استراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي بمدارس التعليم الثانوي الصناعي بـ ج.م.ع.

إعداد: د. ولاء السيد عبد الله السيد صقر

"ملخص البحث"

يساعد التخزين الآمن للمعلومات والبيانات المدارس على استعادة قدراتها بسهولة ويسر، وخاصةً بعد الازمات التي قد تمر بها المؤسسات التعليمية، إذ أن التخزين الآمن للبيانات والمعلومات يتيح لمتخذي القرار استرجاع البيانات والمعلومات اللازمة لاستعادة النظام حيث تظل بيانات أعضاء هيئة التدريس، والطلاب، والنتائج النهائية للطلاب، وسجلات ميزانية المدرسة، وامكاناتها من معامل وأجهزة، وتقارير أداء الإداريين والمعلمين، وعقود الشراكة بين المدارس وغيرها من الهيئات، وبروتوكلات التعاون، وغيرها من السجلات محفوظة بمأمن بعيداً عن أي ضرر قد تكون الأزمة قد تسببت فيه.

وتعتبر المدارس الثانوية الصناعية من أكثر المؤسسات التعليمية تعرضاً للأزمات، وذلك نظراً لأنشطتها وطبيعتها التي تنبع من تعاملها مع أدوات، وأجهزة ومعدات ثقيلة، وماكينات ومعامل، قد يتسبب سوء التعامل معها للعديد من الأزمات، والتي إن لم يتم التنبه لها تتحول إلى كوارث قد تهدد قدرة المدرسة على استمرارية نشاطها، ومن ثم كان هناك بد من الاهتمام بالحفاظ على قواعد بيانات هذا النوع من المؤسسات التعليمية، ومن ثم إدارة عمليات الأمن المعلوماتي بها لسهولة تحقيق نظام معلومات متكامل تستطيع المدرسة الثانوية الصناعية الاعتماد عليه وقت الحاجة.

ويشير مصطلح إدارة الأمن المعلوماتي إلى ذلك الإطار من العمل الذي يتضمن عدد من العمليات الإدارية التي من شأنها الحفاظ على أمن المعلومات بالمؤسسة، ومن تلك العمليات تعزيز أمن المعلومات، والحفاظ عليها، وإدارتها، وتنفيذها، الأمر الذي يتطلب بناء السياسات، وصياغة المعايير، والخطط، والإجراءات اللازمة للحفاظ على المعلومات لحين الحاجة إليها.

وتتمثل حدود إدارة عمليات الأمن المعلوماتي التي قام البحث بالتعامل معها في عدة عمليات إدارية هي التخطيط، والإتصال، وتدريب العاملين، والتقويم.

وهدف البحث إلى التوصل إلى استراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي بالمدارس الثانوية الصناعية بجمهورية مصر العربية، واستخدم البحث أسلوب التحليل الرباعي SWOT Analysis، وفي سبيل تحقيق ذلك تم تطبيق استمارة التحليل الرباعي على عدد من الخبراء التربويين للمساهمة في بناء الاستراتيجية المنشودة.

إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي في مدارس التعليم الثانوي الصناعي في جمهورية مصر العربية

د. ولاء السيد عبد الله السيد صقر [1]

القسم الأول ـ الإطار العام للبحث:

مقدمة:

يشهد العالم اليوم ثورة تكنولوجية هائلة، انعكست آثارها على مناحي الحياة كافة، ومنها التعليم، الذي يعتبر مرآة المجتمع، وقد سببت تلك الثورة العديد من التغيرات بالمؤسسات التعليمية، ومنها المدارس؛ إذ اتجهت الإدارات المدرسية إلى بناء قواعد بيانات وبنوك معلومات ومواقع إلكترونية لها للإعلان عن خدماتها، وتخزين سجلاتها بطريقة آمنة، يسهل استرجاعها عند الحاجة؛ الأمر الذي يساعدها على سرعة اتخاذ القرارات المرتبطة بتطويرها وتحسين خدماتها.

كما يساعد التخزين الآمن للمعلومات والبيانات المدارس على استعادة قدراتها بسهولة ويسر، خاصةً بعد الأزمات والكوارث التي قد تمر بها المؤسسات التعليمية، إذ أن التخزين الآمن للبيانات والمعلومات يتيح لمتخذي القرار استرجاع البيانات والمعلومات اللازمة لاستعادة النظام داخل المدارس التي تعرضت لأزمات أو كوارث؛ حيث تظل بيانات أعضاء هيئة التدريس، والطلاب، ونتائج الطلاب، وسجلات ميزانية المدرسة، وإمكاناتها؛ من معامل، وأجهزة، وتقارير أداء الإداريين والمعلمين، وغيرها من السجلات، محفوظة بمأمن، بعيدًا عن أي ضرر قد تكون الأزمة أو الكارثة سببًا فيه، الأمر الذي يسهم في التعافي منها سريعًا. [1]

وتعد الفترة التالية لحدوث الأزمة من أكثر الفترات التي تساعد المدرسة على التغلب على السلبيات التي تسببت فيها الأزمة أو الكارثة، وهي بمثابة فترة النقاهة التي يقضيها المريض بعد تعرضه لمرض ما، وتتطلب العديد من الإجراءات والخطوات والممارسات الإدارية التي تساعد المدرسة على استرجاع نشاطها، واستعادة قدرتها على القيام بالعمل، كما كانت قبل حدوث الأزمة، ويطلق على تلك الإجراءات والخطوات والممارسات الإدارية، إدارة التعافي Recovery Management، والتي تشير إلى تعافي المنظمة من الآثار السلبية للأزمة التي تعرضت لها. [2]

---

(1) مدرس التربية المقارنة والإدارة التعليمية، كلية التربية ـ جامعة عين شمس.

وتعتبر المدارس الثانوية الصناعية من أكثر المؤسسات التعليمية تعرضًا للأزمات، وذلك نظرًا لأنشطتها وطبيعتها التي تنبع من تعاملها مع أدوات وأجهزة ومعدات ثقيلة، وماكينات ومعامل، قد يتسبب سوء التعامل في نشوب العديد من الأزمات، والتي إن لم يتم إدارتها على نحو فعّال، تتحول إلى كوارث، قد لا تهدد قدرة المدرسة على استمرارية نشاطها فحسب، بل من الممكن أن تهدد البيئة المحيطة بها أيضًا، ومن ثم كان هناك ضرورة لتصميم وبناء قواعد بيانات بهذه المدرسة تتيح للفئات المختلفة من الإداريين والمعلمين، استرجاع البيانات والمعلومات أثناء فترة تعافي المؤسسة التعليمية من الأزمة أو الكارثة التي مرت بها.

وقد قامت وزارة التربية والتعليم، والتعليم الفني، باستكمال التجهيزات وصيانة البنية التحتية لمدارس التعليم الفني، وتوفير الإمكانات المادية والبشرية والمعدات، والآلات والخامات اللازمة لدعم العملية التعليمية بها [3]، كما قامت الوزارة بإمداد المدارس الثانوية الصناعية بالعديد من أجهزة الكمبيوتر، والبرامج الأصلية التي تساعدها على إنشاء قواعد البيانات اللازمة للحفاظ على بيانات أعضاء هيئة التدريس، والإداريين، والطلاب، والإمكانات المادية للمدرسة من أجهزة وميزانية؛ فقد وفرت الوزارة للمدارس الثانوية الصناعية أجهزة كمبيوتر بمكاتب الإداريين، وشئون الطلاب، وشئون العاملين، ومدير المدرسة، وبكل قسم من الأقسام المدرسية، بالإضافة إلى إتاحة خدمة الإنترنت في المدرسة، وعمل شبكة داخلية بين أقسام المدرسة، وكذا شبكة تربط المدارس بعضها البعض لتسهيل التواصل وتبادل الخبرة [4]، الأمر الذي يتيح لها التجهيزات التي تمكنها من الحفاظ على معلوماتها واسترجاعها في الوقت الملائم، ومن ثم استعادة نشاطها بسرعة في حالة حدوث الأزمات.

وفي إطار مبادرة تطوير التعليم المصرية الشاملة، قامت الوزارة بالتعاون مع وزارة الاتصالات بتطبيق مشروع "تطوير التعليم الفني باستخدام تكنولوجيا المعلومات والاتصالات"، ويتمثل الغرض من هذا المشروع في الارتقاء بالتعليم الفني والتدريب المهني وتعزيزه، من خلال استخدام أنظمة تكنولوجيا المعلومات والاتصالات، علمًا بأن فئات المستفيدين المستهدفة تتمثل في المعلمين والطلاب في المدارس الصناعية، فضلًا عن المجتمع الأكبر المحيط بهذه المدارس. وخلال المشروع، تم تحديث 10

مدارس مهنية متقدمة في نواحي البنية التحتية لتكنولوجيا المعلومات والاتصالات والمناهج التعليمية وبناء قدرات التنمية البشرية بها. (5)

كما أُنشئت بكل مدرسة من مدارس التعليم الثانوي الصناعي ـ كمثيلاتها من المدارس الأخرى بمختلف المراحل ـ وحدة لإدارة الأزمات تحسبًا لأي ظروف مفاجئة أو أزمات قد تحدث، أو حدثت بالفعل للمدرسة، الأمر الذي يساعدها على التكيف مع الظروف غير المتوقعة، بل وتخطيها، والتخلص من آثارها السلبية. (6)

مشكلة البحث:

على الرغم من الجهود التي قامت بها الهيئات المسئولة في مجال التعليم الثانوي الصناعي للتغلب على الأزمات والتعافي منها، والحفاظ على البيانات والمعلومات الخاصة في المدرسة، إلا أن هناك العديد من أوجه القصور التي تنتاب أعمال وحدات إدارة الأزمات، ووحدة المعلومات والإحصاء، وكذلك سبل الاستغلال الأمثل للتكنولوجيا الحديثة، التي تستخدم لإنشاء قواعد البيانات اللازمة لتخزين المعلومات والحفاظ عليها، واسترجاعها عند الحاجة إليها، وفيما يلي إيجاز لها:

1- ضعف قدرة التعليم في مصر على مسايرة ما يحدث في نظم كثير من دول العالم ـ المتقدم تعليميًّا ـ من تطوير وتحديث واستخدام للتكنولوجيا المتطورة (7)، ومن ثم ضعف قدرة المدارس الثانوية الصناعية على استخدام تلك التكنولوجيا بشكل عام، واستخدامها في الحفاظ على أمنها المعلوماتي بشكل خاص.

2- ضعف القدرة على توفير البنية التحتية التكنولوجية الحديثة في مصر (8)، الأمر الذي يسري على المدارس كافة، والمدارس الثانوية الصناعية على وجه الخصوص، الأمر الذي أدى إلى افتقار المدارس الثانوية الصناعية للبنية التحتية الملائمة التي تسهم في الحفاظ على الأمن المعلوماتي للمدرسة، واسترجاع تلك المعلومات وقت الحاجة إليها.

3- محدودية استغلال الإمكانات التي تتيحها تكنولوجيا المعلومات؛ فاستخدامات الحاسب الآلي تنحصر في تطبيقات بسيطة، ولم يتحقق الاستخدام الأمثل لها في معظم القطاعات. (9)

4- نقص عدد المتخصصين في مجالات المعلوماتية وعشوائية خبراتهم، وخلفياتهم العلمية. (10)

5- ضعف المعلومات اللازمة للتعامل مع الأزمة قبل وبعد حدوثها لدى مديري المدارس الثانوية الصناعية، بالإضافة إلى ضعف اهتمامهم بتحديث قاعدة البيانات والمعلومات لاستخدامها وقت حدوث الأزمة أو بعدها. (11)

6- لا تسمح إدارة المدرسة الثانوية الفنية للعاملين بالمشاركة في التخطيط المدرسي، إذ إنها لا تطرح المشكلات المدرسية على الشبكة الداخلية للحاسبات الآلية (12)، مما يوضح غياب دور العاملين في التخطيط للحفاظ على الأمن المعلوماتي في المدارس الثانوية الصناعية، على الرغم من إنها الفئة الأقرب قربًا من الواقع وإدراكًا لمشكلاته.

ويمكن تحديد مشكلة البحث في السؤال الرئيس التالي:

كيف يمكن التوصل إلى إستراتيجية مقترحة لإدارة عمليات أمن المعلومات في المدارس الثانوية الصناعية في جمهورية مصر العربية؟

ويتفرع من السؤال الرئيس السابق، الأسئلة الفرعية التالية:

1- ما الأسس النظرية لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية من منظور الأدبيات الإدارية المعاصرة؟

2- ما جوانب القوة والضعف المرتبطة بإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية؟

3- ما الفرص والتهديدات المرتبطة بإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية؟

4- ما الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية؟

أهداف البحث:

تتمثل أهداف البحث فيما يلي:

1- الوقوف على الأسس النظرية لإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في الأدبيات الإدارية المعاصرة.

2- التعرف على جوانب القوة والضعف المرتبطة في إدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية.

3- التعرف على الفرص والتهديدات المرتبطة في إدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية.

4- التوصل إلى إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في جمهورية مصر العربية.

أهمية البحث:

تنبع أهمية البحث من كونها ترتبط في المدرسة الثانوية الصناعية التي تقع في بؤرة تركيز المسئولين عن التعليم بصفة عامة، لما لها من دور هام في النهوض بالاقتصاد المصري. كما أن هذا البحث يركز على قضية هامة وهي قضية الأمن المعلوماتي، تلك القضية التي تتواكب مع اهتمام الدولة بالتكنولوجيا، واستثمارها وتوظيفها في كافة قطاعات الدولة، ومن بينها قطاع التعليم.

مصطلحات البحث:

تتحدد المصطلحات الأساسية للبحث فيما يلي:

1. **التعليم الثانوي الصناعي Industrial Secondary Education:**

هو جميع أنواع التعليم المتعلق بالصناعة، بما في ذلك الفنون الصناعية وتعليم المهن الصناعية على كل المستويات. [13]

2. **الأمن المعلوماتي Information Security:**

هو حماية المعلومات وأنظمة المعلومات من الدخول العشوائي (غير المراقب)، أو الاستخدام غير المرشد، أو الكشف عن تلك المعلومات لغير المعنيين، أو إفساد تلك المعلومات والتغيير والتعديل فيها وتشويهها وتدميرها، وذلك بغرض الحفاظ على ثقة المستخدمين في المنظمة، وسلامة المنظمة، وقدرتها على إفادة الآخرين. [14]

كما أنه يستخدم للتعبير عن العملية التي تضمن الحفاظ على المعلومات الخاصة بأي منظمة أو مشروع، وحمايتها من السطو أو التعديل أو التغيير بدون إذن، أو الاستخدام غير المصرح به، الأمر الذي يسهم في استمرارية ثقة المستفيدين في المنظمة، وسلامتها، والقدرة على استرجاع تلك المعلومات عند حاجة المنظمة إليها. [15]

3. إدارة الأمن المعلوماتي Information Security Management:

هي إطار من العمل يتضمن عددًا من العمليات الإدارية التي من شأنها الحفاظ على أمن المعلومات بالمؤسسة، ومن تلك العمليات تعزيز أمن المعلومات، والحفاظ عليها، وإدارتها، وتنفيذها. الأمر الذي يتطلب بناء السياسات، وصياغة المعايير والخطط، والإجراءات اللازمة للحفاظ على المعلومات لحين الحاجة إليها. (16)

كما عرفت بأنها "ذلك المدخل الفعّال لإدارة أمن المعلومات باستمرار وبفاعلية، ويتضمن ذلك الأفراد، والأعمال، والبنى التحتية؛ بهدف تقليل المخاطر، مع الوضع في الاعتبار ضرورة تحقيق توقعات العملاء، وأهداف العمل الخاص بالمنظمة، وذلك من خلال الاستثمار الأمثل للموارد المادية والبشرية المتاحة للحفاظ على المعلومات واسترجاعها وقت الحاجة، ومن ثم حماية المنظمة من المخاطر والأزمات التي قد تتعرض لها". (17)

وهي كذلك "التخطيط والتطبيق للبنى والعمليات التي تساعد على الترابط والتوازن بين إستراتيجية الأمن المعلوماتي وبين أهداف العمل، والقوانين المطبقة، والمعايير التي تحكم المنظمة". (18)

وبناءً على ما سبق، يتضح أن إدارة الأمن المعلوماتي تتلخص فيما يلي:

- أنها تتضمن عددًا من العمليات الإدارية تهدف إلى الحفاظ على المعلومات الموجودة في المدرسة.
- أنها لكي تقوم بدورها وتحقق أهدافها يلزمها عدد من المتطلبات؛ كبناء السياسات، وصياغة المعايير والخطط، والإجراءات؛ لحماية المعلومات واسترجاعها وقت الحاجة.
- أنها مدخل يقوم على الاستمرارية وتحقيق الفاعلية، من خلال الاستخدام الأمثل للموارد المادية والبشرية المتاحة.
- أنها مدخل شامل يتضمن الأفراد، والأعمال، والبنى التحتية.
- أنها تهدف إلى حماية المنظمة من الأزمات والكوارث، لأنها تستخدم المعلومات المتاحة لديها في الحفاظ على نشاط المؤسسة قبل وقوع الأزمة، وأثنائها، وبعد انتهائها.

ومما سبق يمكن استخلاص التعريف الإجرائي التالي لإدارة الأمن المعلوماتي، وهي: "ذلك المدخل الشامل والفعال الذي يهدف إلى الاستغلال الأمثل للموارد المادية والبشرية المتاحة؛ من أجل الحفاظ على البيانات والمعلومات التي تمتلكها المنظمة؛ لاسترجاعها وقت الحاجة إليها. خاصة في وقت الأزمات والكوارث، مما يسهم في استعادة المنظمة لنشاطها بسرعة بعد انقضاء الأزمة. ولكي تحقق هذا الهدف؛ فيجب أن يتوفر لها عدد من المتطلبات، كبناء السياسات، وصياغة المعايير، والخطط، والإجراءات؛ لحماية المعلومات واسترجاعها وقت الحاجة إليها".

حدود البحث:

يقتصر البحث على ما يلي:

أولًا ـ بالنسبة للمرحلة الدراسية، ونمط المدرسة:

يتناول البحث المدرسة الثانوية الصناعية ذات الثلاث سنوات، والتي تعرضها طبيعة العمل فيها للعديد من الأزمات، نظرًا لما تقوم به من تصميم وتخطيط للمشروعات وتنفيذها، والتي يشارك فيها الطلاب، والمعلمون، والإداريون. وتتطلب ورش وآلات ومعدات، والتي تعتمد على كم هائل من المعلومات والبيانات التي يجب أن تخزن ويتم الحفاظ عليها، لحين استرجاعها وقت الحاجة إليها، كما أنها تتعامل مع طلاب في سن الطفولة، إذ إنهم متخرجون حديثًا من الحلقة الثانية من التعليم الأساسي، كما أنهم يمثلون القاعدة العريضة من صناع مصر.

ثانيًا ـ بالنسبة لإدارة عمليات الأمن المعلوماتي:

يقتصر البحث الحالي على دراسة العمليات التالية: **التخطيط** لإدارة الأمن المعلوماتي في المدرسة الثانوية الصناعية، **والاتصال، وتدريب العاملين** على الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، **وتقويم** قدرة المدرسة على الحفاظ على الأمن المعلوماتي لها، وذلك لقرب تلك العمليات من الأمن المعلوماتي؛ فيبدأ نشاط المنظمة للحفاظ على أمنها المعلوماتي بالتخطيط، ثم الاتصال بغيرها من موارد بشرية، ومؤسسات أخرى للاستفادة منها، وتبادل الخبرات معها، الأمر الذي يتطلب منها ضرورة الحفاظ على أمنها المعلوماتي، ثم تدريب العاملين على الحفاظ على الأمن المعلوماتي، ثم أخيرًا الوقوف على نقاط القوة والضعف في أداء المدرسة وقدرتها على الحفاظ على أمنها المعلوماتي، الأمر الذي يساعدها باستمرار على

الحفاظ على قدرتها على التعافي من الأزمات التي قد تصيبها، بوصفها من أكثر البيئات التعليمية تعرضًا للأزمات.

منهج البحث:

يسير البحث في خطواته وفقًا لخطوات أسلوب SWOT Analysis، الذي يهتم بالاحتمالات المستقبلية لكل من الجوانب الإيجابية والسلبية داخل المنظمة وخارجها، ويعتمد هذا الأسلوب على المعرفة التامة بالوضع الحالي والاتجاهات الحالية، ويساعد في إعداد الخطط والقرارات الإستراتيجية للمنظمة، وتتمثل العناصر الأساسية للتحليل البيئي فيما يلي: [19]

- **مؤشرات عن البيئة الداخلية للمنظمة:** وتشمل تحديد جوانب القوة (S) Strengths، وجوانب الضعف (W) Weaknesses، القائمة بالمنظمة.
- **مؤشرات عن البيئة الخارجية للمنظمة:** ويقصد بها القوى والعوامل الخارجية التي لا يمكن للمنظمة التحكم فيها أو السيطرة عليها، وتشمل الفرص (O) Opportunities، غير المستثمرة، والتهديدات (T) Threats الحالية، ومن هذه المؤشرات الاتجاهات المستقبلية في مجال عمل المنظمة، والعوامل الاقتصادية، ومصادر التمويل، والخصائص الديمغرافية للمنظمة، والتشريعات، والأحداث المحلية والقومية، والدولية.

وينتج عن تحليل جوانب القوة والضعف الداخلية، والفرص والتهديدات الخارجية، الوصول إلى هدف نهائي، يتمثل في التوصل لإستراتيجية مقترحة للمنظمة.

خطوات البحث:

بناء على الخطوات النظرية السالفة، يسير البحث وفقًا للخطوات الإجرائية التالية:

- **الخطوة الأولى:** الإطار العام، ويشمل المقدمة، والمشكلة، والأهداف، والأهمية، والحدود، والمنهج المستخدم، وخطوات البحث.
- **الخطوة الثانية:** إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية "إطار نظري".

- **الخطوة الثالثة:** واقع إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية بـ ج. م. ع، والتي يتم فيها تحديد جوانب القوة والضعف في البيئة الداخلية، والفرص والتهديدات بالبيئة الخارجية.
- **الخطوة الرابعة:** تصميم جدول التحليل الرباعي للخروج بعدة إستراتيجيات لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية بـ ج. م. ع.
- **الخطوة الخامسة:** صياغة الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية بـ ج. م. ع.

القسم الثاني ـ إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية، "إطار نظري":

يتناول البحث في هذا القسم بالتحليل الإطار النظري عن الأمن المعلوماتي في المدرسة الثانوية الصناعية، وذلك وفقًا للمحاور التالية:

أولًا: الأمن المعلوماتي في المدرسة الثانوية الصناعية.

ثانيًا: إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

وفيما يلي تفاصيل ذلك:

أولًا ـ الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تعتمد المدارس بشكل عام على الاحتفاظ بما لديها من معلومات في قواعد بيانات على أجهزتها، ويقوم بعمل تلك القواعد المتخصصون في مجال عمل قواعد البيانات، وتتنوع قواعد البيانات بين قواعد خاصة ببيانات الطلاب، وأعضاء هيئة التدريس، وميزانية المدرسة، وإمكاناتها المادية والبشرية، وكل ما تمتلكه المدرسة، أو تحتاجه لتحقيق أهدافها، ونظرًا للطبيعة الخاصة للمدرسة الثانوية الصناعية فتتنوع قواعد البيانات الموجودة بها، نظرًا لطبيعتها في الإنتاج، وإعداد الميزانيات، وإعداد دراسات الجدوى، وغيرها من الأمور التي ترتبط بالطبيعة الإنتاجية لتلك المؤسسات.

وتهدف المدرسة الثانوية الصناعية إلى تحقيق ما يلي: [20]

- تقديم المعرفة التي تمكن الطلاب من فهم الدور الذي تقوم به التكنولوجيا المتطورة في مجال الصناعة، وتأثيرها على المجتمع والبيئة المحيطة.
- إمداد الطلاب بالمعرفة اللازمة والكفاءة التي تمكنهم من تطبيق تعليمات الصحة والسلامة والأمن الصناعي، وإدارة المخاطر بشكل عملي.

- تمكين الطلاب من امتلاك المعرفة والكفاءة في تصميم المنتجات، وعمل المشروعات العملية.

وبالنظر إلى هذه المدرسة تتضح الطبيعة الخاصة لها؛ فهي تسعى للقيام بمشروعات، وتسعى إلى تمكين الطلاب من مهارات إدارة المخاطر، نظرًا للاقتناع بما يمكن أن يحدث في إطار بيئة العمل التي تسيطر على طبيعتها العملية، كما تسعى إلى تصميم المنتجات؛ الأمر الذي يتطلب كمًّا من المعلومات تحسبًا للظروف التي قد تحدث للمدرسة أثناء محاولتها لتحقيق تلك الأهداف.

1. أهداف الحفاظ على الأمن المعلوماتي في المدارس الثانوية الصناعية:

تتنوع أهداف الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، ومن تلك الأهداف ما يلي: [21]

- الحفاظ على المعلومات الموجودة في المدرسة من الاستخدام غير الآمن.
- التأكيد على ضرورة إحداث التكامل بين المعلومات الموجودة على قواعد البيانات.
- سهولة استرجاع المعلومات وقت الحاجة إليها.
- ضمان استمرارية العمل من خلال الحفاظ على المعلومات التي يتطلبها إنجاز هذا العمل.
- تدريب جميع أعضاء المجتمع المدرسي على حماية بيانات ومعلومات المدرسة بما يضمن سريتها، وسهولة استرجاعها وقت الحاجة.

وكما سبقت الإشارة، يعتبر الحفاظ على الأمن المعلوماتي وسيلة لغاية أكبر منها، ألا وهي مساعدة المدرسة الثانوية الصناعية على التعافي من الأزمات التي قد تتعرض لها، خاصةً أنها بيئة ملائمة لحدوث المشكلات والأزمات، بل وضمان استمرارية عمل المدرسة أثناء حدوث الأزمة، واستمرار تقديم الخدمة التعليمية، بل وأيضًا استمرار إنتاجية المدرسة، خاصةً أن طبيعة عمل تلك المدرسة تركز بالدرجة الأولى على الإنتاج.

2. الأجهزة المستخدمة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تتنوع الأجهزة المستخدمة للحفاظ على الأمن المعلوماتي في المدرسة، فلا يستقيم الحفاظ على الأمن المعلوماتي دون وجود مثل تلك الأجهزة، ومنها: [22]

- **أجهزة الكمبيوتر:** وهي الأجهزة التي سيتم على أساسها عمل الشبكات الداخلية بين الأقسام المختلفة في المدرسة، والشبكات التي تربط المدرسة بما خارجها، سواء بالمجتمع الخارجي، أو على المستوى الدولي، والتي تتمثل في علاقة المدرسة بالمدارس الأخرى على مستوى العالم، ووفقًا لتلك المهمة ينبغي أن تتسم تلك الأجهزة بمواصفات تقنية عالية، والبرمجيات الحديثة والأصلية، وأيضًا تكون مزودة ببرامج مضادة للفيروسات لحماية الأجهزة من الاختراق قدر الإمكان، مع الحرص على تحديث تلك البرامج باستمرار.
- **كاميرات الفيديو:** وتستخدم لتوثيق بعض الأحداث التي تحدث في المدرسة، كزيارة أحد المسئولين، أو معرض، أو ندوة، أو مؤتمر، أو برنامج تدريبي تم عقده بإحدى الوحدات المدرسية، والتي يمكن الرجوع إليها مرة أخرى وقت الحاجة للاستفادة بخبرات المدرسة السابقة في مواقف مشابهة.
- **شبكات وكابلات الإنترنت:** وهي عبارة عن الكابلات والأجهزة المستخدمة لربط أجهزة الكمبيوتر بشبكة المعلومات الدولية، الأمر الذي يسهل على مسئول تكنولوجيا المعلومات في المدرسة الدخول لموقع المدرسة بانتظام والتعديل فيه وتحديثه، كما يسهل للطلاب متابعة كل جديد على موقع المدرسة، بل واستخدام هذا التواصل الدولي في التعرف على خبرات مدارس أخرى، وتبادل الخبرة معهم في مجال التخصص.
- **كابلات الشبكات الداخلية:** وهي الكابلات المستخدمة لربط الوحدات والمكاتب الموجودة في المدرسة ببعضها البعض؛ بهدف تسهيل التواصل بينهم، والسرعة في إنجاز العمل، بل وتبادل المعلومات بينهم كلما اقتضت الحاجة لذلك.

وبالنظر إلى ما سبق، يتضح أن هناك بنية تحتية يجب أن تتوافر لتحقيق الأمن المعلوماتي المرغوب للمدرسة، والتي بدونها لا يستقيم تحقيق هذا الأمن

المعلوماتي، ومن ثم على إدارة المدرسة الثانوية الصناعية توفير تلك الأجهزة والمعدات، تمهيدًا للحفاظ على أمن المعلومات الخاصة في المدرسة.

3. متطلبات الحفاظ على الأمن المعلوماتي في المدارس الثانوية الصناعية:

هناك عدة متطلبات يجب أن تتوافر لتحقيق الأمن المعلوماتي في المدرسة، ومن تلك المتطلبات ما يلي: [23]

- الموارد البشرية المدربة على استخدام وسائل التكنولوجيا المختلفة.
- برامج تدريبية للموارد البشرية للتعرف على كل جديد في مجال الحفاظ على المعلومات واستردادها.
- كتيبات إرشادية توضح للجميع أهمية الحفاظ على الأمن المعلوماتي في المدرسة توزع على مسئولي الوحدات المختلفة.
- إدارة إلكترونية واعية بأهمية الحفاظ على دقة المعلومات وسريتها.
- تغيير كلمة السر الخاصة بالأجهزة والموقع الإلكتروني من آن لآخر.
- تصنيف المعلومات الموجودة في المدرسة وفقًا لطبيعتها والهدف منها.

ومما هو جدير بالذكر أن الأجهزة لا تعتبر هي المتطلب الوحيد للحفاظ على الأمن المعلوماتي للمدرسة الثانوية الصناعية، بل هناك متطلبات أخرى يجب توفيرها لتحقيق الأمن المعلوماتي المطلوب، الأمر الذي يتطلب في المقام الأول إدارة واعية بتلك المتطلبات لتوفيرها في المدرسة، حتى يمكن تأدية مهمة الحفاظ على الأمن المعلوماتي بفاعلية عالية.

4. آليات الحفاظ على الأمن المعلوماتي في المدارس الثانوية الصناعية:

يعتبر الحفاظ على بيانات المدرسة الثانوية الصناعية واستخدامها على نحو جيد من أهم أدوات الوصول إلى جودة أداء المدرسة، واستمرارية أعمالها في وقت حدوث الأزمات والطوارئ، ويتطلب الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية تبني مجموعة من الآليات المحددة، والتي يمكن إجمالها فيما يلي:

- **توفير البنية التحتية ذات الكفاءة العالية لتدعيم الاستخدام الآمن لتكنولوجيا المعلومات:**

لعل الحفاظ على أمن المعلومات لا يقتصر فقط على توفير الأجهزة الإلكترونية ـ كأجهزة الكمبيوتر، والتركيبات الخاصة بالشبكات الداخلية والخارجية،

وأطباق الستالايت، وأجهزة الفيديو، والتليفزيون، وإنما يتطلب أيضًا الكفاءة العالية لتلك الأجهزة التي من شأنها تأمين فرصة للمستخدمين للحصول على المعلومات، وفرصتهم أيضًا للحفاظ عليها، واستعادتها وقت الحاجة، بناء على كفاءتها العالية في الاحتفاظ بالمعلومات وحمايتها من الدخلاء. (24)

وبالنظر إلى الطبيعة الخاصة للمدرسة الثانوية الصناعية، يلاحظ أن بها عددًا ليس بالقليل من المعلومات التي يجب الحفاظ عليها، كالميزانية، والمشروعات التي ينجزها الطلاب، والإيرادات، والمصروفات، وقواعد البيانات الخاصة بالطلاب، وأنشطتهم المختلفة، وقواعد البيانات الخاصة بالمعلمين، ومنظمات الأعمال التي بإمكانها الاستفادة من منتجات تلك المدارس، واتفاقيات الشراكة بين المدارس الثانوية الصناعية وقطاع الأعمال بالمجتمع الخارجي، الأمر الذي يستوجب الحفاظ على تلك البيانات والمعلومات لما لها من دور في الحفاظ على القدرة الإنتاجية للمدرسة الثانوية الصناعية، بالشكل الذي يحافظ على أدائها التعليمي، وقدرتها الإنتاجية.

- **إشراك الطلاب في الحفاظ على الأمن المعلوماتي في المدرسة:**

يعتبر الجيل الجديد من أكثر المقومات التي تساعد إدارة المدرسة على الحفاظ على أمنها المعلوماتي، وذلك بالاستعانة بهم وبخبراتهم في التعامل مع الأجهزة الإلكترونية الحديثة، ومواقع التواصل الاجتماعي، التي يتبنون من خلالها كافة الإجراءات اللازمة للحفاظ على ما بها من بيانات ومعلومات ومحادثة بينهم، وبين زملائهم، والتي من الممكن أن يكون لها وزنها، ويمكن الاستعانة بها في مساعدة المدرسة على تأمين معلوماتها، الأمر الذي يشعرهم بأهمية ما يقومون به من أعمال هم على دراية وخبرة بها، ولكن مع الوضع في الاعتبار أن تضع المدرسة للطلاب القواعد والقوانين التي يعملون في إطارها. (25)

وبالنظر إلى ما سبق، يتضح أن أحد أهم مقومات الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، هم الطلاب أنفسهم، على اعتبار أنهم المخرج الأساسي للمدرسة، كما أنهم في مرحلة عمرية تتميز بالتحدي، والرغبة في إثبات الذات، والشعور بأهمية ما يقومون به من أعمال، كما أنهم في مرحلة عمرية اكتسبوا فيها خبرة طويلة في التعامل مع التكنولوجيا الحديثة، من خلال التفاعل مع جماعات الأقران، والتعامل مع التكنولوجيا الحديثة بالمناهج الدراسية المقررة عليهم

منذ بدء التحاقهم بالمدرسة، وحتى وصولهم إلى المدرسة الثانوية، الأمر الذي انعكس على عمق خبرتهم في التعامل مع التكنولوجيا، وأصبح له مردود في قدرتهم على تقديم الحلول والمقترحات والتوصيات في الحفاظ على الأمن المعلوماتي لما تمتلكه المدرسة الثانوية الصناعية من معلومات يجب الحفاظ عليها، لضمان استمرار تقديم الخدمة التعليمية التي تقدمها، ولكن مع توخي الحذر وإضافة كلمات مرور للمعلومات الهامة الموجودة على الأجهزة من قبل المسئولين عن تلك المعلومات، واتخاذ كافة التدابير والضمانات للحفاظ على هذه المعلومات، حتى لا يكون الطلاب أنفسهم هم السبب الأساسي وراء اختراق المعلومات الهامة للمدرسة.

كما يمكن إضافة الآليات التالية: [26]

- **الحفاظ على أمن البريد الإلكتروني الخاص بالمدرسة:**

ويعني ذلك أن يكون المسئول عن الرد على رسائل أولياء الأمور، أو المعنيين، أو المسئولين بالوزارة أو بالإدارات التعليمية، محتفظًا بكلمة سر آمنة للبريد الإلكتروني، حتى لا يستطيع أي فرد الاطلاع على محتوى تلك الرسائل، إذ إنها محتويات لا يتثنى لأحد الاطلاع عليها إلا المختصين من إدارة المدرسة.

ومن ثم يجب أن يكون ذلك الشخص هو شخص واحد، بحيث لا يمكن لأحد غيره الاطلاع على مثل تلك الرسائل، وبالتالي تكون فرصة تسرب المعلومات الواردة بتلك الرسائل ضئيلة، إن لم تكن معدومة، ويكون دوره محصورًا في نقل محتويات تلك الرسائل إلى مدير المدرسة، الذي بدوره ينقلها إلى باقي أعضاء المجتمع المدرسي، كل فيما يخصه، وما يفيد إنجازه للعمل.

- **الحفاظ على المعلومات وأجهزة الحاسب الآلي في مأمن من الفيروسات:**

يجب الحفاظ على الأجهزة في مأمن من الفيروسات التي قد تضر بالأجهزة، والبرامج، والموضوعات، والبيانات والمعلومات المخزنة عليها، وذلك عن طريق تثبيت برامج أصلية لمقاومة الفيروسات؛ حتى يسهل تحديثها باستمرار، فيكون الجهاز محميًا من الفيروسات التي قد تضر بما عليه من معلومات؛ فالاعتماد على برامج غير أصلية، لا يسمح بتحديثها، ومن ثم يكون الجهاز بما عليه من معلومات عرضة للهجوم الإلكتروني، ونتيجة لذلك تكون قواعد البيانات في خطر مستمر وعرضة للضياع أو التلف أو السرقة.

