): "فاعلية برامج التثقيف الرقمي في الحد من التنمر الإلكتروني لدى الأطفال".

بينت الدراســة أن المجموعة التجريبية (ن=60) التي خضـــعت لبرنامج توعية أظهرت انخفاضاً بمعدل 40% في حالات التنمر الإلكتروني مقارنة بالمجموعة الضابطة.

تؤكد هذه الدراسة أهمية التدخل المؤسسي وتغيير السياسات التعليمية لتشمل التدريب الوقائي (البدري، 2020).

- دراســـة (Anderson & Jiang, 2018): "المراهقون ووســـائل التواصـــل الاجتماعي والتكنولوجيا ٢٠١٨".

أشـــارت للدراســـة إلى أن 95% من المراهقين الأمريكيين لديهم إمكانية الوصـــول إلى الهواتف الذكية، و45% منهم متصـــلون بالإنترنت بشـــكل دائم تقريباً، تؤكد هذه الدراســة أهمية التغيير المؤســسي لمواكبة واقع الاســتخدام الكثيف للتكنولوجيا (Anderson & Jiang, 2018).

وقد استعان الباحث في الدراسة الحالية بمجموعة من التقارير على النحو التالي:

- **(Livingstone et al., 2020) (Ofcom, 2023): "الأطفال والآباء: تقرير استخدام وسائل الإعلام والمواقف لعام 2023".**

كشفت الدراسة أن 77% من الأطفال (5–15 سنة) يمتلكون جهازًا ذكيًا شخصيًا، وأن 62% من الآباء يشعرون بالقلق من تعرض أطفالهم لمحتوى ضار. كما توضح هذه الدراسة وجود فجوة بين وعي أولياء الأمور وتطور التقنيات، مما يستدعي تغييرًا في السياسات المؤسسية (Ofcom, 2023).

- **"نتائج المسح من 19 دولة":**

هدفت هذه الدراسة إلى حماية الأطفال من المحتوى الضار عبر الإنترنت، وأظهرت الدراسة أن حوالي 30% من الأطفال الأوروبيين (9–17 سنة) شاهدوا محتوى جنسي خلال العام السابق، وأن 20% تعرضوا للتنمر الإلكتروني كما تكشف هذه الدراسة أهمية بناء سياسات استباقية عبر تغيير مؤسسي لحماية الأطفال من المحتوى الضار (Livingstone, Ólafsson, & Staksrud, 2020).

- **(NCMEC, 2020) (Australian Safety Commissioner, 2022): "حالة السلامة على الإنترنت بين الأطفال والشباب".**

أظهرت الدراسة أن 67% من الأطفال (8–17 سنة) واجهوا شكلاً من أشكال الإساءة أو التنمر عبر الإنترنت، و30% شاهدوا محتوى غير لائق خلال العام الماضي. تدعم هذه الدراسة ضرورة دمج إدارة التغيير مع الأمن السيبراني لبناء خطط وقائية (Australian eSafety Commissioner, 2022).

- **"تقرير المركز الوطني للأطفال المفقودين والمستغلين لعام 2020":**

سجلت الدراسة أن 21.7 مليون بلاغ عن استغلال الأطفال عبر الإنترنت في عام واحد فقط، وهو رقم تضاعف تقريباً عن العام السابق يوضح الارتفاع الحاد خطورة الوضع، وأبرزت هذه الدراسة الحاجة إلى إدخال استراتيجيات إدارة

التغيير لتعزيز آليات المراقبة والتدريب داخل مؤسسات رعاية الطفل (NCMEC, 2020).

التصور المقترح:

تم الاستعانة في التصور المقترح لتوظيف إدارة التغيير والأمن السيبراني في تعزيز حماية الطفل داخل مؤسسات الرعاية بدراسة كلا من: (أحمد 2015)، (احمد 2020) ، (Hiatt 2006), (ISO, 2022) ، (Kotter 1996) ، (UNICEF 2021) ،(ISACA 2020) ،(بنت سعد ،بنت صالح 2024)، (الصانع 2024)، (المنتدى الدولي للأمن السيبراني 2025).

أولاً: الهدف من التصور المقترح:

يهدف هذا التصور إلى وضع إطار عملي واستراتيجي يساعد مؤسسات رعاية الطفل على الانتقال من وضعها الحالي (المعرّض لمخاطر رقمية متزايدة) إلى وضع مستقبلي أكثر أمانًا واستدامة، وذلك عبر دمج مبادئ إدارة التغيير (Change Management) مع الأمن السيبراني (Cybersecurity) بما يضمن:

- تعزيز ثقافة الحماية الرقمية داخل المؤسسة.
- تمكين العاملين والأهالي من تبني ممارسات آمنة في البيئة الرقمية.
- بناء أنظمة وإجراءات وقائية واستباقية لحماية الأطفال.