- **الحفاظ على الموقع الإلكتروني الخاص بالمدرسة من الاختراق:**

يستخدم موقع المدرسة للإعلان عنها، وعن منتجاتها، وقدراتها، ورؤيتها، ورسالتها قبل أي شيء، ولا يجب أن يكون لأي شخص حق الدخول على موقع المدرسة والتعديل عليه غير الشخص المسئول عن تقديم المعلومات للمستفيدين من الخدمة التي تقدمها المدرسة، كما أنه المسئول عن صدق المعلومات المعروضة لزائري الموقع. وبالتالي تضمن إدارة المدرسة أكبر قدر ممكن من مصداقية المعلومات المعروضة عن المدرسة، والتي تصل إلى المستفيدين من خدماتها كافة.

- **وضع كلمة مرور آمنة لأجهزة الكمبيوتر الموجودة في المدرسة:**

تحتوي أجهزة الكمبيوتر الموجودة في المدرسة على بيانات ومعلومات تتسم بالسرية، ولا يجب أن يتمكن أي فرد من غير المسئولين من الدخول على الكمبيوتر، والاطلاع على تلك المعلومات، بما قد يضر بمصلحة المدرسة، الأمر الذي يتطلب من كل موظف يستخدم جهاز كمبيوتر في مجال عمله، أن يقوم بعمل كلمة مرور له، وللملفات الهامة الموجودة على جهازه، على أن تكون تلك الكلمة آمنة، بمعنى ألا يسهل توقعها، فضلًا على أن تحتوي على حروف وأرقام ورموز في ذات الوقت، الأمر الذي يسهم في صعوبة توقعها، ومن ثَم تأمين الجهاز، وما عليه من معلومات.

ويعتبر استخدام كلمة المرور لكل جهاز، بل وللملفات الهامة الموجودة على الأجهزة ـ خاصةً وإن كان لجهاز الكمبيوتر الواحد أكثر من مستخدم ـ من أكثر الآليات اللازمة للحفاظ على الأمن المعلوماتي للمؤسسات بشكل عام، وللمدارس بشكل خاص، وللمدرسة الثانوية الصناعية بشكل أكثر خصوصية، لما لكل مؤسسة ـ مهما كان تخصصها ـ من معلومات عليها الاحتفاظ بها بمعزل عن غير المتخصصين من العاملين بها؛ لأنهم أصحاب التخصص، وأصحاب الحق في استخدام تلك المعلومات في عملهم داخل المؤسسات والمدارس، ولا يحق لغيرهم استخدامها، أو الاطلاع عليها، ومن ثم يجب على الموظف عند صياغة كلمة مرور أن يتحرى فيها كل عناصر الدقة، والأمان، حتى لا يسهل توقعها من الآخرين، بما قد يعرض المعلومات السرية للسلب، أو التغيير، أو التحريف، أو سوء الاستخدام.

- **اختيار المواقع الآمنة للاستفادة منها:**

تحتاج المدرسة والمسئولون بها إلى الدخول على مواقع إلكترونية من آن لآخر؛ بهدف الاطلاع على خبرات مدارس أخرى، والاستفادة منها، وتناقل الخبرات بينها؛ بغرض التطوير والتحسين. وهذا الأمر يفرض على المسئولين عن أداء تلك الوظيفة اختيار المواقع الآمنة التي يمكن الاعتماد عليها للحصول على مثل تلك المعلومات، دون الإضرار بأجهزة المدرسة، أو موقعها الإلكتروني.

ولعل الاعتماد على مواقع لها سمعتها، مثل المواقع الرسمية للمدارس الثانوية الصناعية ذات السمعة الرسمية بجميع دول العالم، من شأنها عدم الإضرار بأجهزة الكمبيوتر المستخدمة، كما أنها تساعد المسئولين عن تلك الوظيفة في الحصول على معلومات ذات مصداقية عالية، مما يسهل عملية تبادل الخبرة بين المدارس الثانوية الصناعية بأنحاء العالم كافة.

- **الحفاظ على نسخ من قواعد البيانات الموجودة في المدرسة على وسائط تخزين خارجية:**

من الضروري تخزين قواعد بيانات المدرسة على وسائط تخزين خارجية، تحسبًا لحدوث أي مشكلة قد تتسبب في فقدان أي قاعدة بيانات خاصة بالمدرسة، الأمر الذي يحول دون تعطيل سير العمل في المدرسة بسبب الأزمة. (27)

ومن ثم يتضح أن حفاظ المسئول عن الأمن المعلوماتي في المدرسة الثانوية الصناعية، على نسخ احتياطية للمعلومات الموجودة في المدرسة كافة، على أقراص صلبة، أو أقراص مدمجة، وكذلك الهاردات الخارجية والفلاشات والأسطوانات وغيرها، مما قد يستحدث في المستقبل، بالإضافة إلى أنها قد تشمل كذلك التخزين السحابي، مثل التخزين على Google drive, one drive, etc.، وكذلك السيرفرات الخاصة بالتخزين، التي من شأنها الحفاظ على تلك المعلومات وقت الحاجة، واستعادتها عند حدوث أي ظروف في المدرسة، تستلزم استعادتها مرة أخرى، وخاصةً في بيئة مدرسية محفوفة بالمخاطر، مثل بيئة المدرسة الثانوية الصناعية.

وبناء على ما سبق عرضه من آليات من شأنها الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، يتضح أن هناك عددًا ليس بالقليل من تلك السياسات، التي من السهل ـ على المدارس كافة بشكل عام، والمدارس الثانوية

الصناعية بشكل خاص ـ تبنيها، ذلك أن البيانات، والمعلومات بالمؤسسات التعليمية ثروة يجب استغلالها والحفاظ عليها من الضياع أو التلف، إذ إنها سبيل تلك المؤسسات للنهوض، في حالة حدوث أي ظروف طارئة قد تضر بها، أو تحول دون القيام بوظائفها المعتادة، وكذلك الحال بالنسبة للمدارس الثانوية الصناعية؛ حيث إنها أكثر عرضة للمخاطر التي قد تحول دون استمرارية نشاطها، فتكون البيانات والمعلومات آنذاك هي سبيلها لاستعادة هذا النشاط بنفس المستوى الذي كانت عليه.

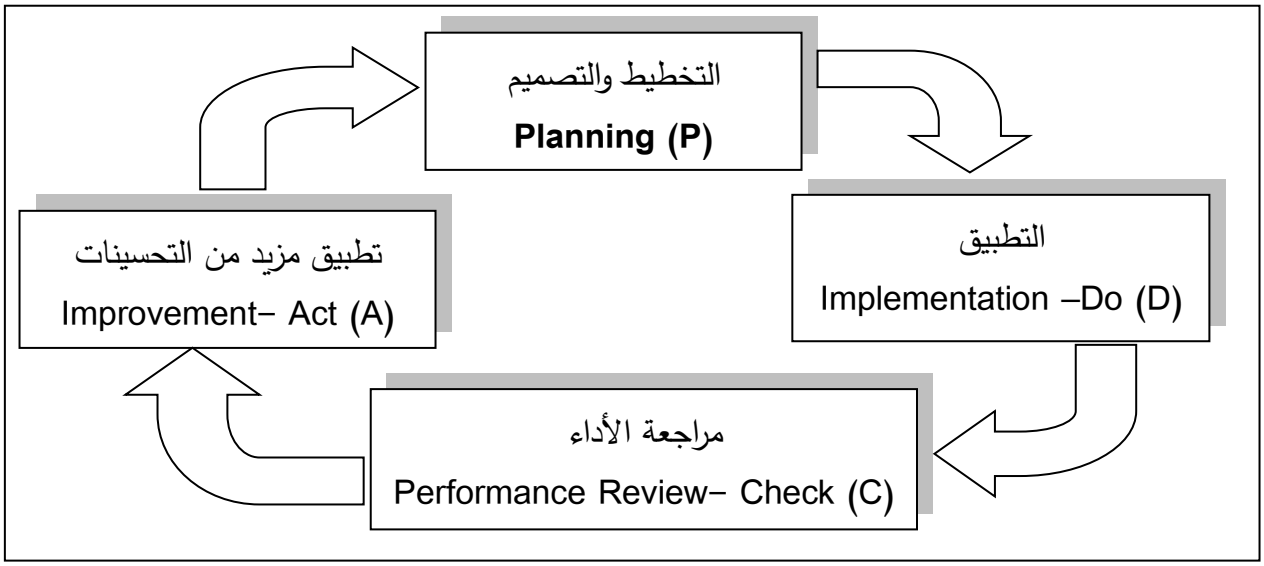
5. دورة حياة الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تعني دورة حياة الأمن المعلوماتي الخطوات والمراحل التي تمر بها المعلومات من بداية استخدامها، وحتى الاستفادة منها بالشكل الذي يحافظ عليها في صورتها، دونما أي خلل أو ضرر قد يحدث لها، مع التأكيد على أن تلك الخطوات تسير في شكل دائري ومستمر، أي أنها عملية غير منتهية.

وتشتمل دورة حياة الأمن المعلوماتي على أربع مراحل أساسية، تبدأ بالتخطيط Planning، الذي يقصد به وضع الخطط قصيرة وطويلة الأمد، والاستعداد للحفاظ على الأمن المعلوماتي للمنظمة ضد أي خطر قد يؤثر سلبًا عليه، ويطلق على المرحلة الثانية مرحلة تطبيق الخطة الموضوعة وتنفيذ المشروع Implementing the Plan and Carrying out the Project، وفيها يتم تنفيذ بنود الخطة الموضوعة في المرحلة السابقة، أما المرحلة الثالثة فتسمى بمرحلة مراجعة الأداء ومراقبة تحقيق الأهداف Performance Review and Monitoring the Achievement of Objectives، وفيها يتم التأكد من تحقيق المنظمة لأهدافها في المحافظة على أمنها المعلوماتي، أي أن المعلومات محفوظة بطريقة فعالة، وأنها آمنة ولم يتم اختراقها، أما المرحلة الرابعة فيطلق عليها تحديد نقاط القوة والضعف في الخطةEliminating Discovered Flows and Improvements، والتي تتضح من خلال التنفيذ، وذلك للاستفادة منها عند وضع الخطط الأخرى، وإذا ثبت أن هناك العديد من نقاط الضعف في الخطة الموضوعة، فيجب العودة إلى مرحلة وضع الخطة، وإجراء مزيد من التعديلات على الخطة التي تم بناؤها في تلك المرحلة للتقليل من نقاط الضعف والوصول إلى خطة عالية الجودة، وبناء عليه قام العالم ديمنج Deming، بتصميم هذه المراحل في نموذج أسماه نموذج دورة حياة الأمن

المعلوماتي Lifecycle Information Security Model، والذي اختصره إلى أربع كلمات أساسية بإمكانها تمثيل المراحل السابقة، وهي: خطط Plan، وافعل Do، وراجع Check، ونفذ Act، وأطلق عليه نموذج PDCA، ويمكن تمثيل دورة حياة الأمن المعلوماتي على الشكل التالي: [28]

شكل رقم (1) دورة حياة الأمن المعلوماتي



مما سبق، يتضح أن دورة حياة الأمن المعلوماتي عملية مستمرة، الأمر الذي يظهر بشكل أكثر وضوحًا في المدرسة الثانوية الصناعية، إذ إن أولى الخطوات تتمثل في وضع الإستراتيجية اللازمة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية، وذلك وفقًا للأهداف المحددة سلفًا لذلك، ثم يأتي دور التطبيق المبدئي، الذي تظهر من خلاله العيوب التي تتسم بها الإستراتيجية، والفجوة بين الأهداف المحددة والإنجازات التي تم تحقيقها، ومن خلال مراجعة نقاط القوة والضعف، ومقارنتها بالأهداف المحددة سلفًا عند بناء الإستراتيجية، يتم تحديد مزيد من التحسينات التي يجب أن يتم إجراؤها على الإستراتيجية؛ لإدارة عمليات الأمن المعلوماتي في المدرسة. الأمر الذي يوضح أن دورة الحياة عملية مستمرة، ولا تتوقف بعد انتهاء بناء إستراتيجية واحدة، إنما الأمر في حاجة إلى بناء عدد لا نهائي من الإستراتيجيات لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

6. دور الإدارة المدرسية في إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية:

لإدارة المنظمات دور لا يمكن إغفاله في إدارة عمليات الأمن المعلوماتي بها، ومن ثم يقوم مدير المنظمة بعدد من الأدوار للحفاظ على الأمن المعلوماتي بمنظمته، وعلى ذلك يستطيع مدير المدرسة الثانوية الصناعية القيام بذات الأدوار لإدارة عمليات الأمن المعلوماتي بمدرسته، ومن تلك الأدوار ما يلي: [29]

- إصدار جميع الأوامر والتوجيهات واللوائح التي تضمن الحفاظ على الأمن المعلوماتي بالمنظمة على مستوى التنفيذ.
- دمج الأمن المعلوماتي بأجهزة المنظمة كافة وإداراتها المختلفة، ومن ثم ضرورة تدريب الموظفين على التمكن من مهارات التعامل معها.
- إدارة الأمن المعلوماتي والحفاظ عليه من خلال وضع إستراتيجية للأمن المعلوماتي، وتحديد أهداف الحفاظ على المعلومات بالمنظمة، ويجب أن يوافق عليها الموظفون بالمنظمة، بالإضافة إلى استثمار التجارب التي واجه فيها الأمن المعلوماتي في المدرسة بعض المخاطر للاستفادة منها في المستقبل، ثم وضع الإجراءات التحصينية المختلفة التي تحافظ على الوضع الحالي للمعلومات الموجودة بالمنظمة، ثم إتاحة الموارد والمصادر اللازمة للحفاظ على الأمن المعلوماتي بالمنظمة من أجهزة وبرامج وغيرها من الموارد الأخرى، ثم الاهتمام بالمراجعة الدورية لإستراتيجية الأمن المعلوماتي الموضوعة، وأخيرًا حث الموظفين على تطبيق بنود الإستراتيجية الموضوعة للحفاظ على الأمن المعلوماتي للمنظمة بشكل فعلي.
- تحديد الأهداف التي تم تحقيقها بالفعل ومقارنتها بالأهداف المحددة سلفًا لتحديد نقاط القوة والضعف في الأداء.

بناء على ما سبق، ثمة أدوار لمدير المدرسة الثانوية الصناعية عليه القيام بها للحفاظ على الأمن المعلوماتي بها، منها إصدار بعض اللوائح التي تلزم العاملين المتخصصين في أعمال الكمبيوتر في المدرسة ـ من إداريين أو معلمين مسئولين عن حفظ سجلات المدرسة ومعلوماتها ـ بالالتزام بالحفاظ على ما تقع أيديهم عليه من معلومات، وتوقيع العقاب عليهم في حال تقصيرهم، كما أن مدير المدرسة الثانوية

الصناعية عليه أن يزود جميع الإدارات لديه بالأجهزة الإلكترونية لتخزين المعلومات عليها، والحفاظ على سريتها، ومن ثم ضرورة تدريب المتعاملين مع تلك الأجهزة للتمكن من مهارات استخدامها، وتخزين أكبر قدر ممكن من البيانات والمعلومات عليها، ثم عليه إعداد تقارير دورية عن المخاطر التي تعرض لها نظام الأمن المعلوماتي في المدرسة؛ للاستفادة منها مستقبلًا، ووضع مزيد من الإجراءات التحصينية التي تحول دون مواجهة تلك المخاطر في المستقبل، وتطوير الإستراتيجية الموضوعة للحفاظ على الأمن المعلوماتي باستمرار؛ لتتواكب مع التغيرات والمستحدثات المحيطة في مجال تكنولوجيا المعلومات، كما أن عليه تشجيع المسئولين عن أمن المعلومات في المدرسة على الحفاظ على المعلومات التي لديهم بالفعل، وفقًا لشروط الإستراتيجية التي تم وضعها والموافقة عليها من قبل المدير وموظفيه، وأخيرًا على المدير تقويم ذاته باستمرار؛ للتأكد من أن الأهداف التي تم وضعها سلفًا تم تحقيقها بالدرجة المتوقعة قبل بدء التنفيذ، وإلا عليه الرجوع مرة أخرى من البداية، واتخاذ مزيد من الإجراءات التحصينية التي تحافظ على الأمن المعلوماتي للمدرسة الثانوية الصناعية.

ويقوم مدير المدرسة أيضًا بتشكيل فريق الأمن المعلوماتي في المدرسة ـ والذي يطلق عليه فريق حارسي البيانات Data Guardians ـ من موظفي وحدة تكنولوجيا المعلومات في المدرسة IT Unit، ولكل منهم مجموعة من المسئوليات والأدوار.

7. فريق الأمن المعلوماتي:

يتكون فريق الأمن المعلوماتي من الأعضاء التاليين: [30]

- **مدير المشروع Director Project:** وهو المسئول عن إنتاج المعلومات الخاصة ببحث أو بعمل علمي يقوم به أعضاء الفريق المدرسي، المسئول عن البيانات أو المعلومات، وذلك بالتعاون بينه وبين أعضاء المجتمع المدرسي المشتركين في هذا البحث، بالإضافة إلى تقديم المشورة لهم عند الحاجة، وتسهيل انتقال المعلومات بين أعضاء الفريق لإنجاز المهمة البحثية، وعليه أيضًا ضمان الاستخدام والانتقال الآمن لهذه المعلومات، والحفاظ عليها، فيتولى حق إصدار كلمات المرور وتغييرها عندما يستدعي الأمر ذلك، وإدارة

المعلومات نفسها عن طريق التحكم في الدخول لمواقع المعلومات، والاحتفاظ بنسخ احتياطية لها، واسترجاعها وقت الحاجة إليها.

- **مديرو النظام System Administrators:** وهم المسئولون عن أنظمة المعلومات بالمنظمة، مثل: التمويل، والتسجيل، والموارد البشرية، بما في ذلك إدارة المستخدمين، مثل: حق الدخول، وميكانزمات الأمن المعلوماتي المستخدمة، وإدارة المعلومات نفسها عن طريق التحكم في الدخول لمواقع المعلومات، والاحتفاظ بنسخ احتياطية لها، واسترجاعها وقت الحاجة إليها.
- **رؤساء القسم Heads of Department:** وهم المسئولون عن توثيق ودعم أمن المعلومات، التي من الممكن أن تشتمل على وثائق المدرسة، وعقود العمل، ومعلومات عن موظفي المنظمة، وقواعد البيانات الخاصة بهم، كما أنها قد تشتمل على قواعد البيانات الخاصة بالعاملين بتلك المنظمة.
- **فريق خدمات المعلومات Information Service Staff:** وهو فريق فرعي منبثق عن الفريق الأساسي (فريق أمن المعلومات)، وهم المسئولون عن التأكد من توافر البنية التحتية اللازمة لتخزين المعلومات والحفاظ عليها وعلى سلامتها، والتأكيد على التوافق بين المتطلبات التي يتطلبها الأمن المعلوماتي داخل المنظمات والإمكانات المادية الموجودة بالمنظمة لمساعدتها على أداء مهامها.

8. الآثار السلبية لاختراق الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تواجه المدرسة العديد من الآثار السلبية في حال تم اختراق معلوماتها، ومن تلك الآثار ما يلي: [31]

- فشل النظام المعلوماتي، أو فساد وإفساد المعلومات.
- حدوث عدوى لأجهزة الكمبيوتر عن طريق بعض الفيروسات المدمرة للأجهزة.
- سرقة بعض المعلومات من على أجهزة الكمبيوتر الموجودة في المدرسة، أو سرقة بعض أجهزة الكمبيوتر المحمول التي قد تحوي معلومات سرية، أو شخصية.
- سوء استخدام بعض الموظفين للأجهزة والتي قد تتلفها، نتيجة نقص خبراتهم في التعامل مع الأجهزة المتاحة لهم للتعامل معها.

- اختراق المواقع الإلكترونية للمدرسة، وتعديل ما عليها من معلومات، الأمر الذي ينتج عنه إضافة معلومات غير حقيقية، ومضللة للمستفيدين من الموقع وخدماته.
- دمار قواعد البيانات الموجودة في المدرسة، سواء ما تخص الطلاب أو المعلمين، أو أي إمكانات في المدرسة؛ مما يؤثر سلبًا على صنع القرارات واتخاذها في الوقت المناسب.

وبالنظر إلى الآثار السلبية سالفة الذكر، يتضح أن تلك الآثار تتحول جميعها إلى أخطار في المدرسة الثانوية الصناعية على وجه الخصوص، ذلك أنها مدرسة غير تقليدية، قد تحدث بها العديد من الأخطار والحوادث غير المتوقعة، نظرًا لطبيعة الدراسة والعمل بها؛ فهناك المعامل، والورش، ويتعامل الطلاب فيها مع الأجهزة، والمعدات الثقيلة، ويطلب منهم القيام بصيانة الأجهزة، وإنتاج منتجات، وتسويقها، وغيرها من مجالات العمل المحاطة بالمخاطر التي قد تضر بالإنتاج من ناحية، وبالنشاط التعليمي من ناحية أخرى، وعليه، إن لم تكن قواعد البيانات والمعلومات في المدرسة، بل والأجهزة محمية بأعلى درجات الأمان؛ لاستخدامها في مثل تلك الظروف الطارئة، فإن المشكلات تتحول إلى أزمات يصعب التعامل معها؛ إذ تتحول المشكلات البسيطة إلى مشكلات مركبة، بل إلى مشكلات معقدة وأزمات، إذا لم تكن هناك البيانات والمعلومات الكافية للتخلص من الآثار السلبية للمشكلات وقت ظهورها.

9. أبعاد الأمن المعلوماتي في المدرسة الثانوية الصناعية:

للأمن المعلوماتي عدد من الأبعاد، تتمثل فيما يلي:

- **البعد البشري: People Dimension**

يمثل العاملون البعد الأكثر أهمية من أبعاد الأمن المعلوماتي، لما لهم من تأثير قوي في الحفاظ على هذا الأمن للمنظمة التي يعملون بها، فإذا كانوا متمكنين من استخدام الأجهزة اللازمة لتخزين المعلومات الموجودة بالمنظمة والحفاظ عليها من الاختراق، فإن ذلك يؤدي إلى وجود نظام فعال للأمن المعلوماتي في المدرسة، أما إذا قلّت قدرتهم على القيام بتلك المهمة نتيجة لجهلهم بالمهارات اللازمة لها، أو قلة تدريبهم عليها، فإن ذلك يهدد أمن المعلومات بمنظمتهم، الأمر الذي يحولهم إلى

أعداء للمنظمة، كما أن ضعف إدراك العاملين بأهمية الدور الذي يقومون به للحفاظ على سرية المعلومات وأمنها من الاختراق أو التزوير أو التلاعب، يؤدي ـ في بعض الأحيان ـ إلى الاستهتار بالمهمة الموكلة إليهم، ومن ثم بدا من المهم أن يُقدم للعاملين بالمنظمات عدد من البرامج التدريبية التي توضح لهم أهمية الدور الذي عليهم القيام به للحفاظ على الأمن المعلوماتي بمنظمتهم، وعلى المنظمة قياس أثر التدريب، الذي يظهر من خلال أداء العاملين بعد حصولهم على البرنامج التدريبي، كما يجب أن تركز تلك البرامج التدريبية على ما يلي: [32]

- تغيير الطريقة التي يفكر بها العاملون حين يعملون في مجال الأمن المعلوماتي بشأن أهمية المهام التي يقومون بها.
- قياس أثر تدريب العاملين في أماكن عملهم.
- تقديم برامج تدريبية تنمي الثقافة الداعمة لأهمية الحفاظ على الأمن المعلوماتي للمنظمة، الأمر الذي يساعد العاملين على القيام بعملهم بناء على قناعة تامة بأن الحفاظ على الأمن المعلوماتي يسهم في تحقيق النجاح لها.

واتساقًا مع ما سبق، يمكن القول: إنه إذا كان الأفراد هم الثروة الحقيقية لأي منظمة، فهم أيضًا الثروة الحقيقية للمدرسة الثانوية الصناعية، وسبل تحقيق ميزتها التنافسية، ولذا فمن المهم أن تولي المنظمات التعليمية عناية فائقة بتدريبهم وتأهيلهم لكي يمتلكوا الكفاءات والجدارات التي تمكنهم من الحفاظ على الأمن المعلوماتي لمدارسهم.

- **البعد السياسي: Political Dimension**

يمثل بعد السياسة أحد الأبعاد الهامة للأمن المعلوماتي، ويشير إلى جميع الموجهات الفكرية التي تساعد المنظمة على اختيار المقاييس والطرق اللازمة لتحقيق الأمن المعلوماتي ومنع التهديدات، ولذا يعتبر بعد السياسة هو المحدد للطرق والأساليب التي تساعد المنظمة على الحفاظ على أمنها المعلوماتي. [33]

وعليه فإنه ينبغي أن تكون سياسات الأمن المعلوماتي واضحة في أذهان العاملين، ويجب أن يكون لديهم وعي بها، ويجب أن تكون نتائجها قابلة للقياس؛ للتأكد من قدرتها على تحقيق الأمن المعلوماتي للمنظمة، كما أنها يجب أن تكون قابلة للتحقيق، ومن ثم فإن السياسات الواضحة من شأنها تحديد المسئوليات

والواجبات التي على الموظفين القيام بها لتحقيق الأمن المعلوماتي المنشود للمنظمة، الأمر الذي يساعد الموظفين على طاعة Compliance الأوامر، وتنفيذ المسئوليات الموكلة إليهم في هذا الشأن. (34)

بناء على ما سبق، يرتبط البعد السياسي بسياسات الحفاظ على الأمن المعلوماتي سالفة الذكر، إذ إن إدراك العاملين لسياسات الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، من شأنه مساعدتهم في الحفاظ على أمن المدرسة، إذ يجعلهم هذا الإدراك واعين، بل ملتزمين باختيار السياسة الملائمة للحفاظ على الأمن المعلوماتي بمدرستهم.

- **البعد التكنولوجي: Technological Dimension**

هو البعد الذي يركز على الموارد المادية التي تساعد على تخزين المعلومات واسترجاعها وقت الحاجة، مثل أجهزة الكمبيوتر التي يستخدمها العاملون لعمل قواعد البيانات، وإدارتها، وكيفية الاستخدام الآمن للمعلومات والبيانات من شبكة الإنترنت. (35)

كما يعد هذا البعد من حتميات الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية؛ فالحفاظ على المعلومات في حاجة إلى أجهزة يتم تخزين المعلومات عليها، ويحتاج إلى شبكات، وغيرها، فبدون أجهزة، ستضعف فرص الحفاظ على البيانات والمعلومات؛ فالمعلومات الورقية أقل أمنًا من المعلومات المخزنة على الأجهزة، إذ إنها تكون أكثر عرضة للإفساد، والتلف، والسطو، والتزوير، وغيرها من المخاطر الأخرى.

- **البعد التدعيمي: Enforcement Dimension**

هو البعد الذي يركز على قدرة العاملين على فهم السياسات المستخدمة للحفاظ على أمن المنظمة المعلوماتي، وذلك لوعيهم بها، وفهمهم لها، واقتناعهم بما يجب أن يقوموا به من أعمال، مما يجعل هناك فرصة أكبر لتحقيق أكبر قدر ممكن من الأمن المعلوماتي للمنظمة، كما يؤدي إلى دعم قدرة المؤسسة على الحفاظ على أمنها المعلوماتي، وهناك عدد من السبل اللازمة لتطبيق هذا البعد، منها ما يلي: (36)

أ- التحكم في بيئة العمل Monitoring Work Environment: يعتبر التحكم في بيئة العمل من أهم العناصر اللازمة لتحقيق البعد التدعيمي

بالمنظمات، إذ إن تأمين بيئة العمل، والأجهزة، وشبكات الاتصال، والمواقع المستخدمة بالمنظمة، من شأنها الحفاظ على سرية المعلومات، وكذلك فإن التأمين المستمر لأجهزة الكمبيوتر، وتحديث برامج مقاومة الفيروسات، وتغيير كلمة السر الخاصة بملفات البيانات، تساعد على الحفاظ على البيانات والمعلومات الهامة التي تخص المنظمة.

ب- **توثيق كافة الحوادث المتعلقة بالأمن Documenting all Security Incidents:** على الرغم من ضرورة التحكم في بيئة العمل كما سبقت الإشارة، إلا أن هناك بعض الاختراقات والحوادث الأمنية التي قد تصيب بيئة العمل، وفي هذه الحالة، على المسئولين عن الحفاظ على الأمن المعلوماتي توثيق تلك الحوادث كافة، ذاكرين الممارسات التي تم القيام بها للتعامل مع تلك الحوادث؛ للاستفادة منها في مواقف مشابهة، ولتفادي الأخطاء التي أدت إلى تلك المشكلات، التي أدت إلى الاختراق الأمني.

ج- **تطبيق تكنولوجيات التدعيم Implementing Enforcement Technologies:** في هذا العنصر، يتم تطبيق البرامج الداعمة للأمن المعلوماتي على أجهزة الكمبيوتر، وعند الاتصال بالشبكة الدولية، أو الشبكات الداخلية، حيث يقوم البرنامج بمنع حدوث الاتصال أو منع المعلومات من الوصول أو الإرسال، إذا كانت عملية الإرسال مهددة بالمهاجمة من قبل فيروس قد يهدد الجهاز، والمعلومات المخزنة عليه، ومن ثم فإن الشركات المسئولة عن إصدار تلك البرمجيات، وتحديثها، تسهم بشكل كبير في تطبيق تكنولوجيات التدعيم والحفاظ على أمن المعلومات الخاصة بالمنظمة من الاختراق أو التلف، والانتقال من مجرد الحفاظ النظري على المعلومات، إلى حيز التنفيذ العملي، والتطبيق الفعلي للحفاظ على أمن المنظمة المعلوماتي.

- **البعد المؤسسي Organizational Dimension:**

للبعد المؤسسي أهمية لا يمكن إغفالها في الحفاظ على الأمن المعلوماتي بالمنظمة، إذ يشير إلى بناء بنية تنظيمية تتلاءم ومتطلبات الأمن المعلوماتي بالمنظمة، كما أن مقاومة أعضاء التنظيم لتحقيق المتطلبات اللازمة للأمن

المعلوماتي، قد يعد أحد أهم العوامل التي تسهم في إحداث الصراع بين رغبة المنظمة في الحفاظ على أمنها المعلوماتي، وبين مقاومة الموظفين للقيام بالمهام التي تساعدهم على الحفاظ على أمن منظمتهم المعلوماتي، وعليه، من المفترض أن يكون بالمنظمة هيكل إداري مسئول عن التنبه للمشكلات التي قد تهدد أمنها المعلوماتي، وكتابة تقرير عنها، ومحاولة مواجهتها قبل أن تتسلل إلى قواعد البيانات الخاصة بالمنظمة، مما يترتب عليه التحديد الدقيق للمسئوليات والواجبات التي على كل موظف متخصص في مجال تكنولوجيا المعلومات في المدرسة القيام بها، بالإضافة إلى عقد اتفاقيات خارجية مع الشركات المسئولة عن تقديم البرمجيات الخاصة بالحفاظ على الأمن المعلوماتي، بوصفها المسئولة عن توفير البرمجيات الأصلية للمنظمة لمساعدتها في الحفاظ على أمنها المعلوماتي، كما يشتمل هذا البعد على العمليات التي على مدير المنظمة والعاملين القيام بها؛ للحفاظ على الأمن المعلوماتي بها، بداية من التخطيط لمواجهة أي اختراقات أمنية قبل حدوثها، مرورًا بعمليات التنظيم، والتمويل، والاتصال، والرقابة، والتقويم... إلخ، الأمر الذي يسهم في الاستعداد لتلك الخروقات والتعامل معها حال حدوثها. (37)

ويتضح مما سبق، أن وجود مثل هذه البنية التنظيمية يساعد المنظمة على التعافي من الأزمات التي من الممكن أن تحدث لها نتيجة للخروقات التي قد تحدث في نظامها الأمني، والتي ينتج عنها تسرب للمعلومات، وانهيار لقواعد البيانات الموجودة لديها.

وإن كان الأمن المعلوماتي آلية لإدارة التعافي بالمنظمات بشكل عام، فهو آلية هامة جدًّا داخل المدرسة الثانوية الصناعية على وجه الخصوص؛ وذلك لما للمدرسة الثانوية الصناعية من معلومات وبيانات تخص بنيتها، ومشاريعها، وميزانياتها، وإنتاجها، ودراسات الجدوى الخاصة بها، وغيرها من المعلومات السرية التي في حاجة إلى أن تُحفظ من الدخلاء؛ لأنها من الممكن أن تستغل لتعافي المدرسة الثانوية الصناعية من الأزمات التي قد تتعرض لها، وما أكثر تلك الأزمات؛ نظرًا لطبيعة المدرسة الثانوية الصناعية المحفوفة بالمخاطر، والذي يرجع إلى مجالات عملها المختلفة، المرتبطة باحتياجات السوق، وإرضاء العملاء، والحفاظ على أمن

الطلاب، والحفاظ على الأمن المعلوماتي لقواعد البيانات في المدرسة، وغيرها من المجالات الأخرى.

ثانيًا ـ إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تتحدد عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية، فيما يلي:

1. التخطيط للأمن المعلوماتي في المدرسة الثانوية الصناعية:

تنبع أهمية عملية التخطيط من كونها العملية الأولى التي تبنى عليها باقي عمليات الإدارة بشكل عام، وباقي عمليات إدارة الأمن المعلوماتي على وجه الخصوص، ويبدأ التخطيط للأمن المعلوماتي برفع وعي العاملين بأهمية هذا الأمر، ومن ثم يتم القيام بما يلي لرفع الوعي بالدرجة المطلوبة: (38)

- الوقوف على الوضع الراهن لاستخدام الكمبيوتر ووسائل التكنولوجيا الأخرى بالمنظمة.
- فهم ما الذي يريد أن يتدرب عليه الموظفون بالفعل.
- قياس مدى استجابة العاملين لما تم تقديمه في برامج التدريب الموجهة لزيادة وعيهم بالأمن المعلوماتي.
- فحص السبل المختلفة التي ستلاقي استحسانًا لدى جمهور العاملين للحصول على التهيئة المناسبة للاقتناع بضرورة الحفاظ على الأمن المعلوماتي.
- التوصل إلى مزيد من الداعمين والحلفاء الذين من شأنهم المساهمة في تحقيق هذا الهدف، ورفع وعي العاملين بأهمية الأمن المعلوماتي، وكيفية الحفاظ عليه.

مما سبق، يتضح أن التهيئة هي أولى خطوات التخطيط للحفاظ على الأمن المعلوماتي، وبالنسبة للمدرسة الثانوية الصناعية، فإن تهيئة الموظفين والإداريين المسئولين عن التعامل مع المعلومات والحفاظ عليها، يعد من أسس الاهتمام بالحفاظ على تلك المعلومات وسريتها، والتمكن من استعادتها وقت الحاجة، سواء كان هذا الوقت عاديًا، أو وقتًا حرجًا كوقت حدوث الأزمات والكوارث، كما أن زيادة وعي مدير المدرسة بهذا الأمر يجعله قادرًا على استخدام المعلومات المتاحة لديه لتعافي المدرسة من الآثار السلبية للأزمات التي تعرضت لها.

وتتحدد خطوات التخطيط للأمن المعلوماتي في: [39]

- تحديد الهدف: وفي هذه النقطة على الهدف أن يتسم بقدر من المرونة، مع التحديد الدقيق والوضوح والبساطة.
- تطبيق الخطة الموضوعة: وهنا على المسئولين القيام بتطبيق الخطة الموضوعة وفق الجدول الزمني المحدد، ووفقًا للمسئوليات المحددة سلفًا للأفراد القائمين بالتنفيذ.
- وضع معايير للحكم على مدى نجاح الخطة التي تم تنفيذها.

كما تم التأكيد في عملية التخطيط للأمن المعلوماتي قبل البدء في التنفيذ على ما يلي: [40]

- **تحديد السلطة:** بمعني تحديد الأفراد القادرين على اتخاذ القرارات التي تخص الحفاظ على الأمن المعلوماتي، وسبل الحفاظ على المعلومات أيضًا.
- **المحاسبية:** بما يسهم في الحفاظ على تنفيذ الخطط الإستراتيجية للأمن المعلوماتي في ضوء أهدافها، وبالتالي تحقيق الأهداف المرجوة.
- **الإمداد:** بمعني تحديد الأفراد المسئولين عن تقديم الإرشاد والتوجيه والدعم لجميع الأفراد ذوي المسئوليات للحفاظ على الأمن المعلوماتي.
- التأكيد على ضرورة استمرار الدعم المقدم في الوقت الحالي للمنظمة والعاملين فيها لتحقيق الأمن المعلوماتي.
- توفير قدر من المهارة في التعامل مع المخاطر والأزمات التي قد تواجه المنظمات، كلما أمكن ذلك، لما يتطلبه الأمر من برامج تدريب، وأفراد مؤهلين... إلخ.

وفي عملية التخطيط، يجب وضع عدة خطط لضمان استمرارية العمل في حالة حدوث ما يهدد الأمن المعلوماتي بالمنظمة، الأمر الذي يوضح ضرورة توقع ما يمكن أن يحدث في حالة ما تم اختراق نظام المعلومات بالمنظمة، على أن تكون تلك الخطط قائمة على أسس ومبادئ إدارة المخاطر، الأمر الذي من شأنه تيسير توقع التهديدات التي قد تصيب المعلومات الموجودة بالمنظمة، كما يجب أن تتسق الخطط الموضوعة لاستمرارية الأعمال مع طبيعة عمل المنظمة، ثم يجب بعد ذلك اختبار الخطط الموضوعة لضمان نجاح تلك الخطط، والتأكد من صلاحيتها، واستعدادها

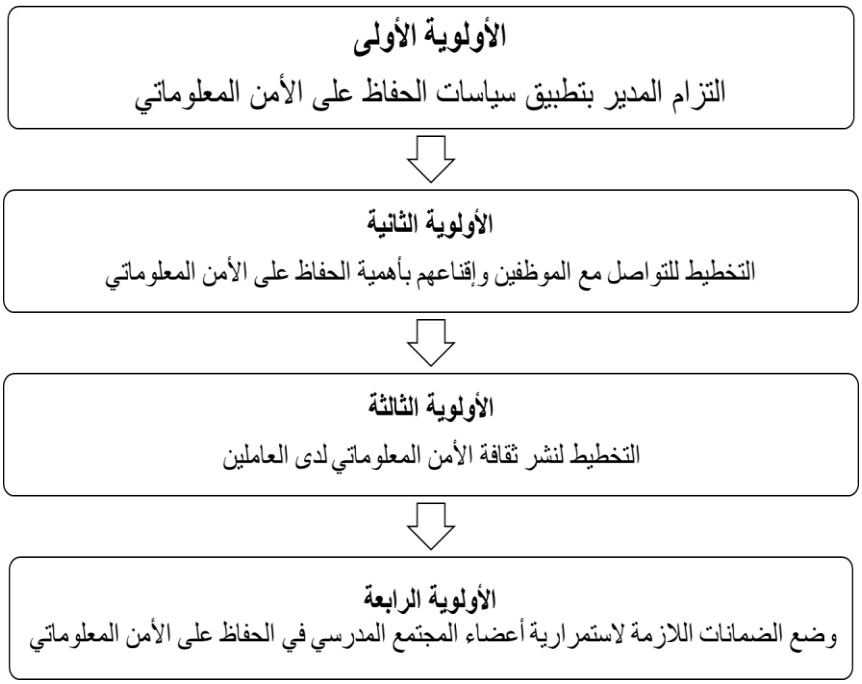
للتعامل مع المواقف الطارئة، وذلك قبل حدوث الأزمة، وأخيرًا تصنيف المخاطر التي قد تقع فيها المنظمة من جراء فقدان معلوماتها، أو عدم إتاحة النظام المعلوماتي، وفقًا للوقت الذي لا تتاح فيه المعلومات للمستفيدين منها، وذلك وفقًا للتصنيف التالي: (41)

درجة الخطر	زمن فقدان القدرة على استخدام النظام	الوصف
عالية	ثلاثة أيام أو أكثر	لا يمكن استخدام النظام الخاص بالمنظمة والمعلومات المتاحة عليه لمدة ثلاثة أيام أو أكثر.
متوسطة	من 8 ساعات وحتى 24 ساعة	لا يمكن استخدام النظام من 8 ساعات إلى يوم كامل.
منخفضة	أقل من 8 ساعات	لا يمكن استخدام النظام كحد أقصى لمدة 8 ساعات.

مما سبق، يتضح أن عملية التخطيط للأمن المعلوماتي تشتمل على الاهتمام بتوقع حدوث الأزمات الخاصة باختراق نظام المعلومات الخاصة بالمنظمة، وفي حالة المدرسة الثانوية الصناعية، تتضح أهمية تلك الخطوة، خاصةً وأن تلك البيئة مليئة بالمشكلات التي قد تتحول إلى أزمات قد تضر بالأمن المعلوماتي للمدرسة الثانوية الصناعية، وبالتالي يؤثر على أدائها وإنتاجيتها بالسلب، ومن ثم كان من اللازم بناء خطة لضمان استمرارية العمل أثناء حدوث مثل تلك الأزمات.

وتبدأ عملية التخطيط للأمن المعلوماتي من الإدارة العليا، ثم تتجه إلى باقي أعضاء المنظمة في شكل هيراركي رأسي، ومن ثم تمر تلك العملية بأربع مراحل أساسية، وهي: التزام الإدارة العليا بالمنظمة بتحقيق الأمن المعلوماتي، ثم التخطيط للتواصل مع أعضاء المنظمة لغرس مبادئ الأمن المعلوماتي لديهم، ونشر ثقافة الحفاظ على أمن المعلومات لديهم، والتخطيط لتعليم أعضاء المنظمة كيفية الحفاظ على أمن المعلومات، ثم التخطيط لضمان التزام العاملين بالمنظمة للحفاظ على الأمن المعلوماتي. (42)

بناء على ما سبق، يتضح أن عملية التخطيط للأمن المعلوماتي في المدرسة الثانوية الصناعية يجب أن تبدأ من قمة الهرم الإداري في المدرسة، ممثلة في مدير المدرسة، وتبدأ بالتزام المدير بتطبيق آليات لإدارة عمليات الأمن المعلوماتي؛ ثم ينقل بعد ذلك هذا الالتزام والاقتناع إلى جميع العاملين، من معلمين وهيكل إداري، أي أعضاء المجتمع المدرسي كافة، عن طريق التواصل معهم، ثم التخطيط لنشر ثقافة الأمن المعلوماتي لديهم، وأخيرًا وضع الضمانات اللازمة للحفاظ على استمرارية حفاظهم على الأمن المعلوماتي في المدرسة، ويمكن تمثيل تلك الأولويات على الشكل التالي: (43)



شكل رقم (2) أولويات مرتبطة بمهام المدير فيما يتعلق بالتخطيط للأمن المعلوماتي في المدرسة الثانوية الصناعية

ويتم تعزيز تلك الأولويات بعدد من المتطلبات التي تساعد في الانتقال السلس بين الأولويات السالفة، وهي: (44)

- الوعي الملائم من قبل الموظفين بأهمية نظم المعلومات وكيفية الحفاظ عليها.
- تعزيز سياسات الحفاظ على الأمن المعلوماتي، وتحديد معايير لتحقيق ذلك.
- تحديد مكان داخل التنظيم الهرمي الموجود بالمنظمة للوظيفة أو الوحدة التي سيتم من خلالها الحفاظ على الأمن المعلوماتي.

- تحديد مصادر تمويل واضحة للحفاظ على الأمن المعلوماتي في المدرسة، وتوضيح ذلك في خطة عمل محددة وواضحة.
- تحديد أهداف قصيرة المدى، وأخرى بعيدة المدى للتغلب على نقاط الضعف من ناحية، ومن ناحية أخرى الحفاظ على الأمن المعلوماتي بالمنظمات.
- السعي وراء الممارسات الأفضل في الحفاظ على الأمن المعلوماتي بالمنظمات، وذلك لتبادل الخبرات والاستفادة من الآخر.

ويتضح مما سبق، أن التخطيط للأمن المعلوماتي في المدرسة الثانوية الصناعية يتطلب تحديدًا دقيقًا للهدف المراد تحقيقه، الذي يتمثل في هذا السياق في الحفاظ على المعلومات الهامة الموجودة في المدرسة، مثل قواعد البيانات المتوفرة عن الطلاب، والمعلمين، والموظفين، والأجهزة، والورش، والمنتجات التي تستطيع المدرسة إنتاجها، بالإضافة إلى الميزانية، وجهات التعاون والمشاركة بين المدرسة الثانوية الصناعية، والشركات والمصانع التي تعقد الشراكات معها، وغيرها من المعلومات التي من شأنها مساعدة المدرسة على التعافي من أزماتها إذا ما حدثت أي مشكلات للمدرسة، خاصة وأنها بيئة مليئة بالمخاطر، التي يجب أن تستعد لها.

ووفقًا لما سبق، تضع السلطات اليابانية إستراتيجية عامة للأمن المعلوماتي بمؤسساتها كافة، ومنها المؤسسات التعليمية، والمدارس الثانوية الفنية بها، وتتضمن تلك الإستراتيجية خطة للأمن المعلوماتي، وذلك وفقًا للخطوات التالية: (45)

- تحديد الهدف من وراء وضع الخطة اللازمة لإدارة الأمن المعلوماتي.
- دراسة الوضع الحالي للمنظمة لمعرفة احتياجاتها ونقاط الضعف فيها.
- وضع الخطة اللازمة لإدارة الأمن المعلوماتي.
- تطبيق الخطة الموضوعة والاستعداد لتعديلها إذا اقتضت الضرورة.
- وضع معايير للحكم على الخطة الموضوعة وتعديلها في المستقبل لتعديل الخطط الجديدة.
- تعديل الخطط المستقبلية وفق المعايير الموضوعة استعدادًا للمستقبل.

يتضح مما سبق، أن السلطات اليابانية تتبع خطوات محددة لوضع خطة للأمن المعلوماتي لديها، تطبق بكافة مؤسسات الدولة لديها، ومنها المدارس العامة والفنية، وذلك لاقتناعها التام بأهمية الحفاظ على المعلومات المتاحة لدى كل منظمة

وفق طبيعتها، خاصة أن التعليم الفني بها يمثل حجر الزاوية في بناء الاقتصاد الياباني.

وعليه يتضح أن التخطيط هو أول العمليات الإدارية اللازمة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية، فهو بمثابة التهيئة الفعلية ورسم الخطوط المستقبلية التي ستسير عليها المدرسة من أجل تحقيق غايتها في الحفاظ على المعلومات التي تمتلكها، واستخدامها وقت الحاجة، خاصةً وقت حدوث الأزمات، أو بعد الانتهاء منها، استعدادًا لاستعادة النشاط مرة أخرى.

2. الاتصال لتحقيق الأمن المعلوماتي في المدارس الثانوية الصناعية:

تعتبر عملية الاتصال Communication إحدى العمليات الهامة بالمنظمات التعليمية على وجه الخصوص، لا سيما في قدرة تلك المنظمات على الحفاظ على أمنها المعلوماتي، وخاصةً عند الاستعداد للمواقف الطارئة التي قد تواجه المدارس الثانوية الصناعية على اعتبار أنها إحدى البيئات التي تتعرض للمخاطر والأزمات باستمرار، إذ يستطيع المدير تحديد الجهات المعنية بالاتصال التي ممكن أن تساعده، كشركات صيانة أجهزة الكمبيوتر، وشركات البرامج الأصلية، والمتخصصين القادرين على تدريب الإداريين على إقامة قواعد البيانات وتشفيرها للاستعانة بها وقت الحاجة، وغيرها من الجهات الأخرى المعنية بمثل تلك الأمور، كما أنها العملية التي تضمن دخول المستفيدين على موقع المدرسة والحصول على المعلومات المتاح لهم الدخول عليها، والتي يحتاجون إليها، وذلك في كافة الأوقات دون التفرقة بين الأوقات العادية ووقت الأزمات.

كما تتضمن عملية الاتصال، قدرة المدرسة الثانوية الصناعية على الاتصال بمنظمات رجال الأعمال، والشركات، والمصانع، التي من شأنها تدعيم بيئة المدرسة، وتقديم خدمات مختلفة لها كخدمات التدريب والتوظيف، وغيرها من الخدمات، الأمر الذي يتطلب قواعد بيانات واسعة النطاق، ودقيقة، ومحدثة؛ لاستخدامها وقت حدوث الأزمات، أو حتى في الأوقات العادية.

وهناك عدة خطوات يجب الاهتمام بها عند الاتصال بالجهات المعنية للحفاظ على الأمن المعلوماتي بالمنظمات، ومن تلك العناصر ما يلي: [46]

- الحفاظ على القدرة على الاتصال عبر الشبكات التي تمتلكها المنظمة Network Security، بمعنى أن يكون للمنظمة القدرة على الاتصال بشبكات الإنترنت، للاتصال بالممولين من المجتمع الخارجي، أو بالشركات التي لها اتصال مع المنظمة.
- مراجعة عناصر الأمان المتوفرة بالمنظمة للحفاظ على أمنها المعلوماتي باستمرار، وذلك لتحديثها، وتطبيق أفضلها للمنظمة.
- مراقبة انتقال المعلومات التي تخص المنظمة، من خلال قنوات الاتصال الشرعية المتاحة بالمنظمة، مثل موقعها الرسمي، الذي يكون لكل مستفيد فيه كلمة مرور، يستطيع من خلالها الحصول على ما يشاء من المعلومات.
- تخزين المعلومات، وفيها يتم تحديد درجة أهمية المعلومة وحساسيتها، والمعلومات الأكثر حساسية يتم تخزينها بشكل لا يسمح للعامة بالاطلاع عليها، أما المعلومات العادية فيمكن لجميع المعنيين والمستفيدين الاطلاع عليها والاستفادة منها.
- درجة التشفير Encryption، يرتبط ذلك العنصر بما سبقه، إذ ترتفع درجة تشفير المعلومات لتصبح غير متاحة للجميع في حالة ارتفاع درجة حساسيتها؛ فمثلًا معلومات وبيانات العاملين وتقارير أدائهم لا يجب أن يعلمها الجميع، وغيرها من المعلومات التي لها ذات الطابع.
- الحفاظ على بيانات ومعلومات المنظمة من الفيروسات باستخدام البرامج الأصلية والحديثة.
- الاحتفاظ ببيانات ومعلومات المنظمة الهامة وذات الحساسية العالية في أماكن أخرى غير أجهزة الكمبيوتر؛ كالأقراص المدمجة، والأقراص الصلبة الخارجية؛ لحمايتها من أعمال القرصنة الإلكترونية.
- ضمان استمرارية عمل المنظمة أثناء الأزمات Business Continuity، من خلال استمرارية الاتصال مع العملاء وطمأنتهم عن جودة الخدمة والمنتجات، واستمرارية حصولهم على الامتيازات التي كانوا يحصلون عليها قبل حدوث الأزمة، ولكن بشرط إعلامهم بالمخاطر التي حدثت بالمنظمة، وبالإجراءات

المتبعة لاستعادة النشاط والتعافي من الأزمة، وذلك لتحقيق الإدارة الشفافة ومصارحة العملاء بما يحدث داخل المنظمة دون تعتيم على الحقائق.

وبالنظر لخطوات الاتصال السالفة، يتضح أنها ضرورية للحفاظ على أمن المعلومات في المدرسة، سواء كانت بيانات ومعلومات عن الميزانية، وأعضاء هيئة التدريس، وتقارير الأداء الخاصة بهم، والممولين الخارجيين، وجماعات الشراكة الخارجية، والشركات والمصانع المتضامنة مع المدارس، وتفاصيل الاتفاقيات المبرمة بينهم، وغيرها من المعلومات التي يجب الحفاظ عليها من الضياع أو القرصنة، وعليه يجب مراعاة توافر العناصر السالفة كافة عند التعامل مع البيانات والمعلومات الخاصة في المدرسة الثانوية الصناعية؛ لضمان قدرتها على تقديم الخدمات المتنوعة التي تقدمها للمستفيدين منها.

وتعتبر قواعد البيانات المتوفرة عن الهيئات والجهات والشركات اللازم الاتصال بها وقت حدوث الأزمات أو بعد حدوثها، من أهم السبل التي تساعد المدرسة الثانوية الصناعية على تعافيها من تلك الأزمات واستعادة نشاطها مرة أخرى، ولعل تنوع وتعدد وسائل الاتصال المستخدمة في المدرسة الثانوية الصناعية وقت الأزمات أو بعدها تمهيدًا لاستعادة النشاط من أهم الأساليب التي تسهم في سرعة استعادة هذا النشاط، فهناك أجهزة الهاتف، وهناك الإنتركوم، الذي يجعل أجزاء المدرسة مرتبطة ببعضها البعض، وهناك أجهزة الكمبيوتر، والبريد الإلكتروني، وأجهزة الفاكس، ويعد هذا التنوع أو التعدد من أشكال الأمن التي يجب على المدرسة توفيرها لذاتها؛ بحيث إذا حدث عطل في إحداها، أصبح الآخر متاحًا، الأمر الذي يسهم في عدم انقطاع المدرسة وانعزالها عن العالم الخارجي في وقت الأزمات، مما يمكنها من الاستعانة بمن يعينونها على تجاوز الأزمة التي تمر بها من المتخصصين. (47)

كما يجب على المدرسة أن تضع لنفسها ما يسمى بشجرة الاتصالات Communication Tree، وترتيبها وفقًا لأهمية وأولوية الجهة التي ستقوم المدرسة بالتواصل معها وقت حدوث الأزمة. (48)

بالإضافة إلى ما سبق، لا يمكن للمدرسة الثانوية الصناعية استخدام وسائل الاتصال السالفة، أو إنشاء شجرة الاتصالات، إلا إذا كانت تمتلك قاعدة بيانات جاهزة للاستخدام وقت حدوث الأزمة، على ألّا يصيب تلك القاعدة أي شكل من

أشكال الضرر نتيجة للأزمة التي تتعرض لها المدرسة، ومن ثم تتضح أهمية الحفاظ على أمن المعلومات في المدرسة الثانوية الصناعية، إذ إنها السبيل للتخلص من تلك الأزمات، عن طريق الاستعانة بعدد من الخبراء والمختصين من المجتمع الخارجي للمساهمة في التخلص من الآثار السلبية للأزمات، بل وتهديد قدرة المدرسة على تقديم خدماتها التعليمية للطلاب.

كما على المدرسة تعيين متحدث رسمي عنها وقت حدوث الأزمة، وهو الشخص الذي تتوافر لديه المعلومات المصرح للآخرين الحصول عليها أثناء الأوقات الحرجة، كما يتاح له الاتصال بجهات الاتصال الأخرى التي بوسعها المساعدة، ومن ثم تكون من سلطاته تقديم صورة كاملة لتلك الجهات عن الوضع الراهن للمدرسة، وذلك بناء على معلومات صحيحة وواضحة يشتقها من قواعد البيانات الموجودة في المدرسة لاستخدامها في هذه الأوقات، وذلك ليكون لديهم القدرة على تحديد الاحتياجات والمساعدات التي يستطيعون تقديمها للمدرسة. (49)

ومما هو جدير بالذكر أن المدارس الفنية ـ بشكل عام ـ بولاية ماساتشوستس الأمريكية، تقدم نموذجًا حيًّا للاتصال بغيرها من جهات الاتصال؛ حيث تحدد جهات الاتصال التي من الممكن الاستفادة منها، وتحتفظ لذاتها بقاعدة بيانات كاملة عن تلك الجهات وكيفية الاتصال بها، ومن تلك الجهات المدارس الفنية الصناعية التي تقع في منطقة واحدة، والمعاهد الفنية الصناعية العليا، ووسائل الإعلام؛ كالجرائد والمجلات وهيئات الإذاعة والتليفزيون بالولاية، وبعض الشركات والمصانع المحيطة بالمدرسة، وبعض شركات الكمبيوتر. (50)

وبناء على ما سبق، يمكن القول إن هناك تعددية في جهات الاتصال بين المدارس الثانوية الصناعية، فهناك الشركات المسئولة عن ترويج منتجات تلك المدارس، وهناك شركات الكمبيوتر المسئولة عن إمداد المدرسة بالبرامج الأصلية التي تحتاجها الأجهزة للحفاظ على الأمن المعلوماتي، كما أنها مسئولة عن الصيانة وقت حدوث الأزمات، وهناك أيضًا المدارس المحيطة، التي يمكن إمداد بعضها البعض بالخبرات التي مرت بها أثناء حدوث الأزمات، كما أن هناك المعاهد العليا، التي يمكن أن تقدم برامج تدريب مختلفة لكل من العاملين، والمعلمين، والطلاب في مختلف الأمور المرتبطة بعملهم، الأمر الذي يتضح من خلاله أن المدرسة الثانوية

الصناعية في حاجة ماسة لقاعدة بيانات عريضة عن أهم الجهات التي يمكنها الاستفادة منها في وقت الأزمات أو في الأوقات العادية، ولعلها بيانات ومعلومات يجب أن تكون محفوظة بشكل سري، في يد المختصين والمعنيين فقط، لاستخدامها عندما تحتاج المدرسة إليها.

3. تدريب العاملين على إدارة الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تحتل عملية التدريب مكانة هامة ضمن عمليات إدارة الأمن المعلوماتي، وذلك لما لها من دور في رفع كفاءة المختصين في التعامل مع أنظمة الأمن المعلوماتي، والحفاظ على بيانات ومعلومات المدرسة من الضياع أو السرقة، الأمر الذي يتطلب تدريبًا مستمرًّا لتبقى تلك الفئة على ذات درجة الكفاءة المطلوبة في التعامل مع المعلومات، واستعادتها وقت الحاجة إليها، بل والوقوف على أحدث ما يمكن التوصل إليه في مجال الأمن المعلوماتي، وتطبيقه في المدرسة.

ويمكن حدوث ذلك من خلال عدة آليات، لعل من أهمها ما يلي: (51)

- الاهتمام بتعليم مستخدمي النظام أهم فنياته، والتدريب على الاستخدام الفعال لذلك النظام.
- تحليل سلوكيات المستخدمين لمعرفة مدى استجابتهم للتغير الذي يطرأ على الأجهزة الإلكترونية وأنظمة الأمن المعلوماتي لديهم.
- تحديد السياسات التنظيمية والتشريعية التي تحكم ممارسات الحفاظ على الأمن المعلوماتي للمنظمة.
- تحديد أهم التهديدات التي تواجه الحفاظ على الأمن المعلوماتي بالمنظمات.
- تطوير الأدوات التي تحافظ على الأمن المعلوماتي بالمنظمات وفقًا لآخر التطورات التي تحدث بأنظمة المعلومات بالعالم المحيط.

كما تقدم عدة مؤسسات دولية عددًا من البرامج لتنمية قدرات المتخصصين للحفاظ على الأمن المعلوماتي، ومن تلك المؤسسات، مؤسسة أنظمة الأمن المعلوماتي Information System Security Association(ISSA)، وهي مؤسسة غير ربحية، يتمثل هدفها الأساسي في إعداد وتدريب كل من يناط به الحفاظ على الأمن المعلوماتي، وذلك عن طريق عقد العديد من المؤتمرات، والمقابلات، وإعداد الكتيبات والمنشورات عن كيفية الحفاظ على الأمن المعلوماتي بالمنظمات. (52)

وهناك أيضًا مؤسسة الرقابة والمراجعة على أنظمة المعلومات The Information Systems Audit and Control Association (ISACA)، وهي مؤسسة غير ربحية أيضًا، مهمتها الأساسية الرقابة والمراجعة على أنظمة المعلومات بالمنظمات، تضم أعضاء متخصصين في المجالات التكنولوجية والإدارية، يقومون بدورهم بممارسات عن التمكن من تكنولوجيا المعلومات Information Technology (IT)، وتقدم عددًا من برامج التدريب للممارسين داخل المنظمات للحفاظ على الأمن المعلوماتي في ضوء ما توصلت إليه من تقارير في أثناء المراجعة والتقييم، كما تقوم بنشر الأخلاقيات المرتبطة بالحفاظ على الأمن المعلوماتي بالمنظمات، الأمر الذي يساعد الممارسين على أداء مهمتهم الخاصة بالحفاظ على الأمن المعلوماتي بمنظماتهم التي يعملون بها. (53)

كما يعتبر معهد إدارة النظام، والأمن، والشبكات The System Administration, Networking, and Security Institute (SANS)، مؤسسة بحثية متخصصة، بعضوية عدد من المتخصصين في مجال الحفاظ على الأمن المعلوماتي، ويقدم بدوره عددًا من الشهادات العلمية للمتقدمين إليه، مثل شهادة ضمان المعلومات الدولية Global Information Assurance Certification، التي تهتم بضرورة تطبيق ما تم دراسته خلال فترة الدراسة بالمعهد على أرض الواقع، والالتزام بالكود الأخلاقي الخاص بالحفاظ على الأمن المعلوماتي، وإلا تعرض الحاصل على الشهادة للعقاب نظرًا لعدم ممارسته لما قام بدراسته فعليًّا. (54)

ويركز العمل بتلك المعاهد والمؤسسات على فكرة مؤداها التغير الدائم في الوظائف اللازمة للحفاظ على نظام الأمن المعلوماتي بالمنظمة، ومن تلك الوظائف التي يجب الانتباه لها وتدريب الموظفين عليها تصميم البرامج التي تحتاج المنظمة إليها، وتحديد المتطلبات وفقًا لطبيعة عمل المنظمة، وإنشاء نظام متكامل لتشفير المعلومات الموجودة بالمنظمة للحفاظ عليها، وتنزيل البرامج الجديدة والأصلية، والاحتفاظ بالمعلومات لحين الحاجة إليها دون أن يخترقها أحد الدخلاء وبدون إذن من المسئولين عن النظام. (55)

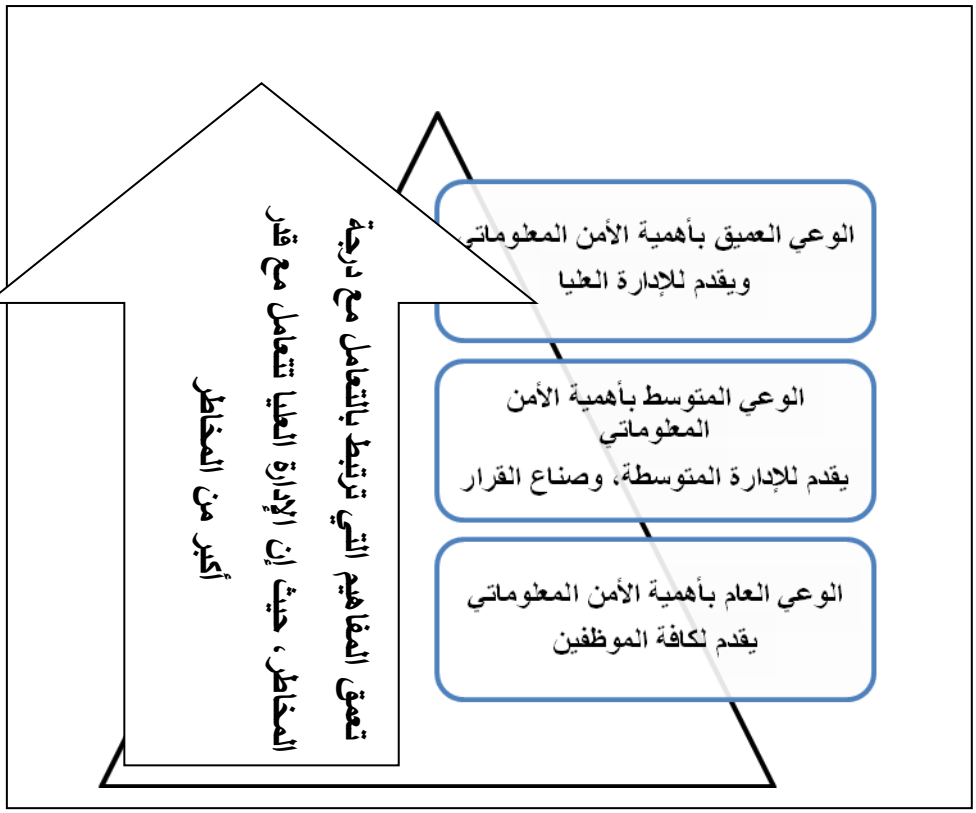
وبناء على ما سبق، يتضح أن برامج التدريب، تركز على التحديث والتجديد المستمر في الوظائف، ذلك أن طبيعة المنظمات الاستجابة للمتغيرات التي تحدث

بالمجتمع الخارجي، وإذا كانت التكنولوجيا الحديثة هي أكثر المتغيرات بروزًا في الآونة الأخيرة، فإن التدريب على التمكن من مهارات التعامل معها، والتمكن منها أصبح متطلبًا هامًّا من متطلبات برامج التدريب، إذ يتطلب هذا التمكن القدرة على تصنيف المعلومات، وتشفير الأكثر حساسية منها، والتأكد من دقتها، وتحديثها باستمرار.

كما تختلف مستويات التدريب الخاصة برفع وعي الموظفين عن الأمن المعلوماتي، وفقًا لمستوى عمق المفاهيم المقدمة بتلك البرامج، وذلك وفقًا أيضًا للمهام المطلوبة من كل فئة من فئات الموظفين، ويمكن تحديد ذلك، من خلال النظر للشكل التالي:

(56)

شكل رقم (3) درجة عمق التدريب الذي يركز على أهمية الأمن المعلوماتي بالمنظمة



مما سبق، يتضح أن هناك ثلاثة مستويات يجب أن تركز عليها برامج التدريب المقدمة إلى المسئولين التربويين في المدارس الثانوية الصناعية؛ حيث يجب أن تركز

البرامج المقدمة إلى جميع الإداريين والموظفين المسئولين عن الحفاظ على الأمن المعلوماتي على المعرفة العامة بأهمية الأمن المعلوماتي وكيفية الحفاظ عليه، الأمر الذي يمكنهم من القيام بمهامهم الوظيفية، أما المستوى الثاني فيركز على موضوعات ومفاهيم أكثر عمقًا، وتوجه إلى الإدارة المتوسطة المسئولة عن صنع القرار، مثل مدير المدرسة والوكلاء، وأخيرًا البرامج المقدمة إلى الإدارة العليا، الخاصة بالوزارة، التي يجب أن تركز على موضوعات ومفاهيم أكثر عمقًا، الأمر الذي يمكنها من اتخاذ القرارات العليا، بناء على المعلومات الموجودة في المدارس والإدارات والمديريات.

كما على برامج التدريب أن تهتم بتقديم مبادئ الأمن المعلوماتي للعاملين بالمنظمة، وذلك لمعرفة نوعية المعلومات التي عليهم الحفاظ عليها، وتلك التي يجب نشرها للفئات المستفيدة من عمل المنظمات، وتلك المبادئ هي: [57]

- **التكامل Integrity**: وهو المبدأ الذي يعني قدرة العاملين على إحداث الربط والتكامل بين المعلومات التي تمتلكها المنظمة، والتي عن طريقها يمكن إمداد المستفيدين بمعلومات كاملة ذات دلالة ومعنى.
- **درجة حساسية المعلومات Confidentiality**: وتعني قدرة العاملين على معرفة المعلومات التي لا يجب أن تعلن للمستفيدين، لأنها تعتبر أسرار لها، تخص سياستها الداخلية التي لا يجب على أي فرد الاطلاع عليها.
- **الإتاحة Availability**: وتعني قدرة العاملين على معرفة المعلومات التي يجب إتاحتها للمستفيدين عن المنظمة، ومن ثم الاستفادة منها.

ويلاحظ مما سبق، أن هناك ضرورة ملحة لتدريب العاملين بوجه عام، والإداريين في المدارس الثانوية الصناعية بشكل خاص، على تلك المبادئ؛ للتفرقة بين نوعية المعلومات التي يجب الحفاظ عليها، والمعلومات التي عليهم نشرها من أجل الصالح العام للمدرسة، مثل: الإعلان عن منتجاتها، وجذب ممولين لها، والتسويق لخدماتها، بل وإحداث التكامل بين المعلومات لخلق فرص التسويق لخدمات المدرسة الثانوية الصناعية، وفي ذات الوقت الحفاظ على المعلومات التي لا يمكن التصريح بها، لأنها تخص ميزانية المدرسة مثلًا، إذ إن مثل هذه المعلومات لا يمكن التصريح بها.

وتهدف برامج التدريب للحفاظ على الأمن المعلوماتي إلى تحقيق عدد من الأهداف، لعل من أهمها ما يلي: (58)

- الفهم التام والتأقلم مع إجراءات وسياسات الحفاظ على الأمن المعلوماتي بالمنظمة.
- التمكن من القواعد التي يجب اتباعها عند حدوث أي اختراق للأمن المعلوماتي بالمنظمة.
- التعاون مع إدارة المنظمة للحفاظ على أمنها المعلوماتي ومقابلة الاحتياجات التدريبية للموظفين الذين يعملون بها.
- ضمان التحديث المستمر للبرامج المستخدمة على أجهزة الكمبيوتر.
- الوعي بأفضل الطرق التي يمكن اتباعها للحفاظ على الأمن المعلوماتي بالمنظمة التي يعملون بها.

كما لا يمكن أن نغفل دور برامج التدريب في تنمية المهارات اللازمة للتعامل مع الحواسيب، والبرامج المضادة للفيروسات، وبناء قواعد البيانات، وتشفير المعلومات، وغيرها من السياسات التي من شأنها الحفاظ على الأمن المعلوماتي بالمنظمة. (59)

بناء على ما سبق، يتضح أنه لا يمكن إغفال تمكين العاملين في مجال الإدارة في المدرسة الثانوية الصناعية ـ على مختلف مستوياتهم ـ من مهارات التعامل مع أجهزة الحاسب الآلي، واستخدام البرامج المختلفة التي من شأنها مساعدتهم على الحفاظ على أمن المعلومات الخاص بالمدرسة، إذ إن ضعف التمكن من تلك المهارات، يعوق تحقيق الغاية القصوى من وراء التمكن منها، ألا وهي الحفاظ على الأمن المعلوماتي المرغوب، وبالتالي مساعدة المدرسة الثانوية الصناعية على تعافيها من الأزمات واستعادة نشاطها سريعًا بما يحقق رضا المستفيدين.

وتطبيقًا على ما سبق، يقدم اتحاد المدارس الفنية الأوروبية European Technical School Union مجموعة من البرامج التدريبية لمختلف الفئات المتوقع تعاملها مع المعلومات وأجهزة الكمبيوتر في المدارس الصناعية بمختلف أنحاء القارة الأوروبية، بدءًا من مدير المدرسة، وحتى المعلمين، والعاملين والإداريين في مختلف التخصصات، ومن أهم البرامج التدريبية الموجهة لتلك الفئات: فهم

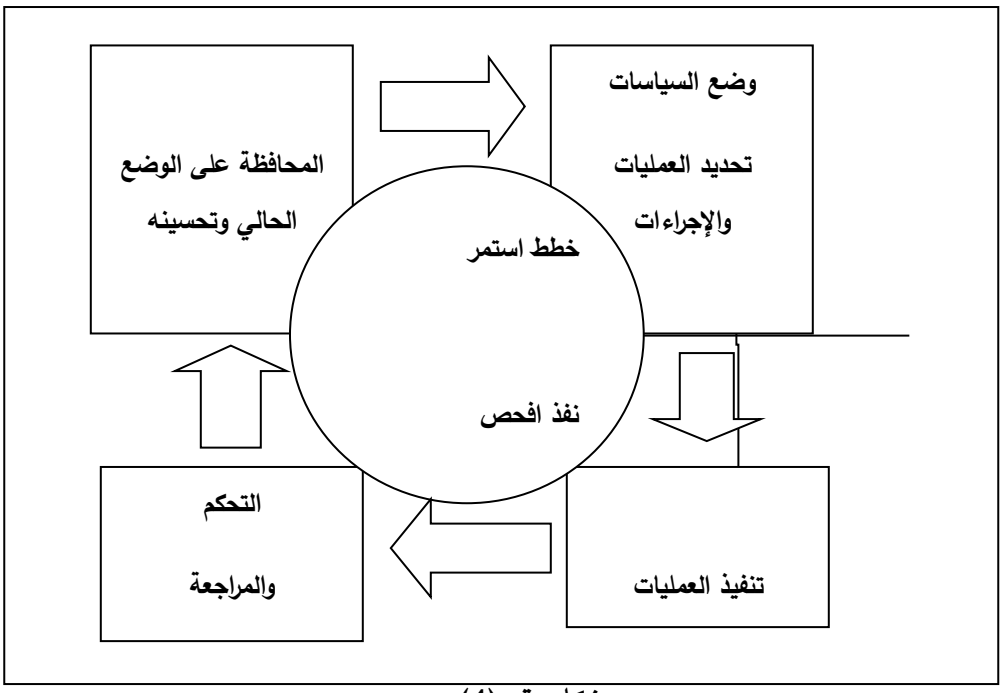
السياق الإستراتيجي لإدارة عمليات الأمن المعلوماتي، وترجمة إستراتيجية الأمن المعلوماتي للواقع الإجرائي، والحفاظ فعليًا على الأمن المعلوماتي للمدرسة، وبعد الانتهاء من تلك البرامج التدريبية يتوقع من المشاركين بتلك البرامج أن يتمكنوا من المهارات التالية: (60)

- إدارة الأمن المعلوماتي وتطوير قدرة المتدرب على إدارة الأزمات والمخاطر، وامتلاك السياسات الملائمة لاحتياجات المدرسة.
- إنشاء نظام للأمن المعلوماتي، وعمليات إدارة المخاطر.
- الوعي بأهمية الحفاظ على الأمن المعلوماتي، وتحديد المقاييس اللازمة للحكم على مستوى الأمن المعلوماتي في المدرسة.
- تقييم المخاطر، ورسم خطط سياسات الحفاظ على الأمن المعلوماتي للمدرسة.
- التنسيق بين فرق العمل المختلفة وتوزيع مهام العمل؛ حيث إن لكل فرد مهمة في الحفاظ على الأمن المعلوماتي للمدرسة.