ثانيًا: الأساس النظري للتصور:

يرتكز التصور على ثلاثة أبعاد رئيسية:

1- إدارة التغيير Change Management:

تُعدّ إدارة التغيير مدخلًا استراتيجيًا لتقليل مقاومة الأفراد وضمان تبني الممارسات الجديدة(Kotter, 1996) ؛ (Hiatt, 2006).

ويُستخدم في هذا السياق كل من:

- نموذج كوتر Kotter's 8 Steps الذي يركز على التغيير المؤسسي عبر خطوات واضحة (إلحاح، قيادة، رؤية، ترسيخ).
- نموذج أتكار–ADKAR (Awareness–Desire–Knowledge–Ability Reinforcement)الذي يركز على الأفراد في رحلة التغيير.

2- الأمن السيبراني Cybersecurity:

يمثل البعد التقني لحماية البيانات والأنظمة، ويشمل:

- أدوات الحماية مثل (IAM, MFA, EDR, SIEM).
- سياسات مؤسسية للوقاية، مثل إدارة كلمات المرور والتشفير (ISO/IEC, 2022).

3- حماية الطفل في البيئة الرقمية Child Protection in Digital Contexts:

بحسب تقارير(UNICEF, 2021)، فإن الأطفال من الفئات الأكثر هشاشة أمام المخاطر الرقمية (التنمر الإلكتروني، الاستغلال، انتهاك الخصوصية)، وهو ما يستدعي دمج آليات وقائية داخل خطط التغيير المؤسسي.

خطوات التصور المقترح (الجدول التطبيقي)

المرحلة	الأهداف المرجوة	الاستراتيجية المقترحة	الأدوات والآليات التنفيذية	النتائج المرجوة	مؤشرات التحقق (KPIs)
مرحلة الإعداد (Preparation)	رفع جاهزية المؤسسة للتغيير من خلال تحديد الفجوات في البنية الرقمية	تحليل الفجوة Gap Analysis + إدارة أصحاب المصلحة Stakeholder Management	استبيان تشخيصي لقياس وعي العاملين - سجل أصحاب المصلحة (الإدارة، المربين، الأهالي،	صورة واضحة للوضع الراهن مع تحديد التحديات	نسبة مشاركة الموظفين بالاستبيانات ≥70% - اكتمال تقرير التحليل

المرحلة	الأهداف المرجوة	الاستراتيجية المقترحة	الأدوات والآليات التنفيذية	النتائج المرجوة	مؤشرات التحقق (KPIs)
	وثقافة العاملين		الأطفال) اجتماعات - تعريفية	والف رص	
مرحلة التهيئة (Readiness & Awareness)	بناء وعي عام وثقافة مؤسسية داعمة للتغيير والرقمنة	التغيير التدريجي Incremental Change + التثقيف السيبراني Cybersecurity Awareness	ورش - عمل مبسطة للعاملين حملات - توعية للأهالي ألعاب - تعليمية للأطفال حول الأمان الرقمي	تعزيز ثقافة الحماية الرقمية	نتائج - اختبار وعي العاملين ≥80% عدد - البرامج التدريبية (≥3 سنويًا)
مرحلة التنفيذ (Implementation)	إدخال الحلول الرقمية وتطبيق أنظمة آمنة لحماية البيانات	استراتيجية التحول الرقمي Digital Transformation	أنظمة - إدارة بيانات الأطفال تطبيقات - مراقبة مشفّرة برامج - كشف التهديدات السيبرانية	رفع كفاءة الإدارة وحماية البيانات	- انخفاض الأخطاء ≥30% التزام - المستخدمين بالسياسات ≥90%
مرحلة الدعم والمواكبة (Support & Reinforcement)	ترسيخ ثقافة التغيير وضمان استمراريته	التحسين المستمر Continuous Improvement	منصة - دعم فني داخلي تحديث - السياسات الأمنية مجموعات - نقاش داخلية	ضمان المرونة ومواجهة التهديدات الجديدة	تقارير - شهرية عن الحوادث رضا - الموظفين ≥85%

الإطار المنهجي (Methodological Framework):

[1] نوع الدراسة:

تنتمي هذه الدراسة إلى المراجعات الأدبية السردية (Narrative Literature Review)، حيث تستند إلى تجميع وتحليل الأدبيات المتوفرة في مجالات إدارة التغيير، الأمن السيبراني، وحماية الطفل في البيئة الرقمية. ويُعد هذا النوع من الدراسات مناسبًا للموضوع نظرًا لطبيعته التكاملية، التي تتطلب ربط مجالات متعددة في إطار واحد يوضح الأبعاد النظرية والتطبيقية.