4. تقويم الأمن المعلوماتي في المدرسة الثانوية الصناعية:

تحتاج المنظمات بشكل عام، والمدارس الثانوية الصناعية على وجه الخصوص لنظام تقويم يؤكد قدرة المدرسة على الحفاظ على أمنها المعلوماتي، ويتم ذلك عن طريق عدة طرق؛ كالاستبيانات، والمقابلات، وملاحظة التقارير الرسمية، وغيرها من الأساليب الأخرى. (61)

ويعتبر نظام ISO27001، أهم الأنظمة المتبعة بالمنظمات للتأكد من قدرة المنظمة على الحفاظ على أمنها المعلوماتي، وهو نظام تم إنشاؤه عام 2005، بهدف إنشاء نظام للأمن المعلوماتي بالمنظمة وتطبيقه وتشغيله ومراجعته والحفاظ على إدارته، كما يشتمل هذا النظام على وضع التحسينات اللازمة لتطوير هذا النظام داخل المنظمات بناء على تقويم الأنظمة الحالية، ويسمى هذا النظام بنموذج PDCA Model حيث يشير الـ P إلى Policies، Processes، Procedures، وتشير الـ D إلى Do، وتشير الـ C إلى Check، وأخيرًا تشير الـ A إلى Act، وذلك كما هو مبين بالشكل التالي: (62)



شكل رقم (4)

تقويم الأمن المعلوماتي وفقًا لنموذج PDCA

يعتبر هذا النموذج أحد نماذج تقويم قدرة المنظمة على الحفاظ على أمنها المعلوماتي، وتحسين الإجراءات التي تتبعها للحفاظ عليه في المستقبل، ولتستطيع المدرسة الثانوية الصناعية تقويم قدرتها على الحفاظ على أمنها المعلوماتي عليها أن تنظر في السياسات والعمليات والإجراءات التي تم تحديدها سلفًا، كما عليها النظر في الطريقة التي نفذت بها العمليات، الأمر الذي سيمكنها من المراجعة، والتقويم، ثم التحسين، وتبني مزيد من الإجراءات التي ستضمن مزيدًا من الحفاظ على الأمن المعلوماتي لها.

ويركز هذا النظام على ضرورة اتباع عدة خطوات لتحقيق عملية التقويم والتأكد من حفاظ المنظمة على أمنها المعلوماتي، وتلك الخطوات هي: [63]

- **الحصول على دعم الإدارة العليا Upper Management Support:**

تعني هذه الخطوة إيمان الإدارة العليا بالمنظمة، والتزامها بالحفاظ على الأمن المعلوماتي بالمنظمة، وحث العاملين على اتباع جميع السياسات للحفاظ على أمن المنظمة المعلوماتي، وتساعد تلك الخطوة في استمرار حماس المديرين والموظفين في

الحفاظ على الأمن المعلوماتي، فالأمن المعلوماتي عملية تبدأ من المدير، وتنتهي إليه؛ فهو الذي يمتلك أساسيات الحفاظ على الأمن المعلوماتي بالمنظمة التي يرأسها.

❖ **وضوح الحدود الفاصلة للأمن Define Security Perimeter:**

لعل من الأولويات الهامة لهذا النظام التقويمي وضع المحيط الذي يتم الحفاظ على الأمن فيه، أي الحدود الفاصلة التي يمكن للأمن المعلوماتي أن يعمل فيها، بمعنى تحديد نمط المنظمة، أو نوعها، وبالتالي تحديد نوعية المعلومات التي يتم الحفاظ عليها وعلى سريتها.

❖ **وضع سياسة للأمن المعلوماتي Create Information Security Policy:**

من الممكن أن تأخذ سياسات الأمن المعلوماتي أكثر من شكل، ويمكن أن توضع في شكل وثيقة واحدة، أو أكثر من وثيقة توجه لعدد من الأفراد، أو توضع في شكل عدد من المعايير التي يجب أن يلتزم بها الأفراد، كما أنها قد تشتمل على الأهداف التي من الممكن أن تتحقق من وراء الحفاظ على الأمن المعلوماتي بالمنظمة.

❖ **إنشاء نظام إدارة الأمن المعلوماتي Create Information Security Management System:**

يقوم هذا النظام التقويمي على النظر في إجراءات إنشاء نظام الأمن المعلوماتي بالمنظمة، بالإضافة إلى إجراءات التطبيق، والتعزيز أيضًا، الأمر الذي يساعد على تحسين الإستراتيجيات، ووضع الإجراءات الجديدة لوضع أنظمة إدارة الأمن المعلوماتي، وبناء الفرق، وتحديد مزيد من الإجراءات اللازمة للحفاظ على الأمن المعلوماتي.

❖ **إجراء تقييم للمخاطر على الأمن Perform Security Risk Assessment:**

في هذه الخطوة يتم توقع جميع المخاطر التي من الممكن أن تهدد الأمن المعلوماتي للمنظمة، وذلك للاستعداد لها، وتتضمن تلك الخطوة الخطوات الفرعية التالية:

- تحديد الأسس والأصول التي تتضمنها عملية الحفاظ على الأمن المعلوماتي، من حفاظ على البرامج، والأجهزة، والبيانات، والمعلومات، وغيرها من الأمور.
- تحديد التهديدات المتوقعة لهذه الأسس والأصول.
- تحديد نقاط الضعف المتوقعة بهذه الأسس والأصول، والتي تحول دون تحقيقها.
- تحديد احتمالية التفاعل بين التهديدات المتوقعة، ونقاط الضعف المتوقعة، والتي قد تحول دون تحقيق الأهداف أيضًا.
- حساب نسبة الضرر التي قد تصيب المنظمة من جراء عدم الحفاظ على الأمن المعلوماتي للمنظمة.
- حساب درجة الخطر التي قد تصيب المنظمة من جراء عدم الحفاظ على أمنها المعلوماتي.

❖ **تنفيذ الخطة واختيار أنماط الرقابة Implementing and Selecting Control:**

يتم في هذه الخطوة مراقبة إجراءات التطبيق التي تتم بالمنظمات للحفاظ على الأمن المعلوماتي بها، بالإضافة إلى اختيار أنماط الرقابة التي سيتم التأكيد على أساسها ما إذا كانت المنظمة تحافظ على أمنها المعلوماتي أم لا.

وتعتبر عملية الرقابة في تلك الخطوة جزء من عملية التقويم، إذ يتم النظر فيها إلى النتائج المحققة، بينما يقوم التقويم بإصدار الحكم النهائي على النتائج المحققة، وعمل برنامج تصحيحي لنقاط الضعف الموجودة، وتدعيم نقاط القوة التي يتسم بها الأداء.

وبناء على الخطوات السابقة، تستطيع المنظمة استرجاع المعلومات وقت الحاجة إليها، خاصةً وقت الأزمات والكوارث، وبالتالي تضمن استمرارية العمل وقت حدوث الأزمة من ناحية، ومن ناحية أخرى مساعدتها على التعافي من الأزمة، واسترجاع مكانتها بسرعة، الأمر الذي يساعدها على زيادة إنتاجيتها، وزيادة ثقة عملائها فيها.

كما يوجد نظام ISO 17799 وهو نموذج آخر لمراقبة قدرة المنظمات على الحفاظ على أمنها المعلوماتي، وقدرتها على استخدام تلك المعلومات في استعادة نشاطها بعد حدوث الأزمات، ويركز هذا النموذج على ضرورة توافر عدد من العناصر للحكم على قدرة المنظمات على الحفاظ على أمنها المعلوماتي، وتتمثل تلك العناصر فيما يلي: (64)

- وجود سياسات مختلفة للحفاظ على الأمن المعلوماتي بالمنظمة.
- توافر قدر من الأمن المؤسساتي للمنظمة، والذي يشير إلى قدرة المنظمة ـ من خلال إمكاناتها المختلفة ـ على الحفاظ على المعلومات الموجودة بها، وذلك عن طريق توفر عدد من الآليات للحفاظ على الأمن المعلوماتي بها، والتي كلما ازدادت وتنوعت دلّ ذلك على قدرة المنظمة على الحفاظ على الأمن المعلوماتي بها.
- الأمن البشري، الذي يشير إلى تأمين قدرة العامل البشري على استخدام جميع الأجهزة الخاصة بالحفاظ على الأمن المعلوماتي للمنظمة، وتدريبهم باستمرار للحفاظ على قدراتهم في هذا الصدد.
- قدرة المنظمة على التواصل مع غيرها من المنظمات الأخرى للمساهمة في التخلص من الأزمات التي قد تواجهها، بالإضافة إلى قدرتها على تبادل المعلومات مع تلك الجهات.
- قدرة المنظمة على مراقبة دخول الآخرين للمعلومات الخاصة بها، والحفاظ على المعلومات ذات الحساسية العالية، التي لا يمكن لأي فرد الدخول إليها، إلا المتخصصين من داخل الإدارة فقط.
- قدرة المنظمة على الاستمرار في تقديم خدماتها للمستفيدين أثناء حدوث الأزمات.
- قدرة المنظمة على تطوير نظامها باستمرار وابتكار أنظمة جديدة للحفاظ على أمنها المعلوماتي.

وبناء على ما سبق، يتضح أن هناك نماذج متعددة لتقويم إدارة الأمن المعلوماتي، تلك النماذج تهدف في مجملها إلى التأكد من قدرة المنظمات بشكل عام، والمدارس الثانوية الصناعية على وجه الخصوص ـ بوصفها أحد أنماط المنظمات ـ

على الحفاظ على أمنها المعلوماتي، بل وتطوير تلك القدرة باستمرار، وتحديثها، من أجل مساعدتها على استعادة نشاطها بعد حدوث الأزمة، وتعافيها من آثار الأزمة السلبية.

ووضعت ولاية أوهايو مجموعة من المعايير التي يمكن للمدارس الثانوية الفنية تقويم قدرتها للحفاظ على الأمن المعلوماتي لديها، ومن تلك المعايير ما يلي: (65)

- توافر بيانات ومعلومات لدى المدرسة عن جهات التسويق، وصيانة الأجهزة، واحتياجات سوق العمل، وأولياء الأمور، وجميع الجهات التي يمكن أن تفيد المدرسة.
- توافر قيادة واعية بالأدوار الأساسية اللازمة للحفاظ على الأمن المعلوماتي في المدرسة.
- توافر وسائل وقنوات اتصال بين المدرسة والجهات المعنية للاستفادة من تلك الجهات وقت الحاجة، كالاتصال بالشركات للتدريب وصيانة الأجهزة، والاتصال بأولياء الأمور لإبلاغهم عن الوضع الحالي للمدرسة، أو الجهات التي يمكن تسويق منتجات المدرسة عن طريقها أو إليها.
- توافر فريق مسئول عن الحفاظ على أمن المعلومات في المدرسة؛ بحيث يكون مدربًا على حفظ المعلومات واسترجاعها وقت الحاجة، بل والإعلان عن الوضع الراهن للمدرسة، خاصةً وقت الأزمات.
- توافر مجموعة من القواعد المعلنة التي يعلمها جميع العاملين في المدرسة عن العقوبات التي تفرض على مخترقي قواعد البيانات والمعلومات.
- توافر الأجهزة والبنية التحتية والبرمجيات الحديثة والأصلية اللازمة لتخزين البيانات والمعلومات.
- تحديد المخاطر المتوقعة التي قد تصيب المدرسة، ووضع الخطط اللازمة للتغلب عليها.
- توافر الاحتياجات اللازمة لعمل شبكات داخلية وخارجية في المدرسة؛ لتسهيل الاتصال بالجهات المعنية.

- توفر أنظمة محددة لتشفير المعلومات ذات الحساسية العالية، والتي يجب أن يتعامل معها فقط المتخصصون من داخل المدرسة.
- توفر قواعد بيانات عن كل كبيرة وصغيرة في المدرسة، بدلًا من السجلات الورقية.

وبالنظر إلى تلك الخطوات يتضح، أن هناك اتساقًا بينها وبين نظامي التقويم المعروضين سالفًا، أي نموذج PDCA، ونظام ISO 17799، أي أن تلك الخطوات جمعت بين النظامين للتأكد من قدرة المدرسة الثانوية الصناعية على الحفاظ على الأمن المعلوماتي بها.

القسم الثالث ـ واقع إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر:

يقدم هذا الجزء من البحث نظرة شمولية لواقع الأمن المعلوماتي في المدرسة الثانوية الصناعية في جمهورية مصر العربية، من خلال إبراز نقاط القوة والضعف في المدرسة الثانوية الصناعية والفرص والتهديدات بالمجتمع المحيط؛ من أجل إدارة عمليات الأمن المعلوماتي للمدرسة، وفيما يلي تفصيلًا لتلك الخطوة، والتي تتناول توضيحًا لواقع المدرسة الثانوية الصناعية في جمهورية مصر العربية، من حيث فلسفتها وأهدافها وإداراتها وممارسات مديريها، وذلك من خلال الدراسات التي أُجريت في هذا الصدد، وفيما يلي تفصيل لذلك الواقع:

تنطلق الرؤية المستقبلية لسياسة التعليم قبل الجامعي، من منطلق أساسي، ألا وهو توفير تعليم عالي الجودة للجميع في إطار نظام اللا مركزية، والمشاركة المجتمعية، وعلى قدرة القيادات في التعامل مع المتغيرات الحديثة بكفاءة، والتخطيط الإستراتيجي الجيد، والتفكير المتأمل، وذلك حتى يكون للقادة دور في التغيير والتطوير، وإعداد جيل متميز ومتفوق قادر على التعامل مع تحديات المستقبل. (66)

ويهدف التعليم قبل الجامعي إلى تكوين الدارس تكوينًا ثقافيًّا وعلميًّا وقوميًّا؛ بقصد إعداد الإنسان المصري المؤمن بربه ووطنه وبقيم الخير والحق والإنسانية، وتزويده بالقدر المناسب من الدراسات النظرية والتطبيقية والعملية، والمقومات التي تحقق إنسانيته وكرامته، وقدرته على تحقيق ذاته، والإسهام بكفاءة في عمليات وأنشطة الإنتاج والخدمات، من أجل تنمية المجتمع، وتحقيق رخائه وتقدمه.

والتعليم قبل الجامعي حق لجميع المواطنين في مدارس الدولة بالمجان، ومن هذا المنطلق تم إنشاء مدارس التعليم الفني بنوعياته، وذلك لإعداد فئة "الفني" في مجالات الصناعة والزراعة والتجارة والإدارة والخدمات، وتنمية الملكات الفنية لدى الدارسين، ويتم القبول في نوعيات التعليم الثانوي الفني بعد الحصول على شهادة إتمام الدراسة بمرحلة التعليم الأساسي، ووفقًا للشروط والقواعد الصادرة بالقرارات الوزارية المنظمة للنواحي التعليمية، وقد تم إنشاء المدارس الفنية بمواصفات فنية وخطط للعمل بها وتحدد أقسام الدراسة في نوعيات التعليم الفني وفقًا لمتطلبات خطط التنمية والظروف المحلية.

كما أن المدارس الفنية تقوم بمشروعات إنتاجية ذات صلة بتخصصها ولخدمة البيئة والمجتمع داخل كل محافظة، وقد صدر قانون التعليم رقم 139 لسنة 1981 المعدل بالقانون رقم (233) لسنة 1988 ومن خلاله صدرت القرارات الوزارية المنظمة للنواحي التعليمية. (67)

ومن ثم تقوم فلسفة التعليم الثانوي في مصر على تنمية الموارد البشرية المدربة والواعية، القادرة على استيعاب التكنولوجيا، وأصولها، وطرق استثمارها، وتكييفها لحاجات التنمية الاقتصادية، ومواجهة تحديات المستقبل، ومتطلبات سوق العمل، من خلال ما يلي: (68)

- العمل على الوفاء بالحاجات التعليمية للمتعلمين، وتطوير المهن والوظائف بما يتفق مع خصائص مرحلة المراهقة.
- الاهتمام بتحقيق أهداف المجتمع بمزيد من التقدم الاجتماعي والاقتصادي عن طريق تنمية طاقات الفرد، ومشاركته الإيجابية في تحقيق الأهداف.
- تهيئة الطلاب للعمل المفيد والربط بين أغراض التربية المدرسية، والأغراض المهنية المحددة.
- الاهتمام بالكشف عن ميول الطلاب وقدراتهم واستعداداتهم، وتوجيه هذه الميول والاستعدادات إلى مسارها السليم.
- إمداد الطلاب بالمهارات الأساسية والمعلومات والمفاهيم العلمية والفنية التي تمكنهم من احتراف المهنة، ومساعدتهم على الاستمرار في التقدم فيها.

بناء على ما سبق، يتضح أن المدرسة الثانوية الصناعية، كجزء من المدرسة الثانوية الفنية، تسعى إلى بناء اقتصاد متقدم قائم على العلم والمعرفة، وقائم أيضًا على مهارات الطلاب الخريجين القادرين على تقديم منتجات عالية الجودة، تكون قادرة على منافسة مثيلاتها من المنتجات الأخرى على مستوى العالم.

ويمكن استنباط نوعيات مختلفة من البيانات والمعلومات التي يجب الحفاظ عليها، وإدارتها، بشكل يسهم في استعادتها وقت الحاجة في المدرسة الثانوية الصناعية، ومن تلك النوعيات:

- بيانات أعضاء هيئة التدريس والإداريين والعاملين في المدرسة، بما فيها بياناتهم الشخصية، وتقارير أدائهم، وسنوات خبرتهم، والبرامج التدريبية التي حصلوا عليها.
- بيانات الطلاب المقيدين في المدرسة وأولياء أمورهم.
- ميزانية المدرسة، والموارد المادية المتاحة لها لتنفيذ خططها الحالية والمستقبلية.
- المعلومات التي تقدمها المدرسة لزائري صفحتها الرسمية على الإنترنت.
- منتجات المدرسة ومواعيد معارضها الرسمية ونسبة الأرباح والخسائر الخاصة بكل مشروع.
- المعلومات التي تجلبها المدرسة عن الممارسات الأفضل لدى مثيلاتها من المدارس الأخرى لتحقيق الإنتاجية الأعلى والمنافسة.
- معلومات عن احتياجات سوق العمل من المهارات والإمكانات المختلفة.
- معلومات عن أهم المصانع والشركات المحيطة، التي يمكن أن تقدم للموظفين أو المعلمين أو الطلاب برامج تدريبية تربط الدراسة النظرية بالدراسة التطبيقية.
- معلومات عن أهم شركات الصيانة والبرمجيات التي يمكنها تقديم برامج الصيانة والبرامج الأصلية للمدرسة، وبالتالي الاستعانة بها بسهولة وقت الحاجة.

يتضح مما سبق، أن المعلومات الموجودة في المدرسة تتراوح في درجة أهميتها بين المعلومات التي تحتاج إلى قدر من السرية فتحتاج إلى تشفير، كالميزانية، وبيانات أعضاء هيئة التدريس والموظفين، خاصةً فيما يتعلق بتقارير الأداء، ونسبة الأرباح والخسائر، والمشروعات المستقبلية التي تنوى المدرسة القيام بها، والممارسات الأفضل لدى المدارس الأخرى، والبيانات العادية التي تتاح على موقع المدرسة،

وتستخدم في تسويق منتجاتها؛ كمواعيد المعارض السنوية، ونوعية المنتجات المقدمة فيها، وغيرها من المعلومات الأخرى.

وسواء كانت المعلومات عادية أو مشفرة، فهي في حاجة لإدارتها، ونظرًا لما لإدارة عمليات الأمن المعلوماتي من أهمية في الحفاظ على المعلومات الخاصة بكل مدرسة، فالأمر ذو أهمية لا يمكن إغفالها بالنسبة للمدرسة الثانوية الصناعية، وذلك لطبيعتها التي جعلتها تحتكم على المزيد من المعلومات التي تحتاج إلى الحفاظ عليها من الضياع أو السرقة مقارنةً بأنماط المدارس الأخرى.

وفي السطور القليلة القادمة يقوم البحث ـ وفقًا لمنهجيته ـ بتحليل البيئة الداخلية للمدرسة الثانوية الصناعية، وذلك من خلال إبراز جوانب القوة والضعف المرتبطة بالحفاظ على الأمن المعلوماتي بها، وتحليل البيئة الخارجية بها، عن طريق إبراز الفرص والتهديدات المرتبطة بالحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية بـ ج. م. ع.

أولًا ـ نقاط القوة المرتبطة بإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية (Strengths (S:

يتعرض هذا الجزء من البحث للجهود التي قامت بها الوزارة لمساعدة العاملين في المدرسة الثانوية الصناعية ـ وعلى رأسهم مدير المدرسة ـ على الحفاظ على الأمن المعلوماتي للمدرسة، ومن ثم تهدف الخطة الإستراتيجية للتعليم قبل الجامعي ـ فيما يخص التعليم الفني ـ إلى إتاحة التجهيزات وتكنولوجيا التعليم بما يتناسب مع نوعية التعليم الفني وعدد الطلاب وفق معايير معدة لذلك، بالإضافة إلى استكمال التجهيزات والبنية التحتية اللازمة للمدارس، وتوفير البنية التحتية والإمكانات المادية والبشرية، والآلات والعدد والخامات والبرامج التدريبية لتفعيل العملية التعليمية في المدارس. (69)

وفي إطار مبادرة تطوير التعليم المصرية الشاملة، يتمثل الغرض من مشروع تطوير التعليم الفني باستخدام تكنولوجيا المعلومات والاتصالات، في الارتقاء بالتعليم الفني والتدريب المهني وتعزيزه، من خلال استخدام أنظمة تكنولوجيا المعلومات والاتصالات، علمًا بأن فئات المستفيدين المستهدفة تتمثل في المعلمين والطلاب في المدارس الصناعية، فضلًا عن المجتمع الأكبر المحيط بهذه المدارس. وخلال

المشروع، تم تحديث 10 مدارس مهنية متقدمة في نواحي البنية التحتية لتكنولوجيا المعلومات، والاتصالات، والمناهج التعليمية، وبناء قدرات التنمية البشرية. وهذا المشروع شراكة بين وزارة الاتصالات وتكنولوجيا المعلومات والبرنامج الإنمائي للأمم المتحدة. (70)

كما استحدثت وزارة التربية والتعليم بعض الوحدات المدرسية داخل المدارس بشكل عام، ومنها وحدة المعلومات والإحصاء، التي صدر قرار بإنشائها عام 2002، بموجب القرار الوزاري رقم 99، الذي نصت مادته الأولى على أن يتم إنشاء وحدة تسمى وحدة المعلومات والإحصاء بجميع المدارس بالمراحل الدراسية كافة، وتتشكل على النحو التالي: (71)

- أحد الوكلاء في المدرسة (ويكون مشرفًا على الوحدة).
- أحد العاملين في المدرسة ممن يجيدون استخدام الحاسب الآلي من غير العاملين بالتدريس.
- عدد من العاملين والسكرتارية.

ويتراوح عدد العاملين بالوحدة من 2 ـ 5 أفراد، وذلك حسب حجم المدرسة، وتكون الوحدة تحت الإشراف المباشر لمدير المدرسة.

ونصت المادة الثانية من القرار على أن الهدف الأساسي للوحدة هو المساهمة في تحقيق نظام معلومات شامل ومتكامل، يلبي متطلبات المستويات الإدارية المختلفة، من بيانات، ومعلومات، ومؤشرات داعمة لاتخاذ القرار بصورة دقيقة وسريعة. (72)

أما عن اختصاصات الوحدة فقد حددها القرار في مادته الثالثة وفقًا لما يلي: (73)

- تجهيز وتدقيق إدخال البيانات اللازمة لنظام المعلومات.
- تسجيل كل ما يطرأ من تغيير على بيانات التلاميذ والعاملين في المدرسة فورًا، وبكل دقة.
- التأكد من صحة البيانات ودقتها، ومطابقتها للواقع باستمرار.
- توفير المعلومات لكل المستويات وتداولها وفق التعليمات.
- الحفاظ على أمن البيانات وسريتها.

- القيام بالإجراءات الفنية الخاصة بعمل نسخ الحفظ وخلافه.
- اتباع كافة التعليمات الصادرة من الإدارة العامة للمعلومات والحاسب الآلي بهذا الشأن.

كما استحدثت وزارة التربية والتعليم وحدة مدرسية جديدة في المدرسة الثانوية الفنية، أطلق عليها وحدة معلومات سوق العمل، وأنشئت بهدف دراسة البيانات الخاصة بسوق العمل وتحليلها، للوصول إلى نتائج تتيح فرص تعليم أفضل وسهولة الانتقال إلى سوق العمل، وتتمثل أهم واجبات المسئول عن تلك الوحدة فيما يلي: (74)

- قيادة قسم معلومات سوق العمل بالوحدة المدرسية.
- الاشتراك مع أعضاء الوحدة في وضع الخطة السنوية للقسم والوحدة.
- التعاون مع مسئول التوظيف في إنشاء قاعدة بيانات عن سوق العمل في نطاق عمل المدرسة.
- تحليل البيانات الخاصة بسوق العمل وتقديم المقترحات لمدير الوحدة المدرسية، ومسئول معلومات سوق العمل بالوحدة الفرعية.
- دراسة سوق العمل في نطاق عمل المدرسة لتحقيق أفضل استفادة للطلاب من البرامج التدريبية.
- بناء علاقات عمل جيدة مع أصحاب الأعمال للوقوف على احتياجاتهم ومحاولة تلبيتها.
- إمداد قسم التدريب بنتائج دراسة سوق العمل وتحليله، حتى تتيح للطلاب برامج تكميلية وتحويلية لمواكبة متطلبات سوق العمل.
- تحديد المهارات والمعارف والقدرات المطلوبة لخريجي المدارس بناءً على معلومات سوق العمل، وذلك لتسهيل انتقال الطلاب إلى سوق العمل.
- رفع بيانات سوق العمل للوحدة الفرعية بالمديرية، حتى تقوم برسم الخريطة الصناعية بالمحافظة، والتي ترفعها بدورها إلى الوحدة المركزية للقطاع لرسم الخريطة الصناعية على المستوى القومي.

كما حددت وزارة التربية والتعليم مسئوليات العاملين عن بعض الوحدات المدرسية المسئولة عن المعلومات الموجودة في المدرسة، كوحدة التوظيف في المدرسة الثانوية الفنية، وهي وحدة مسئولة عن تيسير الانتقال إلى سوق العمل، والتي

أنشئت بقرار وزاري رقم 283 بتاريخ 2014/6/26، وتهتم بتمكين طلاب وخريجي التعليم الفني من الانتقال لسوق العمل، من خلال مساعدتهم على اتخاذ القرارات الصحيحة لحياتهم العملية المبنية على معلومات دقيقة عن سوق العمل، وأصحاب العمل. وتتمثل الواجبات الأساسية لمسئول تلك الوحدة فيما يلي: (75)

- توطيد العلاقة مع أصحاب الأعمال والمجتمع المحيط.
- توفير أكبر قدر من المعلومات عن فرص العمل المتاحة للطلاب وخريجي المدرسة.
- توفير معلومات عن أماكن التدريب المتاحة لخريجي المدرسة.
- المساهمة الفعالة مع مسئول قسم دراسات سوق العمل في تبادل المعلومات وضمان صحتها.
- توفير البيانات والمعلومات المتاحة لدى القسم بقاعدة البيانات لباقي أقسام الوحدة.

يضاف إلى ما سبق تحديد وزارة التربية والتعليم ـ بموجب القرار الوزاري رقم 283 لعام 2014 ـ مسئوليات وواجبات المسئول عن وحدة ريادة الأعمال في المدرسة الثانوية الفنية، وذلك لتيسير الانتقال لسوق العمل أيضًا، ومن مسئولياته ما يلي: (76)

- العمل على وضع خطة للمشاريع الصغيرة لخريجي التعليم الفني.
- يعتبر بمثابة المرجع الرئيس لتقديم معلومات ريادة الأعمال في المدرسة.
- التواصل مع جمعيات رجال الأعمال وأي مؤسسات أخرى، لدعم وتقديم خدمات وبرامج ريادة الأعمال المتكاملة والفعالة لطلاب التعليم الفني.
- إدارة برامج ريادة الأعمال داخل المدرسة وتقييمها والإشراف عليها.
- التعاون مع مدارس التعليم الفني داخل المحافظة لتقديم خدمات ريادة الأعمال للطلاب والخريجين.

يضاف إلى ما سبق اهتمام وزارة التربية والتعليم بتحديد الوصف الوظيفي لمسئول الإرشاد والتوجيه المهني. وتعتبر وحدة الإرشاد والتوجيه المهني إحدى الوحدات المستحدثة في المدارس الثانوية الفنية بوجه عام، وهي المسئولة أيضًا عن تيسير الانتقال إلى سوق العمل، وذلك من خلال مساعدة الطلاب على اتخاذ قرارات

صحيحة لحياتهم العملية، والمبنية على معلومات دقيقة عن سوق العمل، وذلك عن طريق مساعدة الطلاب على التخطيط الوظيفي لحياتهم العملية حسب قدراتهم ومهاراتهم، واحتياجات سوق العمل، وتتمثل الواجبات الأساسية لمسئول تلك الوحدة فيما يلي: (77)

- التعاون مع قيادات التعليم الفني من أجل تنفيذ برامج الإرشاد والتوجيه المهني في المدرسة.
- الإشراف على تدريبات توجيه وتقييم برامج التوجيه والإرشاد التي يتم تقديمها في المدرسة.
- تقديم خدمة الإرشاد والتوجيه المهني لطلاب المدرسة.
- التعاون مع مسئول قسم معلومات العمل لضمان تقديم معلومات صحيحة للخريجين عن احتياجات سوق العمل.

وبالنظر إلى القرارات الوزارية سالفة الذكر، يتضح أن جميع الوحدات المدرسية المستحدثة في المدرسة الثانوية الصناعية ركزت على ما يلي:

- ضرورة توافر البيانات والمعلومات الصحيحة عن قدرات الطلاب ومهاراتهم من ناحية، ومتطلبات سوق العمل من ناحية أخرى.
- ضرورة توفر الأشخاص المؤهلين والأكفاء القادرين على إدخال البيانات والمعلومات واستدعائها وقت الحاجة.
- ضرورة توفر قاعدة بيانات عن أصحاب العمل ورجال الأعمال لما لهم من دور في توظيف الخريجين وتدريب الطلاب.
- التأكيد على أهمية التنسيق بين جميع الوحدات المستحدثة لتبادل المعلومات اللازمة لإرشاد الطلاب والخريجين وتوجيههم.
- التأكيد على أهمية اتصال المدرسة مع المجتمع الخارجي لتحقيق متطلبات المجتمع.
- الاهتمام بالتعاون والتنسيق بين الوحدات من أجل عمل خطة شاملة للتوظيف والوفاء بمتطلبات سوق العمل.
- الاهتمام بعمل قواعد بيانات عن المشروعات الصغيرة التي يمكن للطلاب والخريجين القيام بها، ومن ثم تسهيل فرص العمل المتاحة لهم.

بناء على ما سبق، يتضح أن تواجد جميع الوحدات المدرسية سالفة الذكر في المدرسة الثانوية الفنية، يمثل نقاط قوة لا يجب الاستهانة بها للمدرسة الثانوية الفنية بشكل عام، والمدرسة الثانوية الصناعية على وجه الخصوص، ذلك أنها بمثابة البوابة التي ينطلق من خلالها الطلاب إلى سوق العمل بناء على معلومات صحيحة ودقيقة، تقوم المدرسة بجمعها وتخزينها حتى وقت الحاجة إليها، الأمر الذي إن غاب، أصبحت الأمور تتسم بالعشوائية، بما إنها لا تقوم على معلومات وقواعد بيانات مدققة وسليمة.

وبالتكامل بين ما سبق والعمليات المختارة لإدارة الأمن المعلوماتي في المدرسة الثانوية الصناعية في جمهورية مصر العربية، يمكن تلخيص أهم نقاط القوة في المدرسة في وجود جهود لا يستهان بها للتخطيط للأمن المعلوماتي في المدرسة الثانوية الصناعية، وذلك من خلال الوحدات المدرسية المستحدثة، التي تساعد ـ من خلال قدرتها واختصاصها في الحفاظ على البيانات والمعلومات ـ على الحفاظ على أمن المعلومات في المدرسة، تمهيدًا لاتخاذ القرار الرشيد.

ثانيًا ـ جوانب الضعف المرتبطة بإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية Weaknesses (W):

تعاني المدرسة الثانوية الفنية بشكل عام، والمدرسة الثانوية الصناعية على وجه الخصوص، من عدد من جوانب الضعف، لا سيما في قدرتها على الحفاظ على الأمن المعلوماتي، ومن جوانب الضعف المرتبطة بهذا السياق ما يلي: (78)

- ضعف مشاركة أصحاب المصلحة والمستفيدين الحقيقيين من مخرجات التعليم والتدريب في المدرسة، وهو ما يظهر في صياغة مواصفات المهن المختلفة، والتوصيف الوظيفي للعاملين، ووضع المناهج والبرامج الدراسية، والاشتراك في عمليات المتابعة والتقويم.
- عدم وجود آلية محددة ومدروسة لتمويل عمليات التدريب المختلفة، سواء للتدريب الأساسي، أو التدريب أثناء الخدمة، أو ما قبل الخدمة.

ويمثل ما سبق، نظرة شاملة عن الوضع الحالي للعلاقة بين المدرسة الثانوية الصناعية، وجماعات المصالح والمستفيدين، سواء من رجال الأعمال، أو أصحاب الشركات، تلك الفئة التي من شأنها استيعاب كافة الخريجين من هذا النوع من

المدارس، إذ يتضح أنهم من أكثر الفئات التي على المدرسة الثانوية الصناعية الاستفادة منها في وضع وتحديد مواصفات الخريج والمهارات التي يجب أن يتسموا بها ليتم استيعابهم في سوق العمل، ولعل الانفصال الواضح بين المدرسة، ورجال الأعمال، يظهر مدى المشكلات التي قد تنتج من جراء هذا الانفصال، إذ أصبحت المدرسة الثانوية الصناعية بمعزل عن الاحتياجات الحقيقية لتلك الفئة، ومن ثم ضعفت المشاركة المنشودة.

كذلك يمكن إضافة نقاط الضعف التالية: (79)

- عدم اعتماد البرامج التدريبية على معرفة الاحتياجات التدريبية الفعلية، وبالتالي عدم إعداد برامج تدريبية قائمة على الاحتياجات الحقيقية للأفراد.
- عدم توافر قاعدة بيانات دقيقة توضح البرامج التدريبية، ومدى مناسبتها لأعداد المستفيدين منها وأنواعها.

يضاف إلى ما سبق النقاط التالية: (80)

- انخفاض مستوى أداء الإدارة المدرسية على مستوى بعض مدارس التعليم الفني، وضعف جهاز التوجيه، وقدرته على أداء مهامه.
- غلبة أسلوب الإدارة المدرسية بمفهوم الإدارة والضبط عن مفهوم التوجيه والمشاركة في المسئولية، مما جعل النظام الإداري يمثل عبئًا على كاهل المعلم، واتساع الفجوة بين النظام الإداري، والنظام التعليمي.
- قلة وجود صف ثان من القيادات.
- ضعف قدرات معظم مديري التعليم الفني الصناعي.
- نظام استلام المعدات بشكل عهدة يحولها من تقنية إلى مقتنى، مما يؤثر على استخدامها بوصفها معدات يمكن أن تفسد أو تتلف من الاستخدام.
- ضيق مساحة بعض الأقسام والمعامل وقلة الخامات والأدوات.
- سوء حالة بعض المباني والمرافق لبعض المدارس الفنية وحاجتها لعمليات صيانة شاملة أو إحلال وتجديد.
- وجود بعض الآلات والمعدات والأدوات الفنية الخاصة بالعملية التعليمية والتدريبية التي تحتاج إلى إصلاح وصيانة، وقد يتعذر ذلك بسبب عدم وجود

عقود صيانة لها، بالإضافة إلى عدم توافر قطع الغيار اللازمة لها، مما يجعلها معطلة دون الاستفادة منها.

- عدم توفر الحماية الأمنية للمدارس الفنية لتأمين الآلات والماكينات والعدد والبيانات والمعلومات من السرقة.
- ضعف تسويق المنتجات لقلة عدد المعارض المتاحة.

بالنظر إلى نقاط الضعف السالفة يتضح أنها في المجمل تتلخص في ضعف قدرات مدير المدرسة، وضعف الموارد البشرية من الموظفين، وعدم الاستغلال الأمثل للموارد المادية، وسيطرة فكرة العهدة عليها. الأمر الذي يؤثر على عدم توفر قواعد بيانات عن احتياجات السوق من المنتجات، ومواصفات تلك المنتجات؛ مما يؤثر بالسلب على تسويقها، كما أن عدم توفر خطة صيانة متكاملة لصيانة الأجهزة يهدد جودتها، وقدرتها على الاستمرار في الحفاظ على المعلومات، مما يهدد الأمن المعلوماتي للمدرسة، ويهدد معلوماتها بالضياع أو السرقة، كما يمثل ضعف قدرات وكفاءات مديري المدرسة بشكل عام، ومسئولي الوحدات المستحدثة بشكل خاص، أحد المعوقات الأساسية التي من شأنها تهديد قدرة المدرسة على التخطيط، ووضع خطة لإدارة الأمن المعلوماتي للمدرسة، والاتصال بالغير لتحقيق الأمن المعلوماتي، ووضع خطط تدريبية، وتحديد الاحتياجات التدريبية للعاملين بالوحدات المستحدثة؛ من أجل الحفاظ على الأمن المعلوماتي بها، وتقويم قدرة المدرسة على الحفاظ على الأمن المعلوماتي.

كما يمكن إضافة نقاط الضعف التالية: (81)

- قصور المعلومات الحقيقية عن سوق العمل.
- ضعف البنية التحتية لشبكة المعلومات بمدارس التعليم الثانوي الصناعي.
- سوء مرافق التعليم الثانوي الصناعي والبنية الأساسية للاتصالات وتكنولوجيا المعلومات.
- محدودية التعاون بين المدارس الثانوية الفنية الصناعية والبيئة المحيطة.
- عدم وجود قاعدة بيانات تخص التعليم الفني الصناعي.

بالنظر إلى ما سبق، يتضح أن عدم وجود قاعدة بيانات تخص أهم البيانات والمعلومات التي تحتاج إليها المدرسة الثانوية الصناعية، مثل الجهات التي يمكنها

الاستفادة منها؛ كالشركات والمصانع، ورجال الأعمال، والميزانية، والأرباح التي قد تجنيها من المشروعات التي تقوم بها، ومهارات الخريجين، وخطة التوظيف، والخطط والمشروعات المقترحة الصادرة عن وحدة ريادة الأعمال، وقواعد البيانات الخاصة بالاحتياجات التدريبية للمعلمين والعاملين والطلاب، وخطط التدريب المستقبلية لكافة الفئات السالفة، وقواعد البيانات الخاصة باحتياجات سوق العمل، والمواصفات القياسية للمنتجات، وغيرها من البيانات والمعلومات الأخرى التي تحتاج إليها المدرسة الثانوية الصناعية، سواء في الأوقات العادية، أو للتخلص من الأزمات والتعافي منها، واستعادة نشاط المدرسة بأسرع وقت ممكن.

وبمقارنة الإطار النظري للبحث مع الواقع النظري للمدرسة الثانوية الصناعية في جمهورية مصر العربية، وبالنظر إلى العمليات المختارة، يمكن تلخيص أهم نقاط الضعف في تلك العمليات فيما يلي:

- ضعف قدرة المدرسة الثانوية الصناعية على التخطيط للحفاظ على أمنها المعلوماتي؛ نظرًا لضعف البيانات والمعلومات المتاحة بها، الأمر الذي لا يمكن من إتمام التخطيط، ذلك أنه عملية تعتمد في المقام الأول على ضرورة توافر البيانات والمعلومات الدقيقة والحديثة.
- ضعف قدرة المدرسة الثانوية الصناعية على التخطيط والتدريب للعاملين والمديرين على الحفاظ على الأمن المعلوماتي، لعدم توافر بيانات ومعلومات دقيقة عن البرامج التدريبية، ومدى جودتها، ومدى استفادة المستفيدين منها.
- عدم تقديم برامج تدريبية تتفق والاحتياجات التدريبية للمتدربين، أو احتياجات الوظائف الجديدة التي ظهرت نتيجة للوحدات المدرسية المستحدثة.
- ضعف فرص الاتصال بين المدرسة الثانوية الصناعية والبيئة المحيطة، وضعف مهارات التواصل لدى القائمين على إدارة هذه المدارس والعاملين فيها، مما يؤثر على قدرة المدرسة في تحديد الجهات التي يمكنها الاتصال بها عند الحاجة للحفاظ على الأمن المعلوماتي.
- ضعف فرص المشاركة والاتصال بين المدرسة وأصحاب المصلحة من رجال الأعمال أو أصحاب المشروعات من القادرين على تقديم خدمات للمدرسة من شأنها تحسين مستواها، وتحسن مخرجاتها.

- عدم وجود خطط تقويمية للمدرسة تستطيع عن طريقها تحديد ما إذا كانت قادرة أو غير قادرة على الحفاظ على أمنها المعلوماتي بناء على نماذج أو مؤشرات فعلية تكون بمثابة الحكم على جودة الأداء.

ثالثًا ـ الفرص المرتبطة بإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية (Opportunities (O:

يقدم هذا الجزء من البحث الفرص التي يمكن للمدرسة الثانوية الصناعية في جمهورية مصر العربية استغلالها للتغلب على نقاط الضعف، واستثمار نقاط القوة، فيما يخص الحفاظ على الأمن المعلوماتي بها، ويمكن عرض تلك الفرص فيما يلي:

قامت وزارة التربية والتعليم بالتعاون مع وزارة الاتصالات بعمل الشبكة الداخلية للمدارس لربط جميع أجهزة الحاسب بشبكة واحدة وربطها بالشبكة المعلوماتية الدولية، كما تم توريد وتشغيل ما يلي: (82)

- عدد (2) معمل حاسب آلي بواقع (16) جهاز لكل معمل.
- عدد (6) جهاز حاسب، بواقع (2) للمكتبة، (1) لمدير المدرسة، (1) لشئون الطلاب، (1) لشئون العاملين، (1) للعيادة المدرسية.
- عدد (1) جهاز لكل قسم من أقسام المدرسة.
- عدد (2) فصل مطور لكل مدرسة من المدارس المختارة، ويشمل الفصل المطور (عارض ضوئي+ لاب توب).
- عدد (1) كاميرا ديجيتال، عدد (4) طابعات ليزر، و(1) ماسح ضوئي.
- إتاحة خدمة الإنترنت لعدد (7) مدارس.
- كما قامت وزارة الاتصالات وتكنولوجيا المعلومات بعمل مشروع قانون أمن الفضاء المعلوماتي، والذي يشمل ثلاثة محاور أساسية، هي: (83)
  - حماية الفضاء المعلوماتي بجميع مشتملاته من أي تعدٍّ خارجي.
  - التزام الجهات المختلفة ـ بمختلف تخصصاتها ـ بحماية ما يخصها من الفضاء المعلوماتي، وما يضمه من بيانات ومعلومات، وخاصةً الشخصية منها.
  - إنشاء جهاز قومي للرقابة على جميع أعمال أمن المعلومات، ومنح تراخيص مزاولة أعمال الخبرة، والتخصص في هذا المجال.

كما هدف هذا القانون إلى وضع القواعد اللازم على المتحكم في البيانات والمعلومات اتباعها لتأمين ما يخصه من الفضاء المعلوماتي، وما تحتويه من بيانات ونظم وبرامج وشبكات، وتحديد التزاماته، كما يهدف إلى مكافحة برامج اختراق نظم المعلومات والشبكات؛ بما يؤدي إلى تحقيق الأمن المعلوماتي والقومي، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات وشبكات المعلومات، وحماية المصلحة العامة. (84)

ويتلخص دور الجهاز القومي لأمن المعلومات في ترسيخ فكر وثقافة أمن المعلومات، وتحديد التزامات المتحكم في المعلومات، ووضع نظام لإدارة تشغيل الموارد المعلوماتية، وكيفية تأمين مواقع تشغيل المعلومات، وكيفية الولوج إلى المعلومات والشبكات. (85)

كما وضعت منظمة اليونسكو عددًا من المؤشرات التي يمكن استخدامها للحكم على قدرة المؤسسات التعليمية في استخدام تكنولوجيا المعلومات، ومن تلك المؤشرات ما يلي: (86)

- توافر برامج تدريبية تساعد العاملين بالمؤسسة التعليمية على استخدام أجهزة الحاسب الآلي.
- توافر فرص دورية لصيانة الأجهزة الموجودة في المدرسة.
- وجود شبكات للاتصال بالإنترنت داخل المدرسة.
- وجود معامل للكمبيوتر متاحة لاستخدام العاملين والمعلمين والطلاب.
- وجود برامج أصلية تستخدم للحفاظ على المعلومات الموجودة في المدرسة.

كما أعدت وزارة التربية والتعليم ـ من خلال قطاع التعليم الفني بها ـ قواعد بيانات مختلفة، تمهيدًا لعقد مؤتمرها التقني الأول والثاني، من أجل ربط التعليم الفني بمختلف تخصصاته بسوق العمل؛ حيث يواجه المجتمع العربي تحديات نجمت عن التطورات والتحولات العلمية والتكنولوجية والاقتصادية المتسارعة، وأن سياسات التعليم بوجه عام، والتعليم الفني بوجه خاص، قد تكون الوسيلة التي يجب أن يعتمد عليها المجتمع العربي لمواجهة ضخامة هذه التحديات، وفى ظل الانفتاح الاقتصادي على العالم ومواجهة المتغيرات العالمية ـ التي تتطلب استعدادًا جادًّا لدخول المنافسة الضارية في السوق الدولية ـ كان لا بد للتعليم الفني أن يتحمل مسئولية رفع

إنتاجية المواطن، عن طريق؛ التدريب والتأهيل المستمر، والارتفاع بقدراته التنافسية؛ حتى يمكنه مواكبة ما يحدث في العالم من تطور وتنمية مستمرة. وفى ضوء ما أحدثته ثورة المعلومات في هذا العصر من تطور، أصبح كل من العلم والتكنولوجيا من ضرورات حياة الإنسان المعاصر. ولما كانت الثورة العلمية والتقنية ثورة مستمرة يزداد تأثيرها في الحياة، فإن ذلك تطلب أن تكون هناك وقفة تقويمية لسياسة التعليم ونظامه ومحتواه؛ لمواجهة هذا التغير السريع، وتنمية قدرة الإنسان على المعرفة واكتساب المهارات.

وقد تعددت محاور المؤتمر التقني الأول لتتناول خبرات الاتحاد الأوروبي في مجال التعليم الفني (التقني) وإمكانية تطبيقها، ومعايير الجودة الشاملة، ومستويات المهارة في التعليم الفني والتدريب المهني، وربط التعليم الفني باحتياجات السوق على المستويين المحلي والعالمي، والتعليم والتدريب المستمرين لتأهيل المعلمين. وتعددت الجهات المشاركة في هذا المؤتمر، ومنها: وزارة التعليم العالي، وممثلو اتحاد الصناعات والغرف التجارية، ومخططو وواضعو سياسات تطوير التعليم والتدريب، والمستثمرون، وأصحاب الأعمال، والمراكز البحثية القومية. (87)

وبالنظر إلى ما سبق، يتضح أن تنظيم مثل هذا المؤتمر يتطلب من كل مدرسة إعداد قاعدة بيانات شاملة عن مجتمع المستفيدين، والإمكانات المتاحة بكل مدرسة، والاحتياجات اللازمة، والشركات، والمؤسسات التي يمكنها المساهمة في توظيف الخريجين، أو إمداد المدرسة بمعلومات عن احتياجات تلك القطاعات، وبالتالي ربط المدرسة باحتياجات المجتمع المحيط وسوق العمل.

ولم تتوقف جهود الوزارة عند هذا الحد؛ حيث عقدت المؤتمر التقني الثاني، استكمالًا للمجهودات التي قام بها المؤتمر التقني الأول؛ حيث هدف المؤتمر إلى بحث أساليب وسبل تقوية الشراكة بين مؤهلي ومدربي القوى البشرية الفنية من جهة، ومشغلي تلك القوى من جهة أخرى، وذلك لتطوير التعليم الفني والتدريب المهني بما يجعله قادرًا على تلبية احتياجات سوق العمل، من حيث ملاءمة نوعية الخريج الفني وكفاءته، لمتطلبات التقنيات الحديثة المستخدمة في مجالي الإنتاج والخدمات، حتى يمكن دعم أنشطة الإنتاج والخدمات باحتياجاتها من القوى الفنية المدربة، لتمكينها من رفع إنتاجيتها وخدماتها كمًّا وكيفًا؛ بهدف توفير فرص المنافسة للمنتج المصري

في السوقين المحلي والدولي، بما ينعكس إيجابًا على الاقتصاد القومي، وزيادة فرص العمل لخريجي التعليم الفني والتدريب المهني عن طريق تزويدهم بما يتطلبه سوق العمل المحلي من مهارات وقدرات. (88)

ومن المعلوم أنه لا يمكن تنظيم مثل تلك المؤتمرات، إلا بناء على وجود قواعد بيانات متوفرة بالمدرسة عن احتياجاتها من القوى البشرية والمهارات اللازمة لتحقيق المنافسة المطلوبة، وكذا المهارات اللازمة لتمكين الدارسين من تلك المهارات.

كما يمكن إضافة عدد من الفرص التي تظهر من خلال الأهداف الإستراتيجية لوزارة التربية والتعليم لتطوير التعليم الفني، ومن أهمها ما يلي: (89)

- إتاحة التجهيزات وتكنولوجيا التعليم بما يتناسب مع نوعية التعليم الفني وعدد الطلاب وفق معايير معدة لذلك.
- ربط التعليم الفني بمؤسسات الإنتاج والخدمات في البيئة المحيطة لتدريب الطلاب في هذه المؤسسات الإنتاجية.
- التعاون مع الشركات وأصحاب الأعمال من أجل تطوير التعليم الفني ليتماشى مع التحديات الكبيرة التي تفرضها المنافسة العالمية في الحاضر والمستقبل، وكذلك من أجل إمداد أصحاب الأعمال بخريجين ذوي مهارة ومؤهلات يتطلبها سوق العمل.

بالنظر للتوجهات سالفة الذكر، يتضح أنها تركز على ضرورة إتاحة التكنولوجيا الحديثة بوصفها البنية التحتية اللازمة لتحقيق متطلبات مجتمع المعرفة من ناحية، وبوصفها السبيل الذي لا بد منه لتحقيق الأمن المعلوماتي المنشود للمعلومات التي يجب على المدرسة الثانوية الصناعية الحفاظ عليها من ناحية أخرى، كما ركزت تلك التوجهات على ضرورة إحداث التعاون مع رجال الأعمال. الأمر الذي يؤكد على الاهتمام بالاتصال مع أعضاء المجتمع المحلي لإمدادهم باحتياجاتهم من الخريجين المهرة. الأمر الذي لا يستقيم بدون وجود قواعد بيانات عن عدد الخريجين ومهاراتهم، والبرامج التدريبية التي حصلوا عليها... إلخ، وأصحاب الأعمال، وتخصصاتهم، والدعم المحتمل منهم... وهكذا.

وجدير بالذكر في هذا السياق، أن هناك بعض من جهود الشراكة المجتمعية للمساهمة في دعم التعليم الفني، ومنها ما يلي: (90)

- التعاون مع وزارة الإعلام لتخريج العمالة الفنية المدربة في مجال الإلكترونيات.
- التعاون مع وزارة البترول لتخريج العمالة الفنية المدربة في مجال تكنولوجيا البترول.
- توقيع اتفاقية مع مؤسسة مصر الخير؛ تهدف إلى تأهيل خريجي المدارس الفنية ومساعدتهم ماديًّا على إنشاء مشروعات صغيرة في مجال تخصصهم الدراسي وإدارتها، وتحسين كفاءة الإدارة المدرسية والتوجيه الفني والمعلمين بالتعليم الفني الصناعي.
- توقيع اتفاقية تعاون مع كلية الهندسة بجامعة قناة السويس؛ لتدريب المعلمين والطلاب والموجهين في المحافظات الداخلة في النطاق الإقليمي لجامعة قناة السويس.
- التعاون مع الهيئة القومية للاتصالات السلكية واللا سلكية؛ لتخريج العمالة الفنية المدربة في المجالات التالية (سنترالات إلكترونية ـ تراسل ـ فني اتصالات شبكات ـ فني اتصالات قوى كهربية ـ تكييف ـ حاسبات).

مما سبق، يتضح أن هناك فرصًا واضحة للعيان تتجلى في التعاون بين بعض الهيئات والوزارات، وبين وزارة التربية والتعليم، متمثلة في المدرسة الثانوية الصناعية، الأمر الذي لا يمكن إتمامه بالشكل الصحيح إلا من خلال توافر بيانات صحيحة ودقيقة، ومخزنة بشكل سليم، بأجهزة مقاومة للسطو والتلف، عن تلك الهيئات والوزارات، في المدرسة الثانوية الصناعية، وكذا عن سبل التعاون التي من الممكن أن تتم بين الجانبين، خاصةً أن ذلك التعاون يفرز متخصصين في مجالات متعددة.

كما تضمنت الخطة الإستراتيجية القومية سبل تطوير التعليم الفني في جمهورية مصر العربية، ومن أهم تلك السبل ما يلي: (91)

- استكمال التجهيزات وصيانة البنية التحتية لمدارس التعليم الفني.
- توفير الإمكانات المادية والبشرية، والمعدات، والآلات، والخامات، والتدريبات اللازمة لتفعيل العملية التعليمية في المدارس.

- تحويل مدارس التعليم الفني إلى تعليم قائم على التعليم والتدريب المزدوج، في إطار مدرسة في كل مصنع، مع إصدار القواعد المنظمة للتعاون بين إدارة المدرسة والمؤسسات الإنتاجية.

وبالنظر إلى ما سبق، يتضح أنه إذا تم استكمال البنية التحتية اللازمة للمدرسة الثانوية الفنية، مع استكمال الإمكانات المادية، وتوفير الموظفين القادرين على استخدام الموارد المادية بالشكل الصحيح، فإن ذلك يكون بمثابة الفرصة التي تتيح للمدرسة الثانوية الصناعية تخزين معلوماتها بالشكل الذي يتيح لها استرجاعها واستعادتها وقت الحاجة إليها.

كما يعتبر مركز التطوير التكنولوجي ـ الذي تم إنشاؤه لإدخال التكنولوجيا المتطورة، وتنويع مصادر المعرفة في مجال التعليم ـ أحد الفرص المتاحة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية؛ حيث يوجد 27 مركزًا فرعيًّا للتطوير التكنولوجي، بمعدل مركز بكل مديرية تعليمية.

ويعتبر المركز بمثابة الفرصة لإحداث فرص التدريب على المهام الجديدة التي يمكن أن توكل إلى مسئولي الوحدات المستحدثة، لتدريبهم على القيام بالمهام الجديدة. (92)

كما يوجد مركز المعلومات الفنية للتعليم الصناعي والتدريب، الذي أُنشئ بشبرا عام 1998، وكان هدف إنشائه تدريب معلمي التعليم الفني الصناعي في تخصصات السيارات وغيرها. (93)

ويمكن استغلال وجود مثل هذا المركز في تدريب العاملين المسئولين عن الوحدات المستحدثة عن كيفية بناء شبكات المعلومات، وتخزين المعلومات، واستعادتها، والحفاظ عليها من الفيروسات، والسطو، والضياع، وتحقيق التواصل مع الغير من خلالها، أي باختصار استغلال تلك المعلومات الاستغلال الأمثل، بناء على الحفاظ عليها في المقام الأول.

كما تولى المعهد القومي للاتصالات بالتنسيق مع وزارة الاتصالات والمعلومات ووزارة التربية والتعليم ـ منذ عام 2002 ـ الإشراف على البرنامج القومي الخاص بالتدريب المتخصص في مجال تكنولوجيا المعلومات والاتصالات، وقد تم تنفيذ الدورات التدريبية من خلال مجموعة من الشركات العالمية من أجل تدريب

متخصصين في مجال تكنولوجيا المعلومات، بواقع 5000 متخصص سنويًا في مجالات تطوير البرمجيات، وإدارة قواعد البيانات، ودعم اتخاذ القرار، ونظم المعلومات الجغرافية، وتصميم شبكات الحاسبات وتطويرها، كما تم في إطار الخطة القومية للاتصالات تدريب حوالي 2000 متدرب على أساسيات تكنولوجيا المعلومات والاتصالات بالتعاون مع الجامعات المصرية. (94)

ولعل استغلال المدرسة الثانوية الصناعية للفرص الموجودة بالبيئة الخارجية المحيطة في المدرسة الثانوية الصناعية، يعد بمثابة طوق النجاة التي على المدرسة التمسك بها؛ للتغلب على نقاط ضعفها، ومواجهة ما يواجهها من تهديدات.

وبالنظر إلى ما سبق، يمكن تلخيص أهم الفرص المتاحة بالبيئة الخارجية للمدرسة الثانوية الصناعية فيما يلي:

- وجود بعض الفرص التي تهيئ للمدرسة الثانوية الصناعية التخطيط للحفاظ على أمنها المعلوماتي كما ورد في الخطة الإستراتيجية لتطوير التعليم قبل الجامعي، عن طريق استكمال البنية التحتية، والأجهزة اللازمة للحفاظ على البيانات والمعلومات الموجودة في المدرسة.
- تشريع عدد من القوانين، مثل قانون الحفاظ على الفضاء المعلوماتي كنوع من التمهيد والتخطيط للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية على غرار مثيلاتها من المؤسسات الأخرى.
- تحقيق قدر من الاتصال والتنسيق بين عدد من الوزارات لتقديم تدريب متخصص في مجال تكنولوجيا المعلومات والاتصالات، وبالتالي التمكن من الحفاظ على الأمن المعلوماتي.
- توفير مؤشرات قدمتها اليونسكو يمكن الحكم بها على قدرة المدرسة الثانوية الصناعية على الحفاظ على الأمن المعلوماتي بها.

رابعًا ـ التهديدات المرتبطة بإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية: Threats (T)

تتمثل أهم التهديدات المرتبطة بحفاظ المدرسة الثانوية الصناعية على أمنها المعلوماتي فيما يلي: (95)

- لا توجد قواعد بيانات صحيحة وموثقة تحدد احتياجات سوق العمل من المهن والتخصصات المختلفة بالتعليم الفني.
- ضعف فاعلية تطوير التعليم الفني؛ إذ إن آليات سوق العمل تتغير وتتطور بسرعة تفوق تطور إمكانات ومخرجات التعليم الفني، مما أدى إلى التباين الواضح بين معدل كفاءة الخريجين، ومعدل الصلاحية الفعلية لسد متطلبات سوق العمل.
- عدم وجود دراسات واقعية ومتكاملة لحالة ومتطلبات أسواق العمل العربية من العمالة المؤهلة والماهرة، سواء على المدى القريب أو المدى البعيد.
- جهود التدريب ما تزال مبعثرة، وتتفاوت نظمها وطاقاتها وتخصصاتها ومناهجها بين البلدان العربية.
- ضعف الميزانيات المخصصة لتجهيز المدارس الفنية ومراكز التدريب بالمعامل والمعدات اللازمة التي تخدم المناهج والبرامج، بما يحقق متطلبات سوق العمل، ويساير التطور التكنولوجي.
- عزوف القطاع الخاص عن تقديم فرص تدريب كافية للدارسين للتدريب العملي في المصانع والشركات والقطاعات الاقتصادية المختلفة، بما يمكنهم من اكتساب مهارات وجدارات فعلية على أرض الواقع وإكسابهم ثقافة العمل واحترامه.
- افتقار العديد من برامج التدريب بالتعليم الفني إلى وثاقة الصلة باحتياجات سوق العمل، ومتطلبات عصر التكنولوجيا الحديثة.

يضاف إلى ما سبق، نقاط الضعف التالية: [96]

- قلة الموارد، وعدم الاتساق مع متطلبات سوق العمل.
- وجود عدد من المهن المستحدثة التي لا تجد من يشغلها.
- عدم وجود خطة حالية أو مستقبلية يعول عليها مخططو التعليم في تحديد ما هو مطلوب من مهن وتخصصات في سوق العمل من جهة، مع عدم وجود توصيف دقيق للمهن لدى المختصين من جهة أخرى.

مما سبق الإشارة إليه في تلك الدراسة، يتضح أن ضعف الموارد، سواء كانت مادية أو بشرية تعتبر العائق الأساسي الذي يقف حائلًا في سبيل القيام ببناء قواعد

البيانات، وبالتالي تضيع البيانات الهامة، ويصعب استرجاعها وقت الحاجة، فلا تستطيع المدرسة اتخاذ القرارات اللازمة لمواجهة الأزمات أو التعافي منها، أو الاتصال للمشاركة مع جماعات المصالح أو المستفيدين، أو حتى التواصل مع المدارس الأخرى لتبادل الخبرة، بدون توافر الموارد المطلوبة، بل ومع استحداث الوحدات الجديدة في المدارس الثانوية الصناعية، أصبح من الضروري وجود متخصصين لشغل وظائف المسئولين عن تلك الوحدات، على أن يكونوا مؤهلين للقيام بالمهام الموكلة إليهم، الأمر الذي يسهم في وجود خطط محددة ومدروسة تسهم في تحقيق الأمن المطلوب، والمهام الموكلة للمدرسة الثانوية الصناعية بشكل عام.

بالنظر إلى ما سبق، واتساقًا مع محاور البحث وعمليات إدارة الأمن المعلوماتي المختارة، والإطار النظري للبحث، والتهديدات سالفة الذكر، يمكن تلخيص أهم التهديدات الموجودة بالبيئة الخارجية للمدرسة الثانوية الصناعية فيما يلي:

- غياب التخطيط للأمن المعلوماتي على مستوى المديريات التعليمية، بل على مستوى الوزارة ككل، ويرجع ذلك إلى ضعف قواعد البيانات المتوفرة عن المدارس بالوزارة والمديريات، الأمر الذي يستحيل معه القيام بتخطيط سليم تحسبًا للظروف المستقبلية.
- غياب الخطط المستقبلية التي عن طريقها تحدد الوزارة والمديريات والإدارات التعليمية المهن المتاحة بسوق العمل الخارجي فيما يخص تخصصات خريجي التعليم الثانوي الصناعي.
- ضعف القدرة على الاتصال بين الجهات المعنية بتحقيق الأمن المعلوماتي للمدارس الثانوية الصناعية، كشركات الصيانة والبرامج الأصلية، وجهات التدريب، ووزارة التربية والتعليم، والمديريات التعليمية، والإدارات، نظرًا لعدم وجود قاعدة بيانات تحدد الجهات اللازم الاتصال بها عند الحاجة، وإن وجدت فلا تكون دقيقة، ولا يتم تحديثها.
- ضعف مستوى البرامج التدريبية المقدمة للمسئولين عن الحفاظ عن الأمن المعلوماتي في المدرسة من ناحية، والبرامج المقدمة لمديري المدارس الثانوية الصناعية من ناحية أخرى، مما يجعل مدير المدرسة الثانوية الصناعية على

غير دراية بأهمية الحفاظ على الأمن المعلوماتي في المدرسة، وكيفية الحفاظ عليه.

- غياب البرامج التقويمية التي تساعد المدرسة على تحديد مستواها وقدرتها على الحفاظ على الأمن المعلوماتي بها، مما ينعكس على عدم وجود خطة تقويمية لأداء المدرسة في هذا الصدد.

القسم الرابع ـ تصميم جدول التحليل الرباعي للخروج بإستراتيجيات لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر:

في ضوء ما أسفرت عنه الدراسة النظرية لواقع الحفاظ على الأمن المعلوماتي في المدرسة الثانوية الفنية الصناعية في جمهورية مصر العربية من عناصر قوة وضعف بالبيئة الداخلية للمدرسة، وفرص وتهديدات بالبيئة الخارجية لها، يمكن تصميم جدول التحليل الرباعي، والذي يمثل مصفوفة (Matrix) لتجميع تلك العناصر الأربعة للتحليل البيئي، والمزاوجة بينها؛ للخروج بمجموعة من الإستراتيجيات التي تساعد في صياغة إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الفنية الصناعية في جمهورية مصر العربية، ويتضح ذلك من خلال الجدول التالي:

جدول رقم (2) التحليل الرباعي لعناصر البيئة الداخلية والخارجية للمدرسة الثانوية الصناعية

	تحليل البيئة الداخلية	
	عناصر القوة (Strengths)	**عناصر الضعف (Weaknesses)**
تحليل البيئة الداخلية	1. تهدف الخطة الإستراتيجية للتعليم قبل الجامعي ـ فيما يخص التعليم الفني ـ إلى إتاحة التجهيزات وتكنولوجيا التعليم بما يتناسب مع نوعية التعليم الفني وعدد الطلاب، وفق معايير معدة لذلك، بالإضافة إلى استكمال	1. ضعف مشاركة أصحاب المصلحة والمستفيدين الحقيقيين من مخرجات التعليم والتدريب في المدرسة، في صياغة مواصفات المهن المختلفة، والتوصيف الوظيفي للعاملين، ووضع المناهج والبرامج الدراسية، والاشتراك

	التجهيزات والبنية التحتية اللازمة للمدارس، وتوفير البنية التحتية والإمكانات المادية والبشرية، والآلات والعدد، والخامات، والبرامج التدريبية، لتفعيل العملية التعليمية في المدارس. 2. وجود بعض الوحدات المدرسية داخل المدارس بشكل عام، ومنها وحدة المعلومات والإحصاء. 3. وجود وحدة مدرسية جديدة في المدرسة الثانوية الفنية، أطلق عليها وحدة معلومات سوق العمل. 4. التحديد الدقيق لمسئوليات العاملين في بعض الوحدات المدرسية المسئولة عن المعلومات الموجودة في المدرسة كوحدة التوظيف في المدرسة الثانوية الفنية. 5. يضاف إلى ما سبق تحديد واجبات المسئول عن وحدة ريادة الأعمال في المدرسة الثانوية الفنية. 6. التحديد الدقيق للوصف الوظيفي لمسئول الإرشاد	في عمليات المتابعة والتقويم. 2. عدم وجود آلية محددة ومدروسة لتمويل عمليات التدريب المختلفة، سواء للتدريب الأساسي، أو التدريب أثناء الخدمة، أو ما قبل الخدمة. 3. ضعف اعتماد البرامج التدريبية على معرفة الاحتياجات التدريبية الفعلية، وبالتالي ضعف إعداد برامج تدريبية قائمة على الاحتياجات الحقيقية للأفراد. 4. عدم توافر قاعدة بيانات دقيقة توضح البرامج التدريبية ومدى تواصلها، وأعداد المستفيدين منها وأنواعها. 5. انخفاض مستوى أداء الإدارة المدرسية في بعض مدارس التعليم الفني، وضعف جهاز التوجيه. 6. غلبة أسلوب الإدارة المدرسية بمفهوم الإدارة والضبط على مفهوم التوجيه والمشاركة في المسئولية، مما جعل النظام الإداري يمثل عبئًا على كاهل المعلم، واتساع الفجوة بين

	والتوجيه المهني، وتعتبر وحدة الإرشاد والتوجيه المهني إحدى الوحدات المستحدثة في المدارس الثانوية الفنية بوجه عام. 7. وفي إطار المبادرة المصرية الشاملة لتطوير التعليم، يتمثل الغرض من مشروع تطوير التعليم الفني باستخدام تكنولوجيا المعلومات والاتصالات، في الارتقاء بالتعليم الفني والتدريب المهني وتعزيزه، من خلال استخدام أنظمة تكنولوجيا المعلومات والاتصالات. 8. تحديث 10 مدارس مهنية متقدمة في نواحي البنية التحتية لتكنولوجيا المعلومات والاتصالات والمناهج التعليمية وبناء قدرات التنمية البشرية، مما انعكس إيجابًا على القدرة التكنولوجية لكل مدرسة.	النظام الإداري، والنظام التعليمي. 7. ضعف وجود صف ثان من القيادات. 8. ضعف قدرات معظم مديري التعليم الفني الصناعي. 9. نظام استلام المعدات بشكل عهدة يحولها من تقنية إلى مقتنى، مما يؤثر على استخدامها بوصفها معدات يمكن أن تفسد أو تتلف من الاستخدام. 10. ضيق مساحة بعض الأقسام والمعامل وقلة الخامات والأدوات. 11. سوء حالة بعض المباني والمرافق ببعض المدارس الفنية، وحاجتها لعمليات صيانة شاملة أو إحلال وتجديد. 12. وجود بعض الآلات والمعدات والأدوات الفنية الخاصة بالعملية التعليمية والتدريبية التي تحتاج إلى إصلاح وصيانة، وقد يتعذر ذلك بسبب عدم وجود عقود صيانة لها، بالإضافة إلى

		عدم توافر قطع الغيار اللازمة لها، مما يجعلها معطلة دون الاستفادة منها. 13. عدم توفر الحماية الأمنية للمدارس الفنية لتأمين الآلات والماكينات والعدد والبيانات والمعلومات من السرقة. 14. ضعف تسويق المنتجات لقلة عدد المعارض المتاحة. 15. قصور الاستفادة من الموارد المتاحة، سواء في ذلك البشرية، والمادية. 16. قصور المعلومات الحقيقية عن سوق العمل. 17. ضعف البنية التحتية لشبكة المعلومات بمدارس التعليم الثانوي الصناعي. 18. سوء مرافق التعليم الثانوي الصناعي والبنية الأساسية للاتصالات وتكنولوجيا المعلومات. 19. محدودية التعاون بين المدارس الثانوية الفنية الصناعية والبيئة المحيطة. 20. عدم وجود قاعدة بيانات تخص التعليم الفني الصناعي.

	الفرص (Opportunities)	التهديدات (Threats)
تحليل البيئة الخارجية	1. قامت وزارة التربية والتعليم بالتعاون مع وزارة الاتصالات بعمل الشبكة الداخلية للمدارس؛ لربط جميع أجهزة الحاسب بشبكة واحدة وربطها بالشبكة المعلوماتية الدولية. 2. قامت وزارة الاتصالات وتكنولوجيا المعلومات بعمل مشروع قانون أمن الفضاء المعلوماتي. 3. إنشاء جهاز قومي للرقابة على جميع أعمال أمن المعلومات، ومنح تراخيص مزاولة أعمال الخبرة في هذا المجال. 4. كما وضعت منظمة اليونسكو عددًا من المؤشرات التي يمكن استخدامها للحكم على قدرة المؤسسات التعليمية في استخدام تكنولوجيا المعلومات. 5. أعدت وزارة التربية والتعليم ـ من خلال قطاع التعليم الفني بها ـ قواعد بيانات مختلفة، تمهيدًا لعقد مؤتمرها التقني الأول والثاني من أجل ربط التعليم الفني ـ بمختلف تخصصاته ـ بسوق العمل.	1. لا توجد قواعد بيانات صحيحة وموثقة تحدد احتياجات سوق العمل من المهن والتخصصات المختلفة بالتعليم الفني. 2. ضعف فاعلية تطوير التعليم الفني، إذ إن آليات سوق العمل تتغير وتتطور بسرعة تفوق تطور إمكانات ومخرجات التعليم الفني؛ مما أدى إلى التباين الواضح بين معدل كفاءة الخريجين، ومعدل الصلاحية الفعلية لسد متطلبات سوق العمل. 3. عدم وجود دراسات واقعية ومتكاملة لحالة ومتطلبات أسواق العمل العربية من العمالة المؤهلة والماهرة، سواء على المدى القريب أو المدى البعيد. 4. جهود التدريب ما تزال مبعثرة، وتتفاوت نظمها وطاقاتها وتخصصاتها ومناهجها بين البلدان العربية. 5. ضعف الميزانيات المخصصة لتجهيز المدارس الفنية ومراكز التدريب بالمعامل والمعدات اللازمة التي تخدم المناهج

	6. كما يمكن إضافة الفرص التالية، وذلك من خلال توجهات وزارة التربية والتعليم لتطوير التعليم الفني، والتي ظهرت من خلال عرض الأهداف الإستراتيجية، والتي من أهمها ما يلي: • إتاحة التجهيزات وتكنولوجيا التعليم بما يتناسب مع نوعية التعليم الفني وعدد الطلاب وفق معايير معدة لذلك. • ربط التعليم الفني بمؤسسات الإنتاج والخدمات في البيئة المحيطة لتدريب الطلاب في هذه المؤسسات الإنتاجية. • التعاون مع الشركات وأصحاب الأعمال من أجل تطوير التعليم الفني ليتماشى مع التحديات الكبيرة التي تفرضها المنافسة العالمية في الحاضر والمستقبل، وكذلك من أجل إمداد أصحاب الأعمال	والبرامج، بما يحقق متطلبات سوق العمل، ويساير التطور التكنولوجي. 6. عزوف القطاع الخاص عن تقديم فرص تدريب كافية للدارسين للتدريب العملي في المصانع والشركات والقطاعات الاقتصادية المختلفة، مما يمكنهم من اكتساب مهارات وجدارات فعلية على أرض الواقع وإكسابهم ثقافة العمل واحترامه. 7. افتقار العديد من برامج التدريب بالتعليم الفني إلى وثاقة الصلة باحتياجات سوق العمل، ومتطلبات عصر التكنولوجيا الحديثة. 8. قلة قدرات الموارد البشرية، وعدم اتساقها مع متطلبات سوق العمل. 9. وجود عدد من المهن المستحدثة التي لا تجد من يشغلها. 10. عدم وجود خطة حالية أو مستقبلية يعول مخططو التعليم في تحديد ما هو مطلوب من مهن وتخصصات في سوق العمل من جهة، مع عدم وجود

	بخريجين ذوي مهارة ومؤهلات يتطلبها سوق العمل. 7. وجدير بالذكر في هذا السياق، بعض جهود الشراكة المجتمعية للإسهام في دعم التعليم الفني، ومنها ما يلي: • التعاون مع وزارة الإعلام لتخريج العمالة الفنية المدربة في مجال الإلكترونيات. • التعاون مع وزارة البترول لتخريج العمالة الفنية المدربة في مجال تكنولوجيا البترول. • توقيع اتفاقية مع مؤسسة مصر الخير تهدف إلى تأهيل خريجي المدارس الفنية ومساعدتهم ماديًّا على إنشاء مشروعات صغيرة في مجال تخصصهم الدراسي وإدارتها، وتحسين كفاءة الإدارة المدرسية والتوجيه الفني والمعلمين بالتعليم الفني الصناعي. • توقيع اتفاقية تعاون مع	توصيف دقيق للمهن لدى المختصين من جهة أخرى.