[2] المنهج المستخدم:

تم اعتماد المنهج الوصفي التحليلي في صورته السردية، الذي يقوم على:

- **الوصف**: عرض المفاهيم الرئيسة للدراسة (إدارة التغيير، الأمن السيبراني، حماية الطفل).
- **التحليل**: توضيح العلاقات والارتباطات بين المحاور الثلاثة.
- **الدمج**: صياغة إطار استراتيجي يوضح كيف يمكن لإدارة التغيير أن تسهم في تعزيز الأمن السيبراني لحماية الطفل في البيئة الرقمية.

[3] مصادر البيانات:

اعتمدت الدراسة على:

- الأدبيات الأكاديمية (كتب، مقالات محكمة، رسائل علمية).
- التقارير الدولية اليونيسف UNICEF، الاتحاد الدولي للاتصالات ITU ، البنك الدوليWorld Bank.
- الإصدارات المتخصصة في الأمن السيبراني وإدارة التغيير مثلISACA ، Cybersecurity Ventures.

نتائج الدراسة:

في ضوء مراجعة الأدبيات وتحليلها، توصلت الدراسة إلى مجموعة من النتائج الرئيسة، يمكن تلخيصها فيما يلي:

1) **<u>على مستوى المفاهيم النظرية</u>:** يتضح أن إدارة التغيير ليست مجرد أداة إدارية، بل تمثل إطارًا استراتيجيًا يمكن من خلاله تعزيز التكيف المؤسسي مع التحديات الرقمية، كما أن الأمن السيبراني لم يعد مقتصرًا على الجوانب التقنية، بل بات يشمل أبعادًا اجتماعية وتربوية، خاصة فيما يتعلق بحماية الأطفال.

2) **على مستوى التحديات الرقمية للأطفال:** تشير الأدبيات إلى تزايد معدلات تعرض الأطفال لمخاطر الإنترنت (مثل التنمر الإلكتروني، الاستغلال، الإدمان الرقمي)، وهو ما يعكس قصور السياسات الحالية التي تتسم غالبًا بالطابع التفاعلي (Reactive) أكثر من الوقائي (Proactive).

3) **على مستوى دور إدارة التغيير:** أظهرت النتائج أن دمج إدارة التغيير في استراتيجيات الأمن السيبراني يسهم في:
- بناء ثقافة مؤسسية داعمة للأمن الرقمي.
- إشراك الأطراف المعنية (الأسر، المدارس، المؤسسات) في عمليات الحماية.
- تعزيز مرونة المؤسسات في مواجهة المخاطر الرقمية المستجدة.

4) **على مستوى التصور التكاملي:** تكشف المراجعة أن تبني نموذج تكاملي يدمج بين (إدارة التغيير، الأمن السيبراني، حماية الطفل) من شأنه أن يوفر أساسًا عمليًا لتطوير سياسات وقائية أكثر استدامة وفاعلية داخل مؤسسات رعاية الطفل.

الخلاصة (Conclusion):

تؤكد هذه الدراسة، من خلال مراجعة سردية موسعة للأدبيات، أن حماية الأطفال في العصر الرقمي لم تعد مسؤولية اجتماعية فحسب، بل أصبحت ضرورة استراتيجية تتطلب دمج مفاهيم الأمن السيبراني ضمن خطط إدارة التغيير داخل مؤسسات رعاية الطفولة.

وقد أظهرت النتائج أن تعزيز الأمن السيبراني يتطلب مزيجًا من:

- سياسات تنظيمية واضحة.
- تدريب للعاملين.
- رفع الوعي لدى الأطفال وأسرهم.
- تبني ثقافة مؤسسية مرنة تستجيب للتغيرات الرقمية.

كما أبرزت الدراسة أن اعتماد إدارة التغيير كمدخل أساسي يمكن أن يوفر للمؤسسات القدرة على التكيف مع المخاطر المتجددة، وضمان استدامة بيئة رقمية آمنة للأطفال.