	كلية الهندسة بجامعة قناة السويس لتدريب المعلمين والطلاب والموجهين في المحافظات الداخلة في النطاق الإقليمي لجامعة قناة السويس. • التعاون مع الهيئة القومية للاتصالات السلكية واللا سلكية لتخريج العمالة الفنية المدربة في المجالات التالية (سنترالات إلكترونية ـ تراسل ـ فني اتصالات شبكات ـ فني اتصالات قوى كهربية ـ تكييف ـ حاسبات). 8. وجود خطة إستراتيجية قومية لتطوير التعليم الفني في جمهورية مصر العربية. 9. كما يعتبر مركز التطوير التكنولوجي، ـ الذي تم إنشاؤه لإدخال التكنولوجيا المتطورة، وتنويع مصادر المعرفة في مجال التعليم ـ أحد الفرص المتاحة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية. 10. تولى المعهد القومي	

	للاتصالات بالتنسيق مع وزارة الاتصالات والمعلومات ووزارة التربية والتعليم منذ عام 2002 الإشراف على البرنامج القومي الخاص بالتدريب المتخصص في مجال تكنولوجيا المعلومات والاتصالات، وقد تم تنفيذ الدورات التدريبية من خلال مجموعة من الشركات العالمية من أجل تدريب متخصصين في مجال تكنولوجيا المعلومات بواقع 5000 متخصص سنويًّا في مجالات متعددة.	

وقد تضمن تحليل البيئة الداخلية للمدرسة الثانوية الصناعية في جمهورية مصر العربية، والبيئة الخارجية المحيطة بها تطبيق استمارة التحليل الإستراتيجي على عدد من الخبراء في مجال التعليم الفني الصناعي؛ لاستطلاع آرائهم حول عبارات الاستمارة، وتحليل البيئة الداخلية والخارجية، وتضمنت العينة في مجملها (25) فردًا؛ منهم (4) أساتذة جامعات، (4) من المسئولين عن التعليم الفني الصناعي بمديرية التربية والتعليم بالقاهرة، و(8) من الأساتذة العاملين بشعبة التعليم الفني بالمركز القومي للبحوث التربوية والتنمية، و(7) من الأساتذة العاملين بقطاع التعليم الفني التابع لوزارة التربية والتعليم، و(2) من العاملين بالإدارة العامة لمركز تطوير التعليم الفني، وتضمنت الاستمارة ما يلي:

1- محور نقاط القوة، ويشمل ما يوجد في المدرسة الثانوية الصناعية ويؤثر فيها إيجابيًّا، ومحور جوانب الضعف، ويشمل ما يوجد في المدرسة الثانوية الصناعية ويؤثر سلبًا على قدرتها على الحفاظ على أمنها المعلوماتي.

2- محور الفرص التي يمكن الاستفادة منها، ومحور التهديدات التي يجب التعامل معها ومواجهة تأثيرها السلبي، وذلك في البيئة الخارجية للمدرسة، والذي يدعم أو يهدد قدرة المدرسة على الحفاظ على أمنها المعلوماتي.

3- مدى التأثير، ويعبر عن درجة تأثير العنصر على عمليات إدارة الأمن المعلوماتي في المدرسة الثانوية الصناعي، وتتراوح القيمة بين (1 ـ 5)؛ حيث تمثل (5) الأثر الأعلى، و(1) تبين مستوى التأثير الأضعف.

4- احتمالية الحدوث (بالنسبة للفرص والتهديدات)، ويعبر عن مدى إمكانية الحدوث، وتتراوح القيمة بين (1 ـ 10)؛ حيث تمثل (10) الاحتمالية الأعلى للحدوث، والدرجة (1) الاحتمالية الأقل للحدوث.

5- درجة التواجد (بالنسبة لنقاط القوة والضعف)، وتتراوح القيمة من (1 ـ 10)؛ حيث تمثل الدرجة (10) درجة التواجد، بينما تعبر الدرجة (1) عن الدرجة الأقل للتواجد.

التحليل الإحصائي:

1- متوسط الوزن النسبي لجوانب القوة والضعف = (متوسط مدى التأثير × متوسط درجة التواجد)

2- متوسط الوزن النسبي للفرص والتهديدات = (متوسط مدى التأثير × متوسط احتمالية الحدوث)

3- تم الاعتماد في التحليل الإحصائي للاستجابات على المتوسط الحسابي (لمدى التأثير، واحتمال الحدوث، ودرجة التواجد) وفق المعادلة التالية: [97]

$$\frac{\text{مجموع درجات الاستجابات}}{\text{عدد أفراد العينة}}$$

وتم ترتيب العبارات تنازليًّا وفق متوسط الوزن النسبي، كما سيتضح فيما يلي:

أولًا ـ تحليل عناصر البيئة الداخلية:

1. جوانب القوة:

جدول رقم (3) جدول الأوزان النسبية لعناصر القوة

م	العبـــــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
1	توافر التجهيزات المادية في المدرسة؛ مما يساعدها في الحفاظ على أمنها المعلوماتي.	107	4.28	172	6.88	29.45	2
2	توافر الإمكانيّات البشرية المدربة للتعامل مع التكنولوجيا الحديثة؛ مما يسهم في إدارة عمليات الأمن المعلوماتي في المدرسة.	111	4.44	177	7.08	31.44	1
3	تدريب	101	4.04	168	6.72	27.14	4

م	العبـــــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
	العاملين في المدرسة تدريبًا مستمرًا؛ الأمر الذي يساعدهم على إدارة عمليات الأمن المعلوماتي.						
4	وجود وحدة للمعلومات والإحصاء في المدرسة، تتولى مسئولية الحفاظ على الأمن المعلوماتي.	102	4.08	165	6.6	26.93	5
5	وجود بطاقات توصيف وظيفي	92	3.68	151	6.04	22.22	7

م	العبـــــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
	للمسئولين في وحدة المعلومات والإحصاء، تحدد ما يجب عليهم القيام به للحفاظ على الأمن المعلوماتي.						
6	ارتباط العمل في وحدة التوظيف في المدرسة بوجود إدارة للأمن المعلوماتي بها.	86	3.44	137	5.48	18.85	10
7	حاجة وحدة ريادة الأعمال في المدرسة إلى إدارة	88	3.52	144	5.76	20.28	9

م	العبـــــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
	للأمن المعلوماتي بها.						
8	حاجة وحدة الإرشاد والتوجيه المهني في المدرسة إلى إدارة للأمن المعلوماتي بها.	90	3.6	145	5.8	20.88	8
9	قيام وزارة التربية والتعليم بالتعاون مع وزارة الاتصالات بعمل شبكة داخلية للمدارس؛ لربط جميع أجهزة الحاسب	106	4.24	162	6.48	27.48	3

م	العبـــــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
	بشبكة واحدة، وربطها بالشبكة المعلوماتية الدولية.						
10	توجه المدارس الثانوية الصناعية للأخذ بنظام المعلومات الإدارية.	96	3.84	156	6.24	23.97	6
	مجموع متوسطات الوزن النسبي					**248.6**	

يتضح من الجدول السابق، أن جميع عناصر القوة التي وردت في الجدول لها تأثير كبير على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في جمهورية مصر العربية؛ حيث إن متوسط درجة التأثير لها أكبر من (2.5)، ومتوسط درجة تواجدها أكبر من (5)، وبالتالي فهي تعتبر من العناصر المؤثرة التي يجب الاستفادة منها في بناء جدول التحليل الرباعي، ويرجع السبب في ذلك إلى توجهات الخطة الإستراتيجية للتعليم في مصر لإجراء المزيد من الإصلاحات في قطاعات التعليم كافة من ناحية، وفي قطاع التعليم الفني على وجه الخصوص، إذ حاز عنصر (تجهيز المدارس بوسائل التكنولوجيا الحديثة، والتدريب المستمر على استخدام تلك التكنولوجيا) على النصيب الأكبر من توجهات الوزارة في الآونة الأخيرة،

كما أن وجود عدد من الوحدات المستحدثة ـ كوحدة الإحصاء والمعلومات، والإرشاد والتوجيه المهني، والتوظيف ـ كان لها أثر لا يمكن إغفاله على إدارة عمليات الأمن المعلوماتي، والحفاظ على المعلومات التي تحتاجها المدرسة ـ باختلاف أنواعها ـ من الضياع، واستعادتها وقت الحاجة إليها.

ويمكن للمدرسة الثانوية الصناعية أن تستفيد من تلك النقاط وتدعمها، من خلال الاستمرار في تجهيز المدارس بالتجهيزات الملائمة، التي تستخدم لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية، وإتاحة فرص أكثر في التدريب المتخصص على إدارة عمليات الأمن المعلوماتي في المدرسة للمدير، والإداريين المسئولين عن حفظ المعلومات، والاحتفاظ بها في مختلف الوحدات المدرسية، بالإضافة إلى ضرورة عقد المزيد من بروتوكولات التعاون بين وزارة التربية والتعليم وغيرها من الوزارات المختلفة؛ للمساهمة في بناء نظام للمعلومات، والحفاظ عليه.

2. جوانب الضعف:

جدول رقم (4) جدول الأوزان النسبية لعناصر الضعف.

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
1	انخفاض مستوى أداء العاملين بإدارة المدرسة.	101	4.04	170	6.8	24.72	16
2	عملية التخطيط للأمن المعلوماتي في المدرسة عملية فردية وليست مؤسسية.	102	4.08	175	7	28.56	5
3	ضعف قدرات معظم مديري المدارس على إعداد صف ثان من القيادات، يساعدهم في إدارة عمليات الأمن المعلوماتي في المدرسة.	103	4.12	179	7.16	29.50	2
4	قلة توافر البرامج التكنولوجية المتنوعة اللازمة لإدارة الأمن المعلوماتي في المدرسة.	100	4	167	6.68	26.72	9
5	المكان المخصص لوحدة المعلومات والإحصاء في المدرسة غير مؤمن.	100	4	154	6.16	24.64	17
6	الثقافة التنظيمية في المدرسة لا تدعم تحقيق أهداف إدارة الأمن المعلوماتي.	102	4.08	178	7.12	29.05	3

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
7	ضعف القدرة على الاستخدام الأمثل للأجهزة التكنولوجية المستخدمة في الحفاظ على المعلومات.	99	3.96	160	6.4	25.34	12
8	تتسم التوصيفات للمهن والوظائف بالوحدات المدرسية المستحدثة بالعمومية، وعدم الدقة.	97	3.88	160	6.4	24.33	18
9	ضيق مساحة بعض الأقسام والمعامل، وقلة الخامات والأدوات؛ الأمر الذي يؤثر على قدرة العاملين في إدارة عمليات الأمن المعلوماتي.	91	3.64	176	7.04	25.63	11
10	تدني مستوى البنية التحتية والأساسية للاتصالات وتكنولوجيا المعلومات في المدرسة.	102	4.08	167	6.68	27.25	7
11	ضعف الحماية والتأمين اللازمين في المدرسة للحفاظ على البيانات والمعلومات من السرقة.	100	4	172	6.9	27.6	6
12	ندرة وجود عقود صيانة بين المدرسة والشركات المسئولة؛ مما ينتج عنه تعذر صيانة الأجهزة.	96	3.84	170	6.8	26.11	10
13	ضعف قواعد البيانات التي يمكن من خلالها توفير المعلومات الكاملة والدقيقة عن سوق العمل للمدرسة.	105	4.2	182	7.28	30.58	1
14	قلة المعلومات اللازمة لتسويق المنتجات المدرسية للمجتمع الخارجي.	97	3.88	162	6.48	25.14	13
15	محدودية التعاون بين المدارس الثانوية الفنية الصناعية ومؤسسات المجتمع المحلي؛ نظرًا لغياب قواعد البيانات والمعلومات التي يمكن من خلالها تحديد مجالات الاستفادة.	100	4	180	7.2	28.8	4
16	غياب الوعي لدى أعضاء المدرسة الثانوية الصناعية بأهمية أمن المعلومات.	92	3.68	169	6.76	24.88	14
17	توجه المدارس والوزارة نحو حل المشكلات	101	4.04	166	6.64	26.82	8

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الاستمرارية	متوسط احتمال الاستمرارية	متوسط الوزن النسبي	الترتيب
	الخاصة باختراق المعلومات بعد حدوثها، وليس التخطيط لتفادي حصول المشكلة من الأساس.						
18	لا يتم تدريب العاملين في الوحدات المدرسية المستحدثة على القيام بمهامهم الجديدة في الحفاظ على الأمن المعلوماتي للمدرسة.	92	3.68	168	6.72	24.73	15
مجموع متوسطات الوزن النسبي = 480.4							

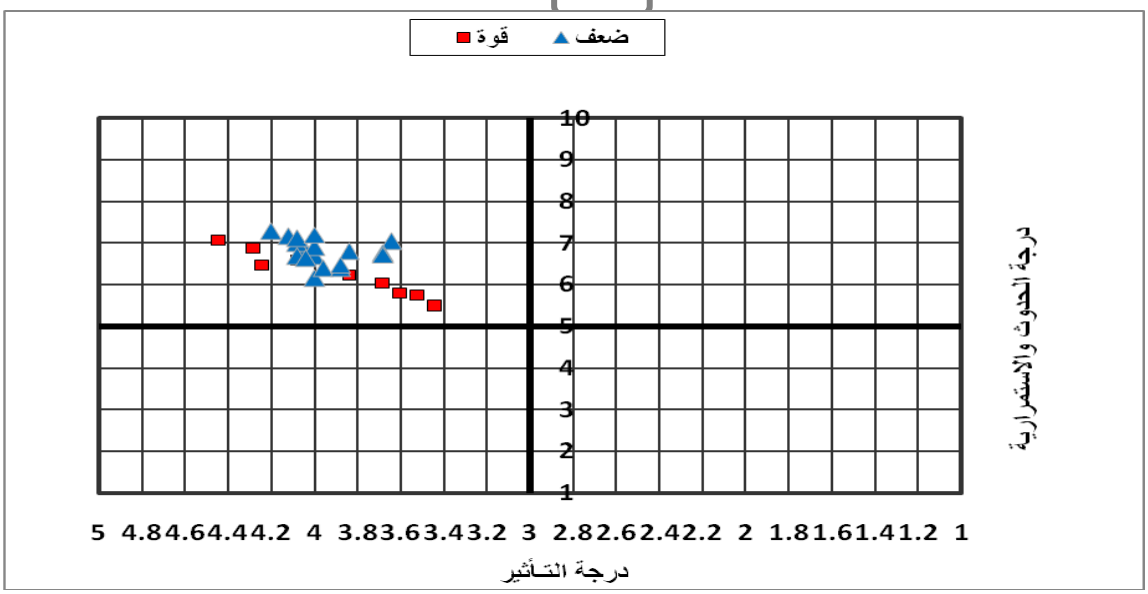
ويتضح من الجدول السابق أن جميع عناصر الضعف التي وردت في الجدول لها تأثير كبير على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر؛ حيث إن متوسط درجة التأثير لها أكبر من (2.5)، ومتوسط درجة تواجدها أكبر من (5)؛ مما يشير إلى وجود الكثير من أوجه القصور في المدرسة الثانوية الصناعية، والذي قد يحول بينها وبين تحقيق الأمن المعلوماتي المنشود، وعلى الرغم من ذلك، فقد رأى أفراد العينة أن هناك عناصر ضعف قد تكون أقل تأثيرًا على تحقيق الأمن المعلوماتي؛ ومن هنا فإنه يمكن تجاهلها، نظرًا لضعف تأثيرها.

وعلى الرغم من ذلك هناك العديد من أوجه القصور في البيئة الداخلية للمدرسة الثانوية الصناعية التي قد تحول دون حفاظها على أمنها المعلوماتي، ممَّا يجعل تعافيها من الأزمات أمرًا صعبًا، وقد اتضح ذلك من استجابات أفراد العينة لنقاط الضعف المحددة بالاستمارة، والتي تعود في معظمها إلى حداثة التوجه نحو إصلاح التعليم الفني بوجه عام، والتعليم الثانوي الصناعي على وجه الخصوص، وعدم اكتمال التجهيزات التكنولوجية اللازمة لجميع المدارس، بما يساعدها على الحفاظ على أمنها المعلوماتي، وقلة وعي المديرين والإداريين بأهمية الاستعداد للأزمات والتخطيط لها قبل حدوثها، وخصوصًا المشكلات الخاصة باختراق المعلومات وسرقتها، كما أن قلة المعلومات، وضعف قواعد البيانات تعتبر في حد ذاتها عائقًا آخر، كما أن ضعف فرص صيانة الأجهزة، وضعف البنية التحتية لبعض المدارس يمثل عائقًا آخر؛ وقد يرجع ذلك إلى عدم امتلاك الهيئات المسئولة لخريطة

زمنية يمكن عن طريقها تحديد موعد الانتهاء من تجهيز المدارس باحتياجاتها التكنولوجية اللازمة كافة؛ للحفاظ على أمنها المعلوماتي، كما أن الاهتمام بمناطق على حساب أخرى، قد يجعل من بعض المدارس الثانوية الصناعية بيئة ملائمة لتحقيق الأمن المعلوماتي، وأخرى غير قادرة على تحقيق هذا الأمر، كما أن الانفصال، وعدم التنسيق، ومحدودية الاتصال، وغياب الخطط التعاونية ـ التي تحدد مجالات الاتصال والاستفادة ـ بين وزارة التربية والتعليم، والوزارات الأخرى، ومؤسسات المجتمع المدني، والهيئات الخاصة قد تكون سببًا واضحًا في ضعف قدرة المدارس على إدارة عمليات الأمن المعلوماتي بها، كما أن المفهوم الخطأ لدى مدير المدرسة عن مهامه، واعتبار ذاته المسئول الوحيد عن التخطيط لجميع مهام المدرسة ـ ومنها إدارة عمليات الأمن المعلوماتي ـ يجعل العاملين يشعرون بالانفصال عن المدرسة، ولا يشعرون بدورهم داخلها، إلا في كونهم تقع عليهم مسئولية تنفيذ الأوامر.

3. **تحليل التوازن بين جوانب القوة والضعف:**

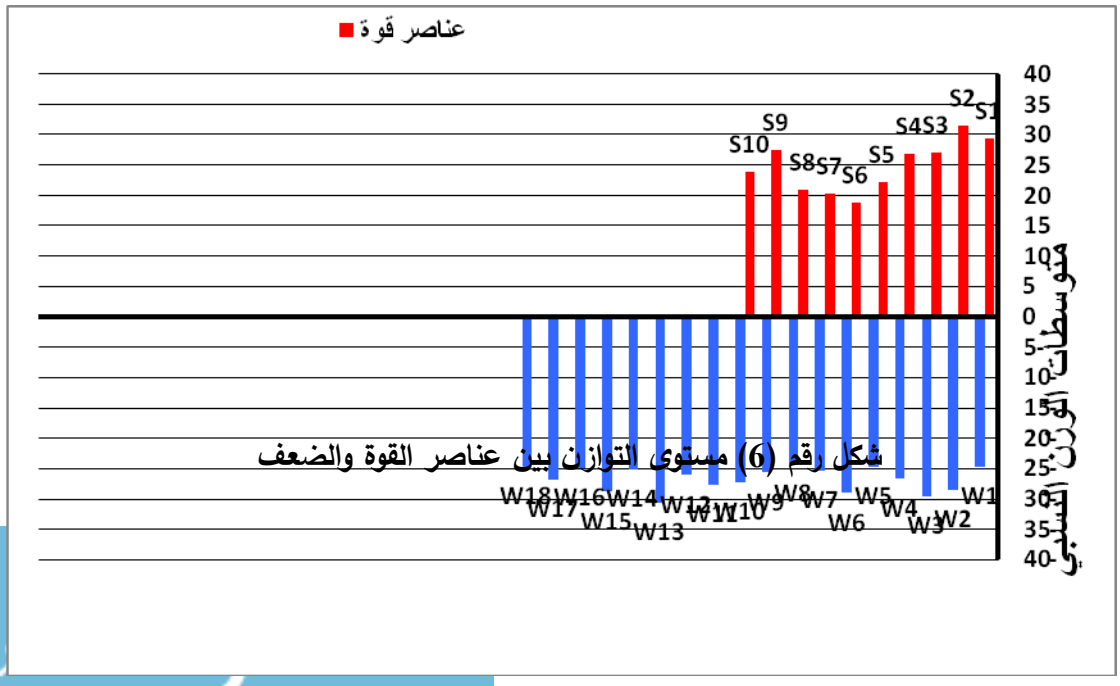
يتضح مما سبق، أن مجموع متوسطات الوزن النسبي لجوانب القوة (248.6)، ومجموع متوسطات الوزن النسبي لجوانب الضعف (480.4)، وعليه، يتضح أن مجموع متوسطات الوزن النسبي لجوانب الضعف أكبر من مجموع متوسطات الوزن النسبي لجوانب القوة، ممَّا يوضح أن واقع إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر يعاني الكثير من أوجه القصور التي يجب التغلب عليها؛ وذلك حتى تكون المدرسة قادرة على الحفاظ على المعلومات الخاصة بها، واستعادتها وقت الحاجة إليها، وربما يرجع ذلك إلى ضعف الإمكانات المادية، والبشرية، وعدم اكتمال توجهات الخطة الإستراتيجية المنشودة الموضوعة من قبل الوزارة، وتطبيقها على أرض الواقع.



شكل رقم (5) موقع عناصر القوة والضعف وفق الوزن النسبي.

يتضح من الشكل السابق أن جميع عناصر القوة والضعف تقع في المربع الرابع؛ مما يعني أن درجة تأثيرها كبير، ودرجة استمراريتها عالية.

ويوضح الشكل التالي، مستوى التوازن بين عناصر القوة والضعف التي لها تأثير على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، بحيث يمثل الاتجاه الأعلى نقاط القوة، والاتجاه الأدنى نقاط الضعف، كما هو موضح بالشكل التالي:



شكل رقم (6) مستوى التوازن بين عناصر القوة والضعف

يتضح من الشكل السابق، أن عناصر الضعف التي تؤثر على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية أكثر من عناصر القوة التي تدعم وجود إدارة فعالة للأمن المعلوماتي؛ مما يوضح أن نسبة تأثير عناصر الضعف ودرجة تواجدها أكبر من نسبة تأثير عناصر القوة، ودرجة تواجدها.

ثانيًا: تحليل عناصر البيئة الخارجية:

1. الفرص:

جدول رقم (5) الأوزان النسبية للفرص

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الحدوث	متوسط احتمال الحدوث	متوسط الوزن النسبي	الترتيب
1	قيام وزارة الاتصالات وتكنولوجيا المعلومات بعمل مشروع قانون أمن الفضاء المعلوماتي.	99	**3.96**	162	**6.48**	**25.66**	**12**
2	إنشاء الجهاز القومي للرقابة على جميع أعمال أمن المعلومات، ومنح تراخيص مزاولة أعمال الخبرة والتخصص في هذا المجال.	106	**4.24**	172	**6.88**	**29.17**	**5**
3	وجود بعض المؤشرات للمنظمات الدولية ـ كاليونسكو ـ التي يمكن استخدامها لتقويم قدرة المؤسسات التعليمية في استخدام تكنولوجيا المعلومات.	93	**3.72**	175	**7**	**26.04**	**11**
4	سعي وزارة التربية والتعليم لعقد عدد من المؤتمرات للربط بين التعليم الفني وسوق العمل، بناءً على قواعد بيانات ومعلومات مسبقة.	101	**4.04**	172	**6.88**	**27.79**	**8**
5	تأكيد الخطة الإستراتيجية لوزارة التربية والتعليم ضرورة إتاحة التجهيزات وتكنولوجيا التعليم؛ بما يتناسب مع نوعية التعليم الفني، وعدد الطلاب وفق معايير معدة لذلك.	104	**4.16**	184	**7.36**	**30.61**	**4**
6	عقد بروتكولات تعاون بين: وزارة التربية والتعليم، والشركات، وأصحاب الأعمال من أجل تطوير التعليم الفني؛ ليتماشى مع التحديات الحالية، عن طريق إتاحة معلومات وافية ودقيقة عن الطرفين.	107	**4.28**	184	**7.36**	**31.50**	**3**
7	التوجه نحو إحداث مزيد من التعاون مع وزارة الإعلام؛ لتخريج العمالة الفنية المدربة في مجال الإلكترونيات.	91	**3.64**	153	**6.12**	**22.27**	**13**

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الحدوث	متوسط احتمال الحدوث	متوسط الوزن النسبي	الترتيب
8	توقيع اتفاقية مع مؤسسة مصر الخير، تهدف إلى تأهيل خريجي المدارس وتحسين كفاءة الإدارة المدرسية والتوجيه الفني والمعلمين في المدرسة من خلال الاعتماد على قواعد بيانات دقيقة ومحدثة.	97	**3.88**	177	**7.08**	**27.47**	**10**
9	الاتجاه نحو تحقيق مزيد من التعاون مع الهيئة القومية للاتصالات السلكية واللاسلكية؛ لتخريج العمالة الفنية المدربة في بعض المجالات.	102	**4.08**	173	**6.92**	**28.23**	**7**
10	إصدار وزارة التربية والتعليم لمجموعة من القواعد المنظمة للتعاون بين إدارة المدرسة والمؤسسات الإنتاجية، وتوفير قواعد البيانات اللازمة لذلك.	99	**3.96**	265	**10**	**39.6**	**1**
11	إنشاء مركز التطوير التكنولوجي، بهدف إدخال التكنولوجيا المتطورة في التعليم بشكل عام.	100	**4**	177	**7.08**	**28.32**	**6**
12	تولي المعهد القومي للاتصالات، بالتنسيق مع وزارتي: الاتصالات والمعلومات، ووزارة التربية والتعليم الإشراف على البرنامج القومي الخاص بالتدريب المتخصص في مجال تكنولوجيا المعلومات والاتصالات.	100	**4**	172	**6.88**	**27.52**	**9**
13	اتجاه الكثير من شركات الكمبيوتر إلى توفير برامج جديدة لبناء قواعد البيانات في المدارس، بما يساعد على تحقق أمن المعلومات في المدرسة.	112	**4.48**	179	**7.16**	**32.1**	**2**
مجموع متوسطات الوزن النسبي						**376.6**	

يتضح من الجدول السابق أن جميع الفرص التي وردت في الجدول لها تأثير كبير على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر؛ حيث إن متوسط درجة التأثير لها أكبر من (2.5)، ومتوسط احتمالية حدوثها أكبر من (5)، ممَّا يشير إلى توفر العديد من الفرص في البيئة الخارجية للمدرسة الثانوية الصناعية، والتي عليها استغلالها لإدارة عمليات الأمن المعلوماتي بها، ومن ثم يمكن الاعتماد عليها في بناء جدول التحليل الرباعي الذي يحدد الإستراتيجيات التي يمكن أن تتبعها المدرسة الثانوية الصناعية، وربما يرجع ذلك إلى ما شهده قطاع التعليم الفني من توجهات متعددة نحو الإصلاح والتطوير، ومحاولات دائمة للتخلص من

المشكلات التي تعوقه عن تحقيق أهدافه، إضافةً إلى التوجه نحو الاستفادة من الدول المتقدمة صناعيًّا، والتي اعتبرت التعليم الفني الصناعي سبيلها لتحقيق التنمية الصناعية المنشودة.

وتمثلت تلك الفرص في إنشاء الجهاز القومي للرقابة على جميع أعمال أمن المعلومات، ومنح تراخيص مزاولة أعمال الخبرة والتخصص في هذا المجال، وسعي وزارة التربية والتعليم لعقد عدد من المؤتمرات للربط بين التعليم الفني وسوق العمل، بناءً على قواعد بيانات ومعلومات مسبقة، وتأكيد الخطة الإستراتيجية لوزارة التربية والتعليم على ضرورة إتاحة التجهيزات، وتكنولوجيا التعليم بما يتناسب مع نوعية التعليم الفني وعدد الطلاب وفق معايير معدة لذلك، وإنشاء مركز التطوير التكنولوجي، بهدف إدخال التكنولوجيا المتطورة في التعليم بشكل عام، فقد رأى أفراد العينة أنها فرص يجب أن تستغلها المدرسة في سبيل تحقيق إدارة جيدة لأمنها المعلوماتي.

وعلى الرغم من وجود فرص من الممكن أن تستغلها المدرسة الثانوية الصناعية، إلا أنها فرص ضعيفة، بناءً على رأي أفراد العينة، مثل العبارات رقم 1، 3، 7، 8 ويرجع السبب في ذلك بالنسبة للعبارة رقم 1 في أن مشروع قانون أمن الفضاء المعلوماتي مازال مجرد مشروع لم يرتق إلى رحلة التطبيق إلى الآن، وعليه لم يؤت بثماره. أما بالنسبة للعبارة رقم 3، فقد يرجع السبب إلى أنها من أقل الفرص تأثيرًا في أن منظمة اليونسكو منظمة دولية، وقد تختلف المؤشرات التي تضعها عن المؤشرات التي تحتاجها المدارس الثانوية الصناعية، باعتبارها مؤسسات تعليمية تختلف طبيعتها من دولة لأخرى، ومن ثَمَّ فهي في حاجة إلى مؤشرات محلية، تضعها هيئات محلية. أما بالنسبة للعبارة رقم 7 فمن الممكن أن تكون الفرصة الأقل تأثيرًا؛ لأن وزارة الإعلام قد تكون معنية بإعداد عمالة في مجال الإلكترونيات، والعدد اللازمة لإدارة مؤسسات الإعلام، وليست معنية بإعداد الإداريين المسئولين عن إدارة عمليات الأمن المعلوماتي في المدرسة. أما بالنسبة للعبارة رقم 8 فقد تكون فرصة ضعيفة الأثر من وجهة نظر أفراد العينة؛ لأن الاتفاقيات من هذا القبيل لا تتسم بالاستمرارية، وإنما تكون اتفاقية تتعلق بأفراد معينين ومن الممكن ألا تتكرر، وبالتالي

لا تعمم الفرصة على المستفيدين منها كافة، وبالتالي يحصل البعض على فرصة دون الآخرين.

وبناءً على ما سبق، يمكن تدعيم تلك الفرص وإجراء بعض التعديلات عليها لتدعيمها، واستخدامها الاستخدام الأمثل لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

2. التهديدات:

جدول رقم (6) الأوزان النسبية للتهديدات

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الحدوث	متوسط احتمال الحدوث	متوسط الوزن النسبي	الترتيب
1	ندرة وجود قواعد البيانات الصحيحة والموثقة والمؤمنة، التي تحدد احتياجات سوق العمل من المهن والتخصصات المختلفة.	107	4.28	177	7.08	30.30	6
2	غياب المؤشرات والمعلومات عن التطورات السريعة لسوق العمل، والتي تفوق تطور إمكانيات ومخرجات التعليم الفني.	108	4.32	176	7.04	30.41	5
3	قلة وجود: الدراسات التحليلية، والبحوث العلمية، والمعلومات الدقيقة عن متطلبات سوق العمل؛ من العمالة المؤهلة، والماهرة.	103	4.12	167	6.68	27.52	12
4	ضعف تقييم خطة التدريب الموجهة للمعلمين، والعاملين، والطلاب على مستوى الوزارة، بناء على الاحتياجات التدريبية للفئة المستهدفة.	98	3.92	174	6.96	27.28	13
5	قلة الميزانيات المخصصة لتجهيز مراكز التدريب التابعة لوزارة التربية والتعليم، واللازمة لتحقيق متطلبات سوق العمل من التكنولوجيا المتطورة.	105	4.2	184	7.36	30.91	4
6	عزوف القطاع الخاص عن تقديم فرص كافية للدارسين في المدارس الفنية للتدريب العملي في: المصانع، والشركات، والقطاعات الاقتصادية المختلفة.	101	4.04	180	7.2	29.88	9
7	ضعف الخطة الحالية التي تتيح لمخططي التعليم تحديد المطلوب من المهن والتخصصات في سوق العمل، والتي تخدم تحقيق الأمن المعلوماتي في المدارس.	100	4	180	7.2	28.8	10

م	العبـــارة	مدى التأثير المحتمل	متوسط مدى التأثير	احتمال الحدوث	متوسط احتمال الحدوث	متوسط الوزن النسبي	الترتيب
8	ضعف قدرة مخططي التعليم على وضع خطط مستقبلية بناء على متطلبات المستقبل، وحاجات سوق العمل؛ نظرًا لقلة قواعد البيانات التي تساعد في تحقيق ذلك.	99	3.96	174	6.96	27.56	11
9	التغير المستمر والسريع في البرامج التي تستخدم في اختراق البيانات والمعلومات.	107	4.28	195	7.8	33.38	1
10	تدني المنظومة القيمية في المجتمع؛ مما يمثل تهديدًا لأمن المعلومات بشكل مستمر.	101	4.04	187	7.48	30.21	7
11	زيادة تكلفة برامج الحماية، وبرامج بناء قواعد البيانات.	104	4.16	190	7.6	31.61	3
12	ضعف الوعي الكافي بكيفية التعامل مع المعلومات وحساسيتها عند استخدام الشبكات الاجتماعية المنتشرة (مثل: فيس بوك، وتويتر ونحوهما).	108	4.32	190	7.6	32.83	2
13	ضعف التخطيط لبناء برنامج متكامل لأمن المعلومات بدءًا من الوزارة، وحتى المدرسة.	105	4.2	179	7.16	30.07	8
	مجموع متوسطات الوزن النسبي					390.76	

ويتضح من الجدول السابق، أن جميع التهديدات السالفة لها تأثير كبير على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية؛ حيث إن متوسط مدى التأثير لجميع العناصر أكبر من 2.5، ومتوسط احتمالية الحدوث لتلك العناصر أيضًا أكثر من (5)، ولكن هناك بعض العناصر تمثل تهديدًا أقل على إدارة عمليات الأمن المعلوماتي وفقًا للترتيب الوارد بالجدول، وعليه يمكن تجنبها بسهولة، مثل العبارات رقم 3، 4، 7، 8. فمثلًا يرجع أفراد العينة ضعف احتمالية حدوث هذه العبارة إلى إجراء المزيد من الأبحاث حول متطلبات سوق العمل في الآونة الأخيرة، ويرجع ذلك إلى وجود وحدات متخصصة تكمن مسئوليتها في معرفة تلك المتطلبات، وإمداد سوق العمل بما يحتاجه من خريجين ذوي كفاءة ومتخصصين ومؤهلين للوفاء بتلك المتطلبات، كما أن خطط التدريب الموجهة للإداريين والعاملين في المدارس الثانوية الصناعية تعد بناءً على احتياجاتهم التدريبية سواء على مستوى المدرسة، أو على مستوى الوزارة، كما أنها تتضمن التوجهات المستقبلية للتدريب، ممَّا انعكس على

تدريب المسئولين في مجال التكنولوجيا على الحفاظ على الأمن المعلوماتي للمدرسة، الأمر الذي يوضح فرص التغيير والتطوير التي طرأت على برامج التدريب في الفترة الأخيرة، والتي اتسمت بمراعاة كل ما هو جديد وفقًا لاحتياجات المدرسة، ومتطلبات سوق العمل.