التوصيات:

استنادًا إلى ما سبق من نتائج، تقدم الدراسة التوصيات التالية:

1) لصناع القرار:

- تضمين إدارة التغيير كجزء من السياسات الوطنية الخاصة بالأمن السيبراني وحماية الطفل.

- وضع تشريعات واضحة تُلزم المؤسسات التعليمية والرعائية بتبني إجراءات وقائية رقمية.

2) لمؤسسات رعاية الطفل:

- تطوير خطط تغيير مؤسسية شاملة، تتضمن التدريب المستمر للعاملين على أدوات الأمن السيبراني.
- إنشاء وحدات أو لجان داخل المؤسسات مختصة بمتابعة التهديدات الرقمية وتحديث السياسات باستمرار.

3) للمجتمع والأسرة:

- تعزيز الوعي الرقمي لدى الأسر، وتزويدها بأدوات إرشادية لمتابعة أنشطة الأطفال على الإنترنت.
- تشجيع الشراكات المجتمعية بين المؤسسات التعليمية والمنظمات غير الحكومية لتعزيز الأمن الرقمي للأطفال.

4) للبحث العلمي:

- الدعوة إلى مزيد من الدراسات التطبيقية الميدانية التي تختبر النماذج النظرية في بيئات رعاية الطفولة.
- الحاجة إلى تطوير أدوات قياس لفاعلية استراتيجيات إدارة التغيير في تعزيز الأمن السيبراني للأطفال.

وفي ضوء ذلك، توصي الدراسة بضرورة:

- صياغة سياسات مؤسسية واضحة لحماية الطفل سيبرانيًا.
- الاستثمار في بناء قدرات العاملين داخل المؤسسات.
- التعاون مع الجهات الحكومية والتقنية لتطوير أنظمة حماية فعالة.

وبهذا، قد أجابت الدراسة عن تساؤلاتها الرئيسة وتفتح المجال أمام بحوث مستقبلية لتجريب وتطوير النماذج المقترحة على أرض الواقع، بما يعزز من تكامل الجهود الأكاديمية والمجتمعية في حماية الطفولة.

البحوث والدراسات المقترحة:

- العلاقة بين التحول الرقمي ومخاطر الأمن السيبراني على الطفولة المبكرة.
- التحول من السياسات التفاعلية إلى السياسات الاستباقية في حماية الطفل.
- دور الأسرة والمعلمين في إنجاح استراتيجيات الأمن السيبراني للأطفال.
- تقييم السياسات الدولية لحماية الطفل على الإنترنت.

المراجع

أولاً المراجع باللغة العربية:

أحمد، علي محمد على محمد (2015). **تصور مقترح لمواجهة مشكلات الحضانات المتعثرة التابعة للتضامن الاجتماعي بالإسكندرية في ضوء إدارة التغيير "دراسة مسحية مطبقة على حضانات التضامن الاجتماعي بالإسكندرية"**، رسالة ماجستير، كلية التربية للطفولة المبكرة، جامعة الإسكندرية.

أحمد، علي محمد على محمد (2020). **واقع بيئة العمل داخل مؤسسات رعاية الطفل وعلاقتها بتحسين فرص التغيير التنظيمي "دراسة وصفية مطبقة على مؤسسات رعاية الطفل"**، رسالة دكتوراه، كلية التربية للطفولة المبكرة، جامعة الإسكندرية.

البدري، م. (2020). فاعلية برامج التثقيف الرقمي في الحد من التنمر الإلكتروني لدى الأطفال. **مجلة التربية الرقمية**. 12(1)، 88-109.

بربخ, فرحان حسن (2012). **إدارة التغيير وتطبيقاتها في الإدارة المدرسية**. ط1. عمان- الأردن: دار أسامة للنشر والتوزيع.

بنت سعد المطيري, م & بنت صالح السدراني, غ. (2024). دور الوالدين في تعزيز الوعي بالأمن السيبراني للطفل. **مجلة الدراسات التربوية والإنسانية**. 16(2)، 463-502.

الشهري، م. (2021). مخاطر الشبكات الاجتماعية على الأطفال والمراهقين في المملكة العربية السعودية. **مجلة البحوث التربوية**. 15(3)، 211-236.

الصانع, ح. خ. (2024). تصوّر مقترح لتعزيز الوعي بالأمن السيبراني لدى مدارس التعليم المتوسط بدولة الكويت. **مجلة بحثية تعليمية** (Pdf) متاحEKB Journals.