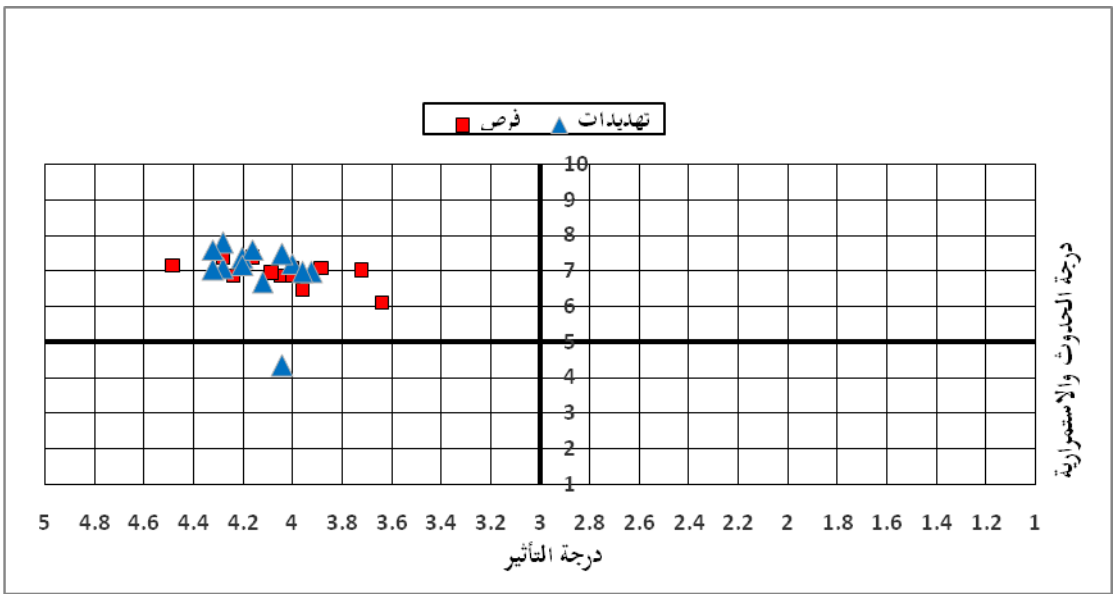
وعلى جانب آخر، يمثل التطور السريع في مجال البرمجيات ـ الخاصة بسهولة سرقة المعلومات والحصول عليها؛ حيث أصبحت هناك برامج تكنولوجية حديثة من شأنها الحصول على المعلومات المشفرة والسرية، حتى وإن كانت المعلومات مؤمنة ومحمية ـ خطورة أخرى على الأمن المعلوماتي في المدرسة، ذلك بالإضافة إلى قلة وعي العاملين بأهمية الحفاظ على سرية المعلومة؛ ممَّا ولد سببًا هامًا لنشر تلك المعلومات على الرغم من ضرورة إبقائها سرية، الأمر الذي يتطلب من المسئولين زيادة وعي العاملين بنوعية المعلومات التي يتعاملون معها، ومن ثم فعليهم تصنيفها، ومعرفة أكثرها حساسية، ومنع الأكثر حساسية من الانتشار، ويتم ذلك عن طريق البرامج التدريبية وورش العمل التي من شأنها تعريفهم بأضرار انتشار المعلومات على أمن المدرسة، وتأثيرها السلبي على عدم قدرة المدرسة على استعادة نشاطها بسهولة وقت الأزمات والكوارث.

يضاف إلى ما سبق، ارتفاع تكلفة البرامج التكنولوجية الحديثة المخصصة لحماية المعلومات والبيانات من السرقة، أو من التلف بسبب إصابتها بالفيروسات التي قد تودي بحياة جهاز الكمبيوتر، وما يحتفظ به من بيانات ومعلومات.

3. تحليل التوازن بين الفرص والتهديدات:

يتضح من جدولي تحليل البيئة الخارجية للمدرسة الثانوية الصناعية (الفرص والتهديدات)، أن مجموع متوسطات الأوزان النسبية للفرص (376.6)، وأن مجموع متوسطات الأوزان النسبية للتهديدات (390.76)؛ ممَّا يعني أن مجموع متوسطات الأوزان النسبية للتهديدات أكبر من مجموع متوسطات الأوزان النسبية للفرص؛ وهو ما يوضح أن التهديدات الموجودة في البيئة الخارجية للمدرسة الثانوية الصناعية أكبر من الفرص المتاحة لها، وهذا يقلل من قدرتها على الاستفادة من الفرص، ويهدد قدرتها في الحفاظ على أمنها المعلوماتي، ويؤكد على ضعف فرص التمويل المقدمة للمدارس لاستكمال تجهيزها بالبنية التحتية اللازمة للحفاظ على الأمن المعلوماتي

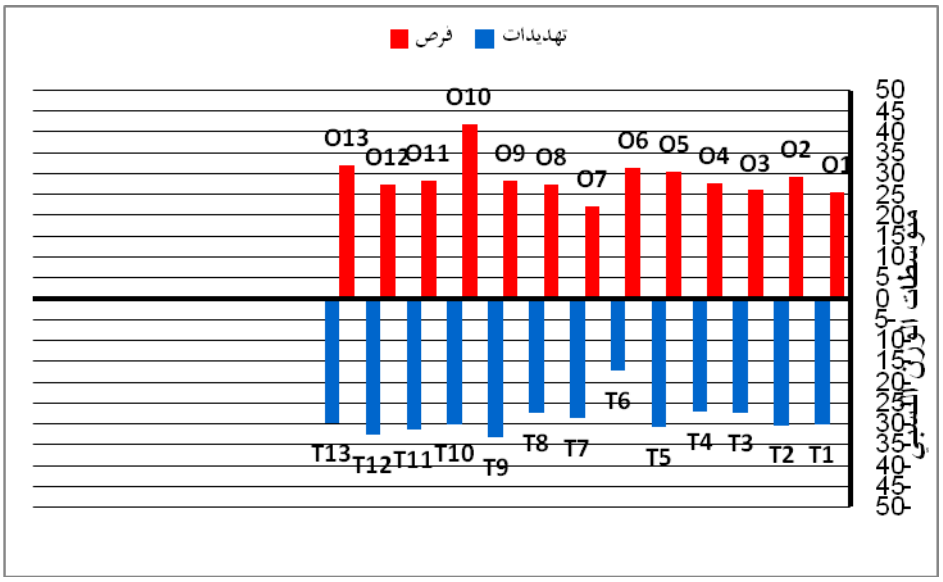
بها، وكذلك ضعف اهتمام القطاع الخاص بتقديم برامج تدريبية للدارسين والعاملين في المدارس الثانوية الصناعية للحفاظ على الأمن المعلوماتي، ذلك أن الغالبية العظمى من الاهتمام ينصب على تقديم القطاع الخاص لخريجي التعليم الثانوي أو الدارسين فيه بعض البرامج التي تتعلق بتوظيفهم داخل الشركة والمصنع فحسب، دون أن يعود ذلك بالنفع على إدارة المدرسة.



شكل رقم (7) موقع الفرص والتهديدات وفق الوزن النسبي

يتضح من الشكل السابق أن جميع الفرص والتهديدات تقع في المربع الرابع، الذي يوضح أن درجة تأثيرها عالية، واحتمال استمراريتها كبير، فيما عدا العبارة رقم (6) في التهديدات، التي نصت على (عزوف القطاع الخاص عن تقديم فرص كافية للدارسين في المدارس الفنية للتدريب العملي في: المصانع، والشركات، والقطاعات الاقتصادية المختلفة)؛ حيث جاءت في الربع الثالث، وهي تعني أن درجة تأثيرها عالية، ولكن احتمالية استمراريتها ضعيفة.

كما يمكن تمثيل مستوى التوازن بين الفرص والتهديدات التي تؤثر على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، كما في الشكل التالي، بحيث يمثل الاتجاه الأعلى الفرص، والاتجاه الأسفل التهديدات:



شكل رقم (8) مستوى التوازن بين الفرص والتهديدات

بالنظر إلى الشكل السابق، يتضح أن هناك تقاربًا بين الأوزان النسبية للفرص والتهديدات، وعلى الرغم من ذلك فإن الوزن النسبي للتهديدات أعلى من الوزن النسبي للفرص؛ ممَّا يقلل من قدرة المدرسة الثانوية الصناعية على الاستفادة منها، وذلك أيضًا في ضوء أن درجة كل من حدوث التهديدات، واستمرارية حدوثها عالية، وفي ذات الوقت يمكن الاستفادة من الفرص المتاحة في بناء الإستراتيجية، إذ إن درجة تأثيرها واستمرارية حدوثها عالية.

ثالثًا ـ بناء مصفوفة التحليل الإستراتيجي SWOT Matrix:

يتضمن بناء مصفوفة التحليل الإستراتيجي الاعتماد على عناصر البيئة الداخلية: (القوة والضعف)، والبيئة الخارجية: (الفرص والتهديدات) الأكثر تأثيرًا على إدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في مصر، وتتضح أبعاد هذه المصفوفة من خلال الجدول التالي:[98]

جدول رقم (7) مصفوفة التحليل الرباعي.

	غير مرغوبة	مرغوبة
لا يمكن السيطرة عليها	التهديدات	الفرص
يمكن السيطرة عليها	عناصر الضعف	عناصر القوة

يوضح الجدول التالي التحليل الرباعي لعناصر البيئة الداخلية والخارجية، التي تم التوصل إليها، وقد تم استبعاد الجوانب الأقل أهمية؛ لتجنب التشتيت عند وضع الإستراتيجيات البديلة كما يتضح فيما يلي:

جدول رقم (8) التحليل الرباعي لعناصر البيئة الداخلية والخارجية

	جوانب قوة (ق)	جوانب ضعف (ض)
البيئة الداخلية	1. توافر الإمكانات البشرية المدربة للتعامل مع التكنولوجيا الحديثة؛ ممَّا يسهم في إدارة عمليات الأمن المعلوماتي في المدرسة. 2. تواجد التجهيزات المادية في المدرسة، بما يساعدها في الحفاظ على أمنها المعلوماتي. 3. قيام وزارة التربية والتعليم بالتعاون مع وزارة الاتصالات بعمل الشبكة الداخلية للمدارس؛ لربط جميع أجهزة الحاسب بشبكة واحدة، وربطها بالشبكة المعلوماتية الدولية. 4. تدريب العاملين في المدرسة تدريبًا مستمرًا، الأمر الذي يساعدهم على إدارة عمليات الأمن المعلوماتي. 5. وجود وحدة للمعلومات والإحصاء في المدرسة، تتولى مسئولية الحفاظ على الأمن المعلوماتي. 6. توجه المدارس الثانوية	1. ضعف قواعد البيانات في المدرسة، التي يمكن من خلالها توفير المعلومات الكاملة والدقيقة عن سوق العمل. 2. ضعف قدرات معظم مديري المدارس على إعداد صف ثانٍ من القيادات، يساعدهم في إدارة عمليات الأمن المعلوماتي في المدرسة. 3. الثقافة التنظيمية في المدرسة لا تدعم تحقيق أهداف إدارة الأمن المعلوماتي. 4. محدودية التعاون بين المدارس الثانوية الفنية الصناعية ومؤسسات المجتمع المحلي؛ نظرًا لغياب قواعد البيانات والمعلومات، التي يمكن من خلالها تحديد مجالات الاستفادة. 5. عملية التخطيط للأمن المعلوماتي في المدرسة فردية وليست مؤسسية. 6. ضعف عمليات الحماية والتأمين

البيئة الخارجية	الصناعية للأخذ بنظام المعلومات الإدارية. 7.وجود بطاقات توصيف وظيفي للمسئولين في وحدة المعلومات والإحصاء، تحدد ما يجب عليهم القيام به للحفاظ على الأمن المعلوماتي. 8.حاجة وحدة ريادة الأعمال في المدرسة إلى إدارة للأمن المعلوماتي بها. 9.حاجة وحدة الإرشاد والتوجيه المهني في المدرسة إلى إدارة للأمن المعلوماتي بها.	في المدرسة للبيانات والمعلومات من السرقة. 7.تدني حالة البنية التحتية والأساسية للاتصالات وتكنولوجيا المعلومات في المدرسة. 8.توجه المدارس والوزارة نحو حل المشكلات الخاصة باختراق المعلومات بعد حدوثها وليس التخطيط لتفادي حصول المشكلة من الأساس. 9.قلة توافر البرامج التكنولوجية المتنوعة اللازمة لإدارة الأمن المعلوماتي في المدرسة. 10. ندرة وجود عقود صيانة بين المدرسة والشركات المسئولة؛ ممَّا ينتج عنه تعذر صيانة الأجهزة. 11. ضيق مساحة بعض الأقسام والمعامل، وقلة الخامات والأدوات، الأمر الذي يؤثر على قدرة العاملين على إدارة عمليات الأمن المعلوماتي. 12. ضعف القدرة على الاستخدام الأمثل للأجهزة التكنولوجية المستخدمة في الحفاظ على المعلومات. 13. قلة المعلومات اللازمة

		لتسويق المنتجات المدرسية للمجتمع الخارجي.
الفرص (O) 1. إصدار وزارة التربية والتعليم مجموعة من القواعد المنظمة للتعاون بين إدارة المدرسة والمؤسسات الإنتاجية، وتوفير قواعد البيانات اللازمة لذلك. 2. اتجاه الكثير من شركات الكمبيوتر إلى توفير برامج جديدة لبناء قواعد البيانات في المدارس، مما يساعد على تحقق أمن المعلومات في المدرسة. 3. عقد بروتوكولات تعاون بين وزارة التربية	**إستراتيجية القوة والفرص (ق Xف) (S/O)** 1. الاستغلال الأمثل للخطة الإستراتيجية لتطوير التعليم بشكل عام، وتطوير التعليم الفني بوجه خاص، وإتاحة المزيد من الإمكانات التكنولوجية في المدرسة الثانوية الصناعية بالشكل الذي يدعم البنية التحتية للأجهزة التكنولوجية، ويساعدها في الحفاظ على أمنها المعلوماتي، الأمر الذي يزيد من عدد المدارس التي تم تنمية البنية التحتية فيها S2, S3, O4 2. توفير البيانات والمعلومات الدقيقة عن إمكانيات خريجي المدرسة من ناحية، ومتطلبات	**إستراتيجية الضعف والفرص (ض x ف) (W/O)** 1. تدعيم قواعد البيانات الموجودة في المدارس الثانوية الصناعية وعنها، وعن المؤسسات التي يمكن الاستفادة منها لإدارة عمليات الأمن المعلوماتي، وكذلك المعلومات اللازمة لتسويق المنتجات المدرسية، واستخدام المعلومات وقت الحاجة، وذلك من خلال الاستفادة من شركات الكمبيوتر والمؤسسات المعنية W1، W13، O1، O2. 2. تدريب الإداريين والمديرين على إعداد صف ثانٍ من القيادات يساعد في إدارة عمليات الأمن المعلوماتي في المدرسة، بحيث يكون قادرًا على استخدام الأجهزة

والتعليم والشركات وأصحاب الأعمال، من أجل تطوير التعليم الفني ليتماشى مع التحديات الحالية، عن طريق إتاحة معلومات وافية ودقيقة عن الطرفين. 4.تأكيد الخطة الإستراتيجية لوزارة التربية والتعليم على ضرورة إتاحة التجهيزات وتكنولوجيا التعليم، بما يتناسب مع نوعية التعليم الفني وعدد الطلاب وفق معايير معدة لذلك. 5.إنشاء الجهاز القومي للرقابة على جميع أعمال أمن المعلومات، ومنح تراخيص مزاولة أعمال الخبرة والتخصص في هذا المجال. 6.إنشاء مركز التطوير التكنولوجي، بهدف إدخال التكنولوجيا	سوق العمل من ناحية أخرى وذلك من خلال الوحدات المدرسية المستحدثة، التي يتم تحديث بياناتها باستمرار وفقًا لآخر متطلبات السوق. S5، S8، S9، O1. 3. تحديد التوصيف الوظيفي لمسئولي الوحدات المستحدثة في المدرسة الثانوية الفنية، ومساعدتهم على تنمية ذاتهم مهنيًا، من خلال تدريبهم على مهام وظائفهم الجديدة، وذلك تحت إشراف الجهاز القومي للرقابة على جميع أعمال أمن المعلومات، ومركز التطوير التكنولوجي. S4، S7، O5، O6. 4. توافر الإمكانيات البشرية اللازمة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية بالتعاون بين وزارة التربية والتعليم والهيئات والوزارات الأخرى المعنية بتدريب العاملين في هذا المجال S1، O9. 5. عقد عدد من بروتوكولات التعاون وعقود الشراكة بين:	التكنولوجية في الحفاظ على الأمن المعلوماتي في المدرسة، من خلال برامج التدريب والمؤتمرات التي تعقد تحت إشراف الوزارة وغيرها من الجهات المعنية؛ مما يدعم الثقافة التنظيمية الإيجابية عن إدارة عمليات الأمن المعلوماتي في المدرسة O8، O9، W2، W3، W12. 3. الاهتمام بعمل قواعد بيانات عن المؤسسات التي من شأنها تقديم المساعدات للمدرسة وقت حدوث الأزمات والمشكلات، وذلك بمساعدة شركات الكمبيوتر المتخصصة في إعداد هذا النوع من قواعد البيانات W4، O2. 4. الاهتمام بصيانة الأجهزة التكنولوجية الموجودة في المدرسة، من خلال تدعيم عقود الصيانة بين المدرسة وبين الشركات المسئولة W10، O2. 5. تقديم المزيد من البرامج التدريبية للإداريين والمديرين التي تؤكد على التعاونية والمشاركة في التخطيط لإدارة الأمن المعلوماتي في المدرسة الثانوية الصناعية،

المتطورة في التعليم بشكل عام. 7.الاتجاه نحو تحقيق مزيد من التعاون مع الهيئة القومية للاتصالات السلكية واللا سلكية؛ لتخريج العمالة الفنية المدربة في بعض المجالات. 8.سعي وزارة التربية والتعليم لعقد عدد من المؤتمرات؛ للربط بين التعليم الفني وسوق العمل، بناءً على قواعد بيانات ومعلومات مسبقة. 9.تولي المعهد القومي للاتصالات ـ بالتنسيق مع وزارتي الاتصالات والمعلومات ووزارة التربية والتعليم ـ الإشراف على البرنامج القومي الخاص بالتدريب المتخصص في مجال تكنولوجيا المعلومات والاتصالات.	الوزارة، والشركات المختصة في مجال التكنولوجيا وشركات رجال الأعمال؛ من أجل توفير البرامج اللازمة وقواعد البيانات الضرورية S6،S3، O1، O2، O3.	وكذلك التخطيط للاستفادة من المعلومات قبل حدوث الأزمات؛ بحيث تكون هناك قواعد بيانات وافية عن القدرات الحالية للمديرين والإداريين، والاحتياجات التي ما زالوا في حاجة للتدرب عليها في هذا الإطار W5، W8، O9. 6.توفير الأماكن الملائمة والبنية التحتية والبرامج التكنولوجية اللازمة للمدارس الثانوية الصناعية ـ خاصةً تلك التي لم يتم تجهيزها بعد ـ تحقيقًا لبنود الخطة الإستراتيجية، وبالتعاون مع مركز التطوير التكنولوجي ومنظمات المجتمع المدني، والقطاع الخاص، وشركات الكمبيوتر، والوزارات المعنية W4، W7، W9،W11،O2، O3، O4، O6.

التهديدات (T)	إستراتيجة القوة والتهديدات (S/T)	إستراتيجية الضعف والتهديدات (W/T)
1. التغير المستمر والسريع في البرامج التي تستخدم في اختراق البيانات والمعلومات. 2. ضعف الوعي الكافي بكيفية التعامل مع المعلومات وحساسيتها عند استخدام الشبكات الاجتماعية المنتشرة (مثل: فيس بوك، وتويتر ونحوهما). 3. زيادة تكلفة برامج الحماية، وبرامج بناء قواعد البيانات. 4. قلة الميزانيات المخصصة لتجهيز مراكز التدريب التابعة لوزارة التربية والتعليم اللازمة لتحقيق متطلبات سوق العمل من التكنولوجيا المتطورة. 5. غياب المؤشرات والمعلومات عن التطور المتسارع	1. الاهتمام بتوفير التجهيزات المادية والبرمجية للمدرسة الثانوية الصناعية، بحيث يتم توفير أجهزة أكثر أمنًا، وبرامج جديدة؛ لمواكبة التغير السريع في البرامج المستخدمة لاختراق المعلومات، وذلك بتكلفة تتلاءم والإمكانات المادية للمدرسة، من خلال عقود شراكة، ومن ثم التغلب عليها ومواجهتها، وبناء قواعد بيانات في المدارس عن: قدرات المدرسة، واحتياجات السوق، وغيرها من البيانات والمعلومات؛ مما يساعد على تحقيق أمن المعلومات في المدرسة، وخاصةً في ظل توجه المدرسة الثانوية الصناعية للأخذ بنظام المعلومات الإدارية، والاهتمام بربط المدرسة بشبكة المعلومات الدولية التي تمكنها من تحديث برامجها والاتصال بغيرها من المدارس للاستفادة من خبراتها S2، S3، S6،	1. تعزيز قدرة المديرين في المدارس الثانوية الصناعية على إعداد صف ثانٍ من القيادات للتخطيط لإدارة الأمن المعلوماتي في المدرسة بشكل جماعي، على مستوى المدرسة، والإدارة، والمديرية، والوزارة، وتدعيم الثقافة التنظيمية التي تعزز لدى العاملين أهمية المعلومات، وتعزيز وعيهم أيضًا بكيفية التعامل معها، وتصنيفها وفقًا لدرجة حساسيتها لضمان عدم تسربها W2، W3، W5، T2، T8. 2. تدعيم البنية التحتية والبرمجية للمدرسة الثانوية الصناعية لمواكبة التغير المستمر والسريع في البرامج التي تستخدم في اختراق البيانات والمعلومات، ومن ثم تدعيم الحماية الأمنية للبيانات والمعلومات الخاصة في المدرسة، وذلك بالتعاون مع القطاع الخاص، ومنظمات المجتمع المدني، وشركات الكمبيوتر التي من شأنها تقديم

لمتطلبات سوق العمل، بما يفوق تطور إمكانات ومخرجات التعليم الفني. 6. ندرة وجود قواعد البيانات الصحيحة والموثقة والمؤمنة التي تحدد احتياجات سوق العمل من المهن والتخصصات المختلفة. 7. تدني المنظومة القيمية في المجتمع؛ مما يمثل تهديدًا لأمن المعلومات بشكل مستمر. 8. ضعف التخطيط لبناء برنامج متكامل لأمن المعلومات بدءًا من الوزارة وحتى المدرسة. 9. عزوف القطاع الخاص عن تقديم فرص كافية للدارسين في المدارس الفنية للتدريب العملي في المصانع والشركات	T1، T3، T6. 2. الاهتمام بتدريب العاملين في مجال تكنولوجيا المعلومات على الوعي بأهمية الحفاظ على المعلومات، وتصنيفها ومعرفة درجة حساسيتها، ومن ثم عدم الإفصاح عن أي معلومة قبل التأكد من درجة حساسيتها أولًا، الأمر الذي لا يضر في المدرسة، بالإضافة إلى توفير برامج تدريبية عن كيفية استخدام التكنولوجيا الحديثة في الحفاظ على المعلومات، مع الوضع في الاعتبار ضرورة أن تكون تحت إشراف الوزارة، وفي قاعات تدريبية مجهزة بالتكنولوجيا الحديثة التي سيتم استخدامها بالفعل، وكذلك استخدام قاعات وحدات المعلومات والإحصاء، وغيرها من الوحدات المجهزة بالأجهزة التكنولوجية. وعليه، ثمة ضرورة لإشراك القطاع الخاص في تمويل تلك البرامج، وتقديمها داخل مؤسساته S1، S4، S5،	البرامج اللازمة للمدرسة بأسعار مخفضة W4، W6، W7، W9، T1، T3، T9. 3. تصميم المزيد من قواعد البيانات التي تضم معلومات عن سوق العمل، والإمكانيات المادية والبشرية للمدرسة، والهيئات التي يمكن للمدرسة الاستعانة بها وقت الأزمات، على أن تكون مؤمنة، ويتم تحديثها باستمرار للاستفادة منها وقت الحاجة إليها W1، W6، T5، T6. 4. اهتمام الوزارة بعمل برامج توعية مستمرة للمعلمين والإداريين والمديرين والطلاب أيضًا؛ بحيث تهدف إلى تدعيم الجانب الأخلاقي والقيمي لديهم، وتنمية شعور الولاء والانتماء لمدرستهم، الأمر الذي يمنعهم من تسريب المعلومات أو سرقتها، أو إتلافها؛ مما يسهم في مساعدة المديرين والمسئولين على التخطيط لإدارة الأمن المعلوماتي قبل اختراق المعلومات، وقبل حدوث الأزمات المترتبة عليها W9، T8. 5. الاهتمام بتقديم المزيد من برامج

والقطاعات الاقتصادية المختلفة.	S8، S9، T2، T9. 3. الاستغلال الأمثل للإمكانيات البشرية الموجودة في المدرسة الثانوية الصناعية، وتلك الموجودة في الإدارة والمديرية والوزارة، من المسئولين عن إدارة عمليات الأمن المعلوماتي وذلك في التخطيط للحفاظ على أمن المعلومات على المستويات كافة، مما يؤدي إلى وجود برنامج متكامل للحفاظ على المعلومات على كل المستويات S1، T8.	التدريب التي تدور حول بناء القدرات التكنولوجية للعاملين في مجال أمن المعلومات، وتعزيز قدراتهم على استخدام الأجهزة، والتعامل معها، والصيانة السريعة لها، والتعامل مع البرمجيات وتحديثها، وكيفية تأمين البيانات والمعلومات، والحفاظ عليها، واسترجاعها وقت الحاجة إليها، وذلك بالتعاون مع وزارة التربية والتعليم، والقطاعات الاقتصادية المختلفة، والمصانع والشركات، وشركات الكمبيوتر W12، T9.

ويتضح من الجدول السابق، أنه بالاستفادة من: نقاط القوة، والفرص، والتهديدات، ونقاط الضعف، تنتج أربع استراتيجيات يمكن إبرازها فيما يلي:

أ. **إستراتيجية القوة/ الفرص (S/O) التوجه الريادي:**

وفيها يتم استخدام مجالات القوة؛ لاقتناص الفرص المتاحة، وتتضمن ما يلي:

1- الاستغلال الأمثل للخطة الإستراتيجية لتطوير التعليم بشكل عام، وتطوير التعليم الفني بوجه خاص، وإتاحة المزيد من الإمكانيات التكنولوجية في المدرسة الثانوية الصناعية بالشكل الذي يدعم البنية التحتية للأجهزة التكنولوجية، ويساعدها في الحفاظ على أمنها المعلوماتي؛ الأمر الذي يزيد من عدد المدارس التي تم تنمية البنية التحتية فيها S2, S3, O4.

2- توفير البيانات والمعلومات الدقيقة عن إمكانات خريجي المدرسة من ناحية، ومتطلبات سوق العمل من ناحية أخرى، وذلك من خلال الوحدات المدرسية المستحدثة، التي يتم تحديث بياناتها باستمرار وفقًا لآخر متطلبات السوق. S5، S8، S9، O1.

3- تحديد التوصيف الوظيفي لمسئولي الوحدات المستحدثة في المدرسة الثانوية الفنية، ومساعدتهم في تنمية ذاتهم مهنيًا من خلال تدريبهم على مهام وظائفهم الجديدة، وذلك تحت إشراف الجهاز القومي للرقابة على جميع أعمال أمن المعلومات، ومركز التطوير التكنولوجي. S4، S7، O5، O6.

4- توافر الإمكانيات البشرية اللازمة للحفاظ على الأمن المعلوماتي في المدرسة الثانوية الصناعية بالتعاون بين: وزارة التربية والتعليم، والهيئات والوزارات الأخرى المعنية بتدريب العاملين في هذا المجال S1، O9.

5- عقد عدد من بروتكولات التعاون وعقود الشراكة بين الوزارة والشركات المختصة في مجال التكنولوجيا وشركات رجال الأعمال، من أجل توفير البرامج اللازمة وقواعد البيانات الضرورية S3،S6 ، O1 ، O2، O3.

ب. إستراتيجية القوة / التهديدات (S/T) التوجه التكيفي:

وفيها يتم تنمية مجموعة من الإستراتيجيات البديلة، التي تستخدم مجالات القوة للحد من التهديدات، وتتضمن ما يلي:

1. الاهتمام بتوفير التجهيزات المادية والبرمجية للمدرسة الثانوية الصناعية، بحيث يتم توفير أجهزة أكثر أمنًا، وبرامج جديدة لمواكبة التغير السريع في البرامج المستخدمة لاختراق المعلومات، وذلك بتكلفة تتلاءم والإمكانات المادية للمدرسة من خلال عقود شراكة، ومن ثم التغلب عليها ومواجهتها، وبناء قواعد البيانات في المدارس عن قدرات المدرسة واحتياجات السوق، وغيرها من البيانات والمعلومات؛ مما يساعد على تحقق أمن المعلومات في المدرسة، وخاصةً في ظل توجه المدرسة الثانوية الصناعية للأخذ بنظام المعلومات الإدارية، والاهتمام بربط المدرسة بشبكة المعلومات الدولية، التي تمكنها من تحديث برامجها، والاتصال بغيرها من المدارس للاستفادة من خبراتها S2، S3، S6، T1، T3، T6.
2. الاهتمام بتدريب العاملين في مجال تكنولوجيا المعلومات على الوعي بأهمية الحفاظ على المعلومات، وتصنيفها حسب درجة حساسيتها، ومن ثم عدم الإفصاح عن أي معلومة قبل التأكد من درجة حساسيتها أولًا، الأمر الذي لا يضر في المدرسة، بالإضافة إلى توفير برامج تدريبية عن كيفية استخدام

التكنولوجيا الحديثة في الحفاظ على المعلومات، مع الوضع في الاعتبار ضرورة أن تكون تحت إشراف الوزارة، وفي قاعات تدريبية مجهزة بالتكنولوجيا الحديثة التي سيتم استخدامها بالفعل، وكذلك استخدام قاعات وحدات المعلومات والإحصاء، وغيرها من الوحدات المجهزة بالأجهزة التكنولوجية. وعليه، فإن ثمة ضرورة لإشراك القطاع الخاص في تمويل تلك البرامج، وتقديمها داخل مؤسساته S1، S4، S5، S8، S9، T2، T9.

3. الاستثمار الأمثل للإمكانيات البشرية الموجودة في المدرسة الثانوية الصناعية، والموجودة في: الإدارة، والمديرية، والوزارة، من المسئولين عن إدارة عمليات الأمن المعلوماتي، وذلك في التخطيط للحفاظ على أمن المعلومات على المستويات كافة؛ مما يؤدي إلى وجود برنامج متكامل للحفاظ على المعلومات على كل المستويات S1، T8.

ج. إستراتيجية الضعف والفرص (W/O) التوجه الدفاعي ـ الإصلاحي:

ويتم فيها تنمية مجموعة من الإستراتيجيات البديلة، من خلال التغلب على نقاط الضعف لاقتناص الفرص، وتتضمن ما يلي:

1. تدعيم قواعد البيانات الموجودة في المدارس الثانوية الصناعية وعنها، وعن المؤسسات التي من الممكن الاستفادة منها لإدارة عمليات الأمن المعلوماتي، وكذا المعلومات اللازمة لتسويق المنتجات المدرسية، واستخدام المعلومات وقت الحاجة، وذلك من خلال الاستفادة من شركات الكمبيوتر والمؤسسات المعنية W1، W13،O1 ، O2.
2. تدريب الإداريين والمديرين على إعداد صف ثانٍ من القيادات يساعد في إدارة عمليات الأمن المعلوماتي في المدرسة، ويكون قادرًا على استخدام الأجهزة التكنولوجية في الحفاظ على الأمن المعلوماتي في المدرسة، من خلال برامج التدريب والمؤتمرات التي تعقد تحت إشراف الوزارة وغيرها من الجهات المعنية؛ مما يدعم الثقافة التنظيمية الإيجابية عن إدارة عمليات الأمن المعلوماتي في المدرسة O8، O9، W2، W3، W12.

3. الاهتمام بعمل قواعد بيانات عن المؤسسات التي من شأنها تقديم المساعدات للمدرسة وقت حدوث الأزمات والمشكلات، وذلك بمساعدة شركات الكمبيوتر المتخصصة في إعداد هذا النوع من قواعد البيانات W4، O2.
4. الاهتمام بصيانة الأجهزة التكنولوجية الموجودة في المدرسة، من خلال تدعيم عقود الصيانة بين المدرسة والشركات المسئولة W10، O2.
5. تقديم المزيد من البرامج التدريبية للإداريين والمديرين، التي تؤكد على التعاونية والمشاركة في التخطيط لإدارة الأمن المعلوماتي في المدرسة الثانوية الصناعية، وكذلك التخطيط للاستفادة من المعلومات قبل حدوث الأزمات، بحيث تكون هناك قواعد بيانات وافية عن القدرات الحالية للمديرين والإداريين، والاحتياجات التي ما زالوا في حاجة للتدرب عليها في هذا الإطار W5، W8، O9.
6. توفير الأماكن الملائمة والبنية التحتية والبرامج التكنولوجية اللازمة للمدارس الثانوية الصناعية ـ خاصةً تلك التي لم يتم تجهيزها بعد ـ تحقيقًا لبنود الخطة الإستراتيجية، وبالتعاون مع مركز التطوير التكنولوجي ومنظمات المجتمع المدني، والقطاع الخاص، وشركات الكمبيوتر، والوزارات المعنية W4، W7، W9، W11، O2، O3، O4، O6.

د. إستراتيجية الضعف والتهديدات (W/T) توجه المحافظة على البقاء:

يتم فيها تنمية مجموعة من الإستراتيجيات البديلة من خلال التغلب على نقاط الضعف للحد من التهديدات، وتتضمن ما يلي:

1. تعزيز قدرة المديرين في المدارس الثانوية الصناعية على إعداد صفٍ ثانٍ من القيادات للتخطيط لإدارة الأمن المعلوماتي في المدرسة بشكل جماعي، على مستوى المدرسة، والإدارة، والمديرية، والوزارة، وتدعيم الثقافة التنظيمية التي تعزز لدى العاملين أهمية المعلومات، وتعزيز وعيهم أيضًا بكيفية التعامل معها وتصنيفها وفقًا لدرجة حساسيتها لضمان عدم تسربها W2، W3، W5، T2، T8.
2. تدعيم البنية التحتية والبرمجية للمدرسة الثانوية الصناعية؛ لمواكبة التغير المستمر والسريع في البرامج التي تستخدم في اختراق البيانات والمعلومات،

ومن ثم تدعيم الحماية الأمنية للبيانات والمعلومات الخاصة في المدرسة، وذلك بالتعاون مع القطاع الخاص، ومنظمات المجتمع المدني، وشركات الكمبيوتر التي من شأنها تقديم البرامج اللازمة للمدرسة بأسعار مخفضة W4، W6، W7، W9، T1، T، T9.

3. تصميم المزيد من قواعد البيانات التي تضم معلومات عن سوق العمل، وإمكانيات المدرسة المادية والبشرية، والهيئات التي يمكن للمدرسة الاستعانة بها وقت الأزمات، على أن تكون مُؤَمَّنة، ويتم تحديثها باستمرار؛ للاستفادة منها وقت الحاجة إليها W1، W6، T5، T6.
4. اهتمام الوزارة بعمل برامج توعية مستمرة للمعلمين، والإداريين، والمديرين، والطلاب أيضًا، تهدف إلى تدعيم الجانب الأخلاقي والقيمي لديهم، وتنمية شعور الولاء والانتماء لمدرستهم، الأمر الذي يمنعهم من: تسريب المعلومات، أو سرقتها، أو إتلافها، الأمر الذي يسهم في مساعدة المديرين والمسئولين على التخطيط لإدارة الأمن المعلوماتي قبل اختراق المعلومات، وقبل حدوث الأزمات المترتبة عليها W9، T8.
5. الاهتمام بتقديم المزيد من برامج التدريب التي تدور حول بناء القدرات التكنولوجية للعاملين في مجال أمن المعلومات، وتعزيز قدراتهم على استخدام الأجهزة، والتعامل معها، والصيانة السريعة لها، والتعامل مع البرمجيات وتحديثها، وكيفية تأمين البيانات والمعلومات، والحفاظ عليها، واسترجاعها وقت الحاجة إليها، وذلك بالتعاون مع وزارة التربية والتعليم، والقطاعات الاقتصادية المختلفة، والمصانع والشركات، وشركات الكمبيوتر W12، T9.

رابعًا- الإستراتيجيات البديلة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر (التداعيات والافتراضات):

تتضمن الإستراتيجيات البديلة أربع إستراتيجيات تم التوصل إليها من نتائج التحليل الرباعي (جدول 6)، والتي يمكن الاستفادة منها في التوصل إلى الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وفيما يلي عرض للافتراضات الأساسية التي يقوم عليها كل بديل، والتداعيات المحتملة عند تبنيه:

البديل الأول ـ {التوجه الريادي: إستراتيجية تعظيم القوة، واستثمار الفرص (S/O)}

يهدف هذا البديل إلى تنمية مجموعة من الإستراتيجيات لتحقيق الريادة والتميز لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وذلك من خلال الاستفادة من نقاط القوة، وتعظيمها في اقتناص الفرص المتاحة، ويقوم هذا البديل على عدد من الافتراضات، وله العديد من التداعيات التي يمكن توضيحها فيما يلي:

1. **الافتراضات التي يستند إليها البديل الريادي:**

- توفير التمويل اللازم لتجهيز المدارس الثانوية الصناعية بالبنية التحتية اللازمة للمدرسة الثانوية الصناعية؛ لحفظ معلوماتها إلكترونيًا.
- الالتزام بتنفيذ بنود الخطة الإستراتيجية؛ لتطوير التعليم بشكل عام والتعليم الفني على وجه الخصوص.
- الاحتفاظ بالبيانات والمعلومات التي تمتلكها المدرسة الثانوية الصناعية داخل قواعد بيانات منظمة، تساعد المدرسة على استرجاع تلك البيانات والمعلومات وقت الحاجة إليها.
- الاستغلال الأمثل للوحدات الموجودة في المدرسة الثانوية الصناعية ـ كوحدة المعلومات والإحصاء ـ واستخدامها في الحفاظ على المعلومات، واسترجاعها وقت الحاجة.
- تحديث بطاقات الوصف الوظيفي للعاملين بشكل عام، والعاملين بالوحدات المستحدثة في المدرسة الثانوية الصناعية، وذلك لتواكب مهامهم كل حديث في مجال تكنولوجيا المعلومات، والتخزين الآمن للمعلومات.
- الاهتمام بالتنمية المهنية المستمرة للعاملين في مجال الحفاظ على المعلومات المدرسية، الأمر الذي يمكنهم من التعامل مع الأجهزة والبرمجيات المستحدثة التي تساعدهم على الحفاظ على تلك المعلومات من الضياع أو السرقة.
- اهتمام الوزارة بتفعيل التعاون بينها وبين جميع الأطراف المعنية من مؤسسات قطاع خاص، أو مؤسسات مجتمع مدني، أو شركات كمبيوتر، وذلك في

عمل برامج تدريبية للعاملين، أو في شراء البرمجيات، والأجهزة، أو في توفير أماكن للتدريب، والأجهزة اللازمة لإتمامه.

2. التداعيات التي يستند إليها البديل الريادي:

تتمثل التداعيات المتوقع حدوثها نتيجة تبني البديل الريادي لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في جمهورية مصر العربية، فيما يلي:

- الاستعداد للأزمات والكوارث قبل حدوثها، ومن ثم قدرة المدرسة الثانوية الصناعية على تعافيها من الأزمات والكوارث بسرعة، واستمراريتها في تقديم خدماتها للعملاء.
- توفير قواعد البيانات والمعلومات اللازمة للمدرسة الثانوية الصناعية، وبالتالي حفظها من التلف أو السرقة.
- رفع وعي العاملين في المدرسة بأهمية المعلومات والبيانات، وقدرتهم على تصنيف المعلومات وفقًا لحساسيتها.
- زيادة شعور العاملين بالانتماء للمدرسة، ومن ثم الحفاظ على المعلومات الخاصة في المدرسة من الإفصاح عنها، وذلك إن كانت درجة حساسيتها عالية، وذلك للحفاظ على المدرسة من الدخلاء، واستغلالهم السيئ للمعلومات التي تخص المدرسة في غير مصلحتها.
- إثراء قدرات العاملين في المدرسة الثانوية الصناعية، من خلال برامج التدريب المختلفة التي يلتحقون بها، ومن ثَم تمكنهم من استخدام الأجهزة التكنولوجية، واستخدام البرامج الحديثة التي تساعدهم على التخزين الآمن للمعلومات.
- تفعيل دور الوحدات المدرسية المستحدثة، واستخدام ما بها من إمكانيات مادية وبشرية في تخزين المعلومات بشكل آمن، والحفاظ عليها من التلف أو السرقة.
- زيادة مشاركة العاملين في التخطيط لإدارة الأمن المعلوماتي، الأمر الذي يجعل التخطيط يتحول من عملية فردية إلى عملية جماعية، يشارك فيها

جميع العاملين في المدرسة؛ مما يشعرهم بالمسئولية تجاه ما يقومون به من أعمال تصب في مصلحة المدرسة.

- زيادة التنسيق بين وزارة التربية والتعليم والهيئات المعنية؛ مما يؤدي إلى التكامل بين أعمال الوزارة، وتلك الهيئات؛ لتحقيق إدارة فعالة للأمن المعلوماتي في المدرسة الثانوية الصناعية.
- تحقيق المزيد من التزام العاملين بأداء المهام الموكلة إليهم بالوحدات المستحدثة، نتيجة لوجود توصيف دقيق وواضح لمهامهم في بطاقات التوصيف الوظيفي، خاصةً تلك المرتبطة بإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

البديل الثاني ـ التوجه التكيفي {إستراتيجيات تعظيم القوة وتجنب التهديدات (S/T)}:

يهدف هذا البديل إلى تنمية مجموعة من الإستراتيجيات البديلة التي تستفيد من جوانب القوة؛ للحد من التهديدات التي تواجه إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وتتمثل افتراضات وتداعيات هذا البديل فيما يلي:

1. **الافتراضات التي يستند إليها البديل التكيفي:**

- قلة مصادر التمويل المتاحة، التي تنعكس على صعوبة تجهيز المدارس الثانوية الصناعية بالبنية التحتية اللازمة؛ لحفظ المعلومات وتخزينها، وتوفير البرمجيات اللازمة لإنشاء قواعد البيانات وتأمينها، وتوفير الأماكن الملائمة للوحدات المستحدثة المسئولة عن حفظ تلك البيانات والمعلومات واسترجاعها وقت الحاجة، وتوفير برامج التدريب للعاملين لمساعدتهم على القيام بالعمل على الوجه الأكمل.
- غموض التوصيفات الخاصة بالعاملين بالوحدات المستحدثة، وعدم الاهتمام بتحديثها وفقًا للمتطلبات الحديثة.
- غياب التنسيق بين وزارة التربية والتعليم والهيئات والمؤسسات المعنية كالشركات والمصانع وشركات الكمبيوتر؛ ومن ثم ضعف فرص الاستفادة منهم لتحقيق إدارة جيدة للأمن المعلوماتي في المدرسة الثانوية الصناعية.

- ضعف الاهتمام بنشر الوعي بين العاملين بأهمية المعلومات ودرجة حساسيتها، وضرورة الحفاظ عليها من الاختراق والسرقة.
- استمرار انحدار المنظومة القيمية لدى أعضاء المجتمع المدرسي، ومن ثم عدم الاهتمام بالحفاظ على البيانات والمعلومات الموجودة في المدرسة.
- الشعور بالانفصال والانعزال عن المدرسة، وعدم الانتماء لها، ومن ثم عدم الاهتمام بتسرب أي قدر من المعلومات، وخاصةً في حالة عدم تقدير مخاطر مثل ذلك الأمر.
- بدائية البرامج التدريبية الموجهة للعاملين، وقلة إمكانات القاعات التي يقدم بها التدريب؛ ومن ثم اقتصاره على الحقائق النظرية، دون الاهتمام بالتطبيق العملي لتلك الحقائق، ومن ثم محدودية الأثر الإيجابي للتدريب بعد انتهائه.
- انفراد وزارة التربية والتعليم بالتخطيط، ونظرتها للمستويات الأخرى (المديرية، والإدارة، والمدرسة) كافة على أنها مجرد جهات تنفيذية لتوجهات الوزارة، ومن ثم فقدان فرص الاستفادة من خبرة الجهات الأخرى في التخطيط لهذا الأمر.

2. التداعيات التي يستند إليها البديل التكيفي:

تتمثل التداعيات المتوقع حدوثها نتيجة تبني البديل التكيفي لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، فيما يلي:

- النظر في المشكلات التي تتعرض لها المدرسة الثانوية الصناعية بعد حدوثها، أي ضعف قدرة المدرسة الثانوية الصناعية على التنبؤ بالمشكلات، والتي قد تتحول لأزمات، ثم كوارث لا يمكن التغلب عليها، وقد تضر بنشاط المدرسة ككل.
- ضياع بعض البيانات والمعلومات التي تمتلكها المدرسة، ومن ثم ضعف قدرتها في الاعتماد على تلك المعلومات عند رغبتها في استعادة نشاطها مرة أخرى بعد انتهاء الأزمة.
- شعور القائمين على إدارة المدرسة والعاملين فيها بأنهم مجرد تروس في آلة، وأن أدوارهم تنحصر في تنفيذ الأوامر فقط، الأمر الذي يزيد من انفصالهم عن بيئة المدرسة.

- ضعف مردود البرامج التدريبية المقدمة للقائمين في الوظائف الإدارية المرتبطة بالحفاظ على الأمن المعلوماتي، واستخدام التكنولوجيا الحديثة، والمديرين، ومن ثم عدم قدرتهم على إدارة عمليات الأمن المعلوماتي في المدرسة.
- استمرار عمل كل هيئة داخل المدرسة في معزل عن باقي الهيئات؛ مما يوضح الانفصال والانعزال التام، وعدم التنسيق بين الهيئات لتحقيق إدارة فعالة للأمن المعلوماتي.
- التركيز على الجانب النظري فقط في التدريب، ومن ثم إهمال التطبيق العملي.
- تهالك البنية التحتية الموجودة في المدارس الثانوية الصناعية، وصعوبة استكمال تجهيز باقي المدارس، الأمر الذي يؤدي إلى اعتماد المدارس على السجلات الورقية، والأساليب البدائية التي لا تصلح لإدارة عمليات الأمن المعلوماتي.

البديل الثالث ـ التوجه الدفاعي {إستراتيجية معالجة الضعف واستثمار الفرص (W/O)}

يهدف هذا البديل إلى تنمية مجموعة من الإستراتيجيات البديلة التي تساعد المدرسة الثانوية الصناعية في مصر في التغلب على نقاط الضعف؛ لاقتناص الفرص المتاحة لإدارة عمليات الأمن المعلوماتي، ويقوم على مجموعة من الافتراضات والتداعيات كالتالي:

1. **الافتراضات التي يستند إليها البديل الدفاعي:**

تتضمن هذه الافتراضات ما يلي:

- الاستفادة من عقود الشراكة وبروتوكولات التعاون المبرمة بين وزارة التربية والتعليم، والوزارات الأخرى، والمصانع والشركات، ومؤسسات القطاع الخاص، ومؤسسات المجتمع المدني، وشركات الكمبيوتر المختلفة؛ للمساهمة في تجهيز المدارس الثانوية الصناعية بوسائل التكنولوجيا الحديثة.
- الاستفادة من خبرات شركات الكمبيوتر المختلفة في تدريب العاملين في المدرسة على إنشاء قواعد البيانات، وتنظيم البيانات والمعلومات، وتصنيفها

وفقًا لدرجة حساسيتها، مقابل تولي المدرسة الإعلان عن تلك الشركات والبرامج التي تقدمها.

- استخدام المديرين لبعض العمليات الإدارية التي تساعدهم على إنجاز العمل بشكل أسرع وأفضل، مثل التفويض الإداري، الذي يسهم في عمل صف ثانٍ من القيادات، وتدريب هؤلاء المفوضين على إدارة عمليات الأمن المعلوماتي في المدرسة؛ للحفاظ على البيانات والمعلومات بالشكل الذي يتيح لها استعادة نشاطها بسهولة.
- توفير مصادر تمويل إضافية عن تلك المصادر التي توفرها وزارة التربية والتعليم؛ وذلك لتوفير الأماكن الملائمة للوحدات المستحدثة، وتوفير الأجهزة، وبرامج التدريب الملائمة، وتوفير الأماكن الملائمة للتدريب، والمجهزة بالأدوات التي يجب أن تستخدم للحفاظ على أمن المعلومات في المدرسة الثانوية الصناعية.
- الاستفادة من العاملين المدربين على الأساليب التكنولوجية الحديثة، وإنشاء قواعد البيانات، لتدريب باقي العاملين من غير الحاصلين على برامج تدريب في هذا الإطار، وذلك بالاستعانة بوحدة التدريب والتقويم والجودة الموجودة في المدرسة.
- الاستفادة من قواعد البيانات الموجودة في المدرسة عن الإمكانات البشرية والمادية، والهيئات التي من شأنها تقديم مساعدات للمدرسة وقت الحاجة، على أن يتم تحديثها باستمرار، ووضع جميع المساعدات التي يمكن لكل هيئة تقديمها أمام اسم كل هيئة لسهولة الوصول لتلك الهيئات ومعرفة ما يمكن أن تقدمه من خدمات.

2. التداعيات التي يستند إليها البديل الدفاعي:

تتمثل التداعيات المتوقع حدوثها نتيجة تبني البديل الدفاعي لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، فيما يلي:

- إشراك الأطراف المعنية، مثل: الشركات، والمصانع، والقطاعات الاقتصادية المختلفة؛ للمساهمة في إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية

الصناعية، وذلك بتوفير البرامج التدريبية، والتجهيزات اللازمة، وغيرها من الأمور المرتبطة بهذا السياق.

- الحاجة إلى إعطاء مديري مدارس التعليم الثانوي الصناعي المزيد من الحرية في إشراك العاملين في التخطيط لإدارة الأمن المعلوماتي على مستوى الإدارة، والمديرية، وتوصيل جهودهم للوزارة، ومن ثم تدريب عامليه على المشاركة في التخطيط للأمن المعلوماتي في المدرسة وعلى المستويات كافة.
- الحد من تدهور البنية التحتية لبعض المدارس الثانوية الصناعية ـ خاصةً تلك التي لم تجهز بعد ـ عن طريق توفير احتياجاتها الأساسية من التكنولوجيا المتطورة.
- الاهتمام بقياس المردود الإيجابي للبرامج التدريبية المقدمة للإداريين المتخصصين في مجال استخدام التكنولوجيا، والمديرين، والمعلمين أيضًا، عن طريق ربط النظرية بالتطبيق، وقياس أثر التدريب بعد انتهاء البرنامج، عن طريق مراقبة ممارسات المسئولين عن إدارة عمليات الأمن المعلوماتي في المدرسة عند أداء مهامهم المرتبطة بالحفاظ على المعلومات وحمايتها.
- ازدياد الحاجة للاستفادة القصوى من الإمكانات البشرية المتاحة في المدرسة، وتنمية شعورهم بالانتماء للمدرسة الثانوية الصناعية.
- الحد من عدم مبالاة العاملين بأهمية البيانات والمعلومات الخاصة في المدرسة، عن طريق نشر ثقافة تنظيمية تدعم ضرورة الاهتمام بالبيانات والمعلومات، وتدعم ضرورة وجودها للحفاظ على وضع المدرسة، وخاصة وقت الأزمات، لاسترجاع نشاط المدرسة بسهولة.

البديل الرابع ـ توجه المحافظة على البقاء {إستراتيجية معالجة الضعف وتجنب التهديدات(W/T)}

يهدف هذا البديل إلى تنمية مجموعة من الإستراتيجيات البديلة التي تساعد المدرسة الثانوية الصناعية في التغلب على نقاط الضعف للحد من التهديدات التي تواجه تحقيق إدارة فعالة لعمليات الأمن المعلوماتي، والحد من تدهور الأوضاع، ويقوم على مجموعة من الافتراضات والتداعيات، وبيانها على النحو التالي:

1. الافتراضات التي يستند إليها بديل المحافظة على البقاء، وتتضمن ما يلي:

- استمرارية تدهور البنية التحتية في الغالبية العظمى من المدارس الثانوية الصناعية، ومن ثم ضعف قدرة تلك المدارس على التخزين الآمن للبيانات والمعلومات، واستخدامها لاستعادة نشاط المدرسة وقت الحاجة لذلك.
- استمرارية انفراد كل مستوى إداري بالتخطيط للأمن المعلوماتي، وعدم الاهتمام بإشراك المرؤوسين في هذا الأمر؛ مما يؤدي إلى الانفصال بين الفئات المختلفة، وفقدان فرصة الاستفادة من خبراتهم.
- لا تزال الثقافة التنظيمية الموجودة في المدرسة بعيدة عن الاهتمام بالمعلومات ودورها في الحفاظ على استقرار المدرسة، واستمرارية العمل بها، الأمر الذي ينعكس على اللا مبالاة والاستهانة بها.
- تركيز البرامج التدريبية على الجانب النظري، وتدني قدرات وإمكانات قاعات التدريب التي تتم بها فاعليات التدريب، الأمر الذي ينعكس على ضعف الاهتمام بالجانب العملي، وضعف ممارسة ما تم التدرب عليه في البرامج التدريبية في الواقع العملي.
- ضعف وغموض قواعد البيانات الموجودة في المدرسة، وعليه تعزر استخدامها وقت الحاجة.
- الاستمرارية في الانفصال وعدم التنسيق بين الوزارات والهيئات والجهات المعنية، ومن ثم عدم الاستفادة منها في إتاحة فرص التدريب، أو التجهيز، أو غيرها من الجهود التي يمكن القيام بها في هذا الإطار.

2. التداعيات التي يستند إليها بديل المحافظة على البقاء:

تتمثل التداعيات المتوقع حدوثها نتيجة تبني بديل المحافظة على البقاء لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، ما يلي:

- تدهور الحالة التكنولوجية للمدرسة، وانهيار قدرة ما بها من تجهيزات تساعد المدرسة على إنجاز مهامها الإدارية.

- استمرارية الاعتماد على السجلات الورقية في حفظ المعلومات؛ مما يعرضها للفقدان، والسرقة، والتلف.
- ضياع المردود الإيجابي للبرامج التدريبية المقدمة للعاملين، الأمر الذي يجعلها بدون جدوى، فيضيع ما صرف عليها من أموال، دون أن يكون لذلك مردود إيجابي.
- بدائية قواعد البيانات الموجودة في المدارس الثانوية الصناعية، ومن ثم ضعف القدرة على الاعتماد عليها عند اتخاذ القرارات الخاصة باستعادة نشاط المدرسة، أو حل مشكلاتها.
- ازدياد الانفصال بين المستويات الإدارية المختلفة بدايةً من الوزارة، وحتى المدرسة.
- ازدياد تعرض المدارس الثانوية الصناعية للعديد من المشكلات، والأزمات، وربما الكوارث، وذلك دون استعداد، أو تخطيط مسبق لذلك؛ مما يساعد المدرسة على تدبير أمرها، الأمر الذي قد يؤدي إلى انهيار الخدمة.

وسوف يتم الموازنة بين البدائل الإستراتيجية الأربعة التي تم التوصل إليها من خلال مجموعة من المعايير، وهي: التوافق، والمنفعة، والقبول، والتمويل، والمواءمة، والتطابق، وذلك وفقًا للجدول التالي:

جدول رقم (9) الموازنة بين البدائل الإستراتيجية وفق معايير الإستراتيجيات.

البعد	الوصف	الريادي	التكيفي	الدفاعي	المحافظ
التوافق	أن يكون البديل متوافقًا مع الأهداف العامة للمدرسة الثانوية الصناعية.	المرتبة الأولى	المرتبة الثانية	المرتبة الثالثة	المرتبة الرابعة
المنفعة	قدرة البديل على المساهمة في تحقيق إدارة فعالة للأمن المعلوماتي في المدرسة الثانوية الصناعية.	المرتبة الأولى	المرتبة الثانية	المرتبة الثالثة	المرتبة الرابعة
القبول	قبول البديل من قبل الهيئات التربوية، ومؤسسات المجتمع وهيئاته.	المرتبة الأولى	المرتبة الثانية	المرتبة الثالثة	المرتبة الرابعة
التمويل	قدرة البديل على توفير التمويل اللازم، والدائم لتنفيذه.	المرتبة الثانية	المرتبة الثالثة	المرتبة الأولى	المرتبة الرابعة
المواءمة	يقصد بها مواءمته للقوانين والتشريعات، والثقافة السائدة لدى المجتمع المحيط.	المرتبة الثانية	المرتبة الأولى	المرتبة الرابعة	المرتبة الثالثة
التطابق	يحقق البديل توافقًا بين الفرص والتهديدات في البيئة الخارجية، ونقاط القوة والضعف في البيئة الداخلية.	المرتبة الأولى	المرتبة الثانية	المرتبة الثالثة	المرتبة الرابعة

يتضح من الجدول السابق، أنه في ضوء أبعاد الموازنة بين البدائل المختلفة أن التوجه الريادي الذي تقوم إستراتيجياته على تعظيم القوة واستثمار الفرص هو التوجه المثالي في ضوء نتائج التحليل، وأبعاد الموازنة بين البدائل، وذلك للحيثيات التالية:

التوافق: اتضح من خلال النظر لأهداف مدارس التعليم الفني الصناعي أن البديل الريادي يتفق وتلك الأهداف التي تركز على استخدام وسائل التكنولوجيا الحديثة في العمليات التي تتم في المدرسة كافة، استجابةً لمتطلبات عصر المعرفة.

المنفعة: اتضح من خلال نتائج التحليل البيئي أن ضعف وجود قواعد البيانات، وضعف فرص التعامل معها، وعدم التخزين الآمن للبيانات، والمعلومات، يُصعِّب على المدرسة فرصة التعامل مع المشكلات والأزمات التي تتعرض لها، الأمر الذي

فرض تغييرًا جوهريًا في سبل التعامل مع البيانات والمعلومات التي تملكها المدرسة، لمواكبة عصر المعلومات، ومساعدة المدرسة على سرعة التعافي من أزماتها.

القبول: تبين من نتائج التحليل الرباعي رغبة الهيئات التربوية في تطوير التعليم الفني بشكل عام، والتعليم الفني الصناعي بشكل خاص، الأمر الذي اتضح في بنود الخطة الإستراتيجية لتطوير التعليم، وانعكس على توجهات الوزارة والمسئولين التربويين في تجهيز المدارس الثانوية الصناعية بالبنية التحتية اللازمة؛ للمساهمة في تحقيق إدارة فعالة للأمن المعلوماتي.

التمويل: تبين من نتائج التحليل البيئي ضعف التمويل الموجه لتجهيز مدارس التعليم الفني الصناعي باحتياجاتها، الأمر الذي يوضح ضعف فرصة البديل الريادي في هذا الأمر، إذ يعتمد على ضرورة تجهيز المدارس الثانوية الصناعية بالبنية التحتية اللازمة لإدارة عمليات الأمن المعلوماتي في المدرسة، الأمر الذي لا يستقيم دون توفر التمويل اللازم، أما البديل الدفاعي فقد احتل المرتبة الأولى في هذا الإطار، وذلك لأنه اعتمد على توفير مصادر تمويل بديلة تهيئ للمدرسة توفير احتياجاتها التكنولوجية.

المواءمة: اتضح من نتائج التحليل البيئي استمرارية نمط الإدارة المركزية؛ حيث ما زال هناك انفراد بالتخطيط في المستويات العليا، دون الاهتمام بالمشاركة من قبل الجهات الدنيا، الأمر الذي يتعذر معه تطبيق البديل الريادي؛ حيث احتل البديل التكيفي المرتبة الأولى، في هذا الإطار، إذ ركز على استمرارية استخدام نظام الإدارة المركزية في إدارة شئون التعليم بشكل عام؛ مما انعكس على انفراد الإدارة بالتخطيط للأمن المعلوماتي دون الاستفادة من خبرات المستويات الإدارية الأقل، الأمر الذي يتطلب تغييرًا في التشريعات والقوانين التي مازالت تتعامل وهذا النمط الذي لا يهتم بالتعامل مع أفكار العاملين والاستفادة من خبراتهم.

التطابق: اتضح من نتائج التحليل البيئي أن البديل الريادي يحقق تطابقًا وتوافقًا بين الفرص والتهديدات في البيئة الخارجية، ونقاط القوة والضعف في البيئة الداخلية، ذلك أن تحقيق الفرص ومقاومة التهديدات تتلاءم مع توجهات هذا البديل، وتدعم نقاط القوة، وتتخلص من نقاط الضعف، وتتلاءم أيضا مع توجهاته.

وبناءً على ما سبق، وفي ضوء الموازنة بين البدائل الإستراتيجية، تم التوصل إلى أن البديل الريادي ـ الذي تقوم إستراتيجياته على تعظيم القوة واستثمار الفرص ـ هو التوجه المثالي؛ وذلك لأنه احتل المركز الأول في أربعة أبعاد من أبعاد الموازنة. وعليه، وفي ضوء ما تضمنه البديل الريادي، سيقوم البحث بصياغة الإستراتيجية لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وذلك كما سيتضح في الخطوة التالية من البحث.

القسم الخامس ـ صياغة الإستراتيجية لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر.

تهدف تلك الخطوة لصياغة الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وينقسم ذلك القسم إلى عدد من المحاور، بيانها على النحو التالي:

1. مرتكزات الإستراتيجية المقترحة.
2. رؤية الإستراتيجية المقترحة.
3. رسالة الإستراتيجية المقترحة.
4. الغايات والأهداف الإستراتيجية المقترحة.
5. ملامح الإستراتيجية المقترحة.
6. متطلبات تنفيذ الإستراتيجية المقترحة.
7. معوقات تنفيذ الإستراتيجية المقترحة وسبل مواجهتها.

وفيما يلي عرض لتلك المحاور بالتفصيل:

1. مرتكزات الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر.

تقوم الإستراتيجية المقترحة على عدة مرتكزات، يمكن إبرازها فيما يلي:

- تطور متطلبات عصر المعلومات والمعرفة، وضرورة استجابة المنظمات التعليمية كافة، والمدارس الثانوية الصناعية على وجه الخصوص لتلك المتطلبات.
- إن المعلومات أصبحت في الآونة الأخيرة الثروة الحقيقية التي تمتلكها المدرسة، وعليها حسن استخدامها؛ لضمان تحقيق أهدافها.

- توفير البنية التحتية والتكنولوجية اللازمة للحفاظ على المعلومات من الضياع أو السرقة.
- أصبح للمدرسة القدرة على توقع ما يمكن أن يحدث لها من مشكلات أو أزمات قد تعترض تحقيقها لأهدافها، أو تقديم خدماتها لعملائها.
- وجود معايير ثابتة لتقويم قدرة المدرسة على إدارة عمليات الأمن المعلوماتي بها، وتحسين المسار باستمرار إذا كانت هناك مشكلات في الأداء.
- تلعب إدارة الأمن المعلوماتي دورًا هامًا في تدعيم قدرة المدرسة على مواجهة المشكلات والأزمات، والتعافي السريع من الأزمات.
- إن التدريب من العمليات الهامة لإدارة الأمن المعلوماتي، لما له من دور في الوقوف على آخر المستجدات في مجال تخصص كل فرد فيهم، خاصةً إن كان الأمر يتعلق باستخدام التكنولوجيا الحديثة، التي تتسم بالتغير المستمر في فترات وجيزة جدًا.
- أن هناك نوعان من المعلومات التي يتضمنها النظام المدرسي وهي المعلومات التي يجب الإفصاح عنها لجمهور المستفيدين، والمعلومات التي يجب على إدارة المدرسة الاحتفاظ بها لنفسها، لحساسيتها الشديدة، ولأنها تستخدم في استعادة نشاط المدرسة بعد تعرضها لإحدى الأزمات.
- تتطلب إدارة عمليات الأمن المعلوماتي مشاركة عدد لا نهائي من الهيئات في تحقيق إدارة فعالة للأمن المعلوماتي في المدرسة الثانوية الصناعية، كالشركات، والمصانع، ومؤسسات المجتمع المدني، ووزارة التربية والتعليم، وشركات الكمبيوتر وغيرها؛ من أجل المساهمة في التجهيز، والتدريب، وغيرها من المهام اللازمة لتحقيق إدارة فعالة للأمن المعلوماتي.
- سعي الهيئات التربوية المسئولة عن التعليم نحو تمكين العاملين، ومشاركتهم في صنع القرار، والمشاركة في التخطيط، وغيرها من العمليات التي تشعرهم بانتمائهم للمدرسة، ومسئولياتهم عن كل ما يتم داخلها.

2. رؤية الإستراتيجية المقترحة:

"تسعى المدرسة الثانوية الصناعية في مصر إلى وضع إستراتيجية لإدارة عمليات الأمن المعلوماتي استجابة لمتطلبات عصر التكنولوجيا والوصول إلى مركز تنافسي ريادي".

3. رسالة الإستراتيجية المقترحة:

تتمثل رسالة الإستراتيجية المقترحة في (تحسين قدرة المدرسة الثانوية الصناعية على إدارة عمليات الأمن المعلوماتي بها ولما تمتلكه من بيانات ومعلومات، وذلك استجابةً لمتطلبات عصر تكنولوجيا الاتصالات والمعلومات، وما يتطلبه ذلك من حماية للبيانات والمعلومات التي تمتلكها المدرسة من التلف، أو السرقة، أو التسرب، خاصةً تلك التي لا يجب الإفصاح عنها، الأمر الذي يساعد المدرسة على الاستعداد للمشكلات قبل حدوثها، والتعافي من الأزمات التي قد لا تستطيع المدرسة توقعها، والاستعداد لها بسرعة تمكنها من استمرارية تقديم الخدمة، والتعافي السريع من الآثار السلبية للأزمة).

4. الغايات والأهداف الإستراتيجية المقترحة:

تتحدد الغايات والأهداف الإستراتيجية فيما يلي:

الغاية الأولى ـ (دعم التوجه اللا مركزي في إدارة المدرسة الثانوية الصناعية في مصر، الأمر الذي يتيح للمدير والمرؤوسين وجميع المستويات الإدارية الأخرى المشاركة في التخطيط لإدارة عمليات الأمن المعلوماتي في المدرسة)، ويمكن تحقيق تلك الغاية من خلال الأهداف الإستراتيجية التالية:

أ- اتباع أسلوب التفويض الإداري من الرؤساء للمرؤوسين، وذلك بوضع الخطوط العريضة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

ب-تشجيع المرؤوسين على المستويات كافة (المديرية، الإدارة، المدرسة) من المشاركة في صنع القرار، وبالتالي إبداء الرأي في سبل تحقيق إدارة فعالة للأمن المعلوماتي في المدرسة.

ج- إكساب المسئولين عن حفظ المعلومات في المدرسة الثانوية الصناعية المهارات التي تمكنهم من تصنيف المعلومات، ومعرفة درجة حساسيتها، ومن ثم التخطيط لاستخدامها وتخزينها وفقًا لدرجة حساسيتها.

الغاية الثانية ـ (العمل على تنمية قدرات الإمكانات البشرية في المدرسة الثانوية الصناعية، الأمر الذي يمكنهم من الحفاظ على المعلومات التي تمتلكها المدرسة، واستخدامها وقت الحاجة إليها)، ويمكن تحقيق تلك الغاية من خلال الأهداف الإستراتيجية التالية:

أ- تدريب العاملين في المدرسة الثانوية الصناعية على استخدام وسائل التكنولوجيا الحديثة والحفاظ عليها، وذلك بناءً على احتياجاتهم التدريبية.

ب-اكتشاف مصادر الحصول على برمجيات حديثة وأصلية تساعد العاملين على إدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية.

ج- تدريب العاملين على استخدامها، وتشفيرها، واسترجاعها وقت الحاجة.

د- تشجيع العاملين الحاصلين على تدريب في مراكز التدريب الرسمية على تبادل الخبرة مع زملائهم؛ مما يعمل على تعميم أثر التدريب على عدد أكبر من العاملين، وذلك داخل وحدة التدريب في المدرسة الثانوية الصناعية.

هـ- قياس أثر التدريب بعد انتهاء البرنامج، للتأكد من انعكاس ما تم الحصول عليه في البرنامج التدريبي على الممارسات الفعلية للعاملين في الحفاظ على أمن المعلومات.

و- تحديث قواعد البيانات الموجودة في المدرسة، والتدقيق فيما تحويه من بيانات، وتحديثها باستمرار؛ وذلك لضمان رشد القرار الذي سيتم اتخاذه بناء عليها.

الغاية الثالثة ـ (إعداد خطة شاملة تركز على التنسيق الدائم بين وزارة التربية والتعليم والوزارات الأخرى، والهيئات المعنية، والشركات، والمصانع من أجل المساهمة في تحقيق إدارة فعالة لعمليات الأمن المعلوماتي)، ويمكن تحقيق تلك الغاية من خلال الهدف الإستراتيجي التالي:

أ. عقد شراكة وبرتوكولات تعاون بين وزارة التربية والتعليم والجهات المعنية الأخرى، وخاصةً تلك التي تمتلك إمكانات مادية تسهم في تجهيز المدارس، وتوفير عقود الصيانة، وبرامج التدريب، وتجهيز قاعات التدريب بما تحتاجه من إمكانات.

الغاية الرابعة ـ (الاستغلال الأمثل لإمكانيات المدرسة الثانوية الصناعية؛ بما يسهم في إدارة عمليات الأمن المعلوماتي بها)، ويمكن تحقيق تلك الغاية من خلال الأهداف الإستراتيجية التالية:

أ. التنسيق بين الوحدات المدرسية المختلفة، مثل وحدة إدارة الأزمات في المدرسة الثانوية الصناعية، وذلك لما لها من دور في جمع البيانات والمعلومات التي من شأنها التنبؤ بالمشكلات والأزمات قبل حدوثها، ووحدة المعلومات والإحصاء باعتبارها المكان المسئول عن حفظ كل المعلومات التي تمتلكها المدرسة.

ب. استثمار الوحدات المدرسية الأخرى الموجودة في المدرسة، مثل: وحدة تيسير الانتقال لسوق العمل، ووحدة الإرشاد المهني، ووحدة ريادة الأعمال في تقديم البرامج التدريبية الخاصة بتدريب العاملين على استخدام الأجهزة التكنولوجية الحديثة، واستخدام برامج إنشاء قواعد البيانات وتشفيرها واسترجاع ما بها من بيانات ومعلومات عند الحاجة.

الغاية الخامسة: (دعم الثقافة التنظيمية للعاملين في المدرسة الثانوية الصناعية عن أهمية المعلومات، للحفاظ على الأمن المعلوماتي)، ويمكن تحقيق تلك الغاية من خلال الأهداف الإستراتيجية التالية:

أ. توعية العاملين بأهمية المعلومات للمدرسة الثانوية الصناعية، وخاصةً القائمين على اتخاذ القرارات.

ب. دعم ولاء العاملين وانتمائهم للمدرسة الثانوية الصناعية، وذلك من خلال إشراكهم في صنع القرار، والأخذ بآرائهم المختلفة لحل مشكلات المدرسة، وبالتالي الشعور بمسئولياتهم تجاه ما يتم اتخاذه من قرارات تخص المدرسة.

5. ملامح الإستراتيجية:

يعرض الجدول التالي ملامح الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدارس الثانوية الصناعية في مصر، من حيث: الغايات، والأهداف الإستراتيجية، والأهداف الإجرائية، وكذلك أنشطة التنفيذ، ومؤشرات الإنجاز، والمدى الزمني المقترح لتنفيذها:

جدول رقم (10)

الإستراتيجية المقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر

الغاية الأولى ـ (دعم التوجه اللا مركزي في إدارة المدرسة الثانوية الصناعية في مصر، الأمر الذي يتيح للمدير والمرؤوسين وكل المستويات الإدارية الأخرى المشاركة في التخطيط لإدارة عمليات الأمن المعلوماتي في المدرسة).

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمنى المقترح
أ. اتباع أسلوب التفويض الإداري من الرؤساء للمرؤوسين، وذلك من خلال وضع الخطوط العريضة لإدارة عمليات الأمن المعلوماتي في المدرسة	• تكليف مدير المدرسة لبعض المعلمين، والوكلاء، والهيئة الإدارية، ومسئولي الوحدات المدرسية المستحدثة بوضع إستراتيجية لإدارة عمليات الأمن المعلوماتي في المدرسة ومتابعة تنفيذها. • تدوير السلطة بين الفرق المدرسية لضمان مشاركة الجميع في وضع تلك الإستراتيجية ومتابعة تنفيذها. • التزام الهيئات الإدارية العليا بالوزارة والمديرية والإدارة بترك بعض الحرية للمدير لإدارة	• تفعيل القوانين والتشريعات التي تدعو لتحقيق اللا مركزية والإدارة الذاتية للمدرسة بما يتيح لها الحرية المطلوبة للمشاركة والتعاون. • عمل اجتماعات دورية بين أعضاء الفريق المحدد لوضع بنود الإستراتيجية وسبل متابعتها. • عقد ورش عمل حول كيفية بناء الإستراتيجية، وكيفية اختيار الأساليب المناسبة للمتابعة. • كتابة تقارير دورية من قبل الفريق المكلف بإدارة عمليات الأمن المعلوماتي عن الإنجازات	• وجود خطة أساسية وخطط بديلة جاهزة للتنفيذ لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية. • وجود محاضر الاجتماعات التي جمعت أعضاء الفريق، والتي تتضمن مراحل وضع الخطة. • وجود تقارير فعلية من قبل أعضاء الفريق عن الخطة وسبل متابعتها. • وجود عدد من المقترحات للتغلب على العقبات التي واجهت تطبيق الخطة من	وزارة التربية والتعليم، ومدير المدرسة، والمسئولين عن حفظ البيانات والمعلومات في المدرسة، والفريق المكلف بإعداد الإستراتيجية ومتابعتها من المعلمين والإداريين والوكلاء، ومسئولي وحدة التدريب والتقويم والجودة؛ حيث إنهم المسئولون عن تقديم ورش العمل.	مستمر

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمنى المقترح
الثانوية الصناعية.	عمليات الأمن المعلوماتي لديه وفقًا لرؤيته، ورؤية مرؤوسيه وظروف مدرسته.	ونقاط الضعف، وما أسفرت عنه متابعة الإستراتيجية. • تقديم كل مدير مدرسة صناعية تقرير ختامي للجهات الإدارية الأعلى عن إنجازات