العساف، أ. (2022). التربية الرقمية ودورها في الوقاية من مخاطر الإنترنت لدى الأطفال. **مجلة دراسات تربوية**. 18(2)، 45-67.

اللامي, غسان (2007). **إدارة التكنولوجيا مفاهيم ومداخل تقنيات تطبيقات عملية**. الأردن- عمان: دار المناهج للنشر والتوزيع.

المنتدى الدولي للأمن السيبراني .(2025) .مبادرة حماية الطفل في الفضاء السيبراني .استُعرض في موقع المنتدى

.https://gcforum.org/ar/initiatives/child-protection-الدولي
.in-cyberspace/ gcforum.org

ثانياً: المراجع باللغة الأجنبية:

Anderson, M., & Jiang, J. (2018). **Teens, social media & technology 2018**. Pew Research Center.

Australian eSafety Commissioner. (2022). **State of online safety among children and young people**. Australian Government.

Burnes, B. (2017). **Managing change**, (7th ed.). Pearson Education.

Cameron, E., & Green, M. (2020). **Making sense of change management: A complete guide to the models**, tools and techniques of organizational change. Kogan Page.

Council of Europe. (2020). **Protecting children in the digital environment**. Council of Europe Publishing.

Council of Europe. (2021). **Mapping responses to online child sexual exploitation and abuse**. Strasbourg: Council of Europe.

Cybersecurity Ventures (2022). **Cybercrime report**. Cybersecurity Ventures.

Cybersecurity Ventures. (2022). **2022 Official cybercrime report**. Retrieved from https://cybersecurityventures.com

Cybersecurity. **ISACA** Now. https://www.isaca.org. ISACA

Da Veiga, A. (2018). **Combining ADKAR and ISCA to support information security culture change**. Information & Computer Security. (example of combining change models and security-culture instruments).

Hiatt, J. (2006). **ADKAR: A model for change in business**, government and our community. Prosci Learning Center Publications.

https://jehs.journals.ekb.eg/article_350694.html
jehs.journals.ekb.eg

International Organization for Standardization (ISO). (2022). **ISO/IEC 27001: Information security management systems – Requirements**. ISO.

International Organization for Standardization (ISO). (2022). **ISO/IEC 27001:2022 Information security**, cybersecurity and privacy protection. ISO Standards.

International Telecommunication Union (ITU). (2020). **Child Online Protection (COP) Guidelines + implementation pages**. https://www.itu.int. ITU+1

International Telecommunication Union (ITU).(2023). **Child online protection guidelines**. Geneva: ITU.

International Telecommunication Union. (2023). **Child Online Protection guidelines**. ITU. https://www.itu.int/cop

ISACA. (2020). **State of cybersecurity 2020**. ISACA.

ISACA. (2020). **State of cybersecurity 2020: Current trends in workforce development**. ISACA.

ISACA. (2024). **The intersection of change management and**.

ISO. (2022). ISO/IEC 27001: **Information security management systems**. ISO. https://www.iso.org/standard/27001. ISO

ITU. (2023). **Child online protection guidelines**. International Telecommunication Union.

Kotter, J. P. (1996). **Leading change**. Harvard Business Review Press.

Kotter, J. P. (2012). **Leading change**. Harvard Business Review Press.

Livingstone, S., & Stoilova, M. (2021). **The 4Cs: Classifying online risk to children**. Communications, 46(3), 345–358.

Livingstone, S., Carr, J., & Byrne, J. (2017). **One in three: Internet governance and children's rights**. UNICEF Office of Research.

Livingstone, S., Ólafsson, K., & Staksrud, E. (2020). **EU Kids Online 2020: Survey results from 19 countries**. London School of Economics and Political Science.

National Center for Missing and Exploited Children. (2020). **CyberTipline 2020 report**. NCMEC.

National Institute of Standards and Technology (NIST). (2018). **Framework for improving critical infrastructure cybersecurity**. NIST.

NIST. (2018). **Cybersecurity Framework** (V1.1). NIST. NIST Publications

Ofcom. (2023). **Children and parents: Media use and attitudes report 2023**. UK Communications Regulator.

OWASP Foundation. (2023). **OWASP top 10 web application security risks**. OWASP.

OWASP. (2021). **OWASP Top 10 – Web application security risks**. OWASP. https://owasp.org/Top10/. OWASP Foundation

PubMed Central. (2021). **Training interventions for digital safety and child protection: A systematic review**. National Institutes of Health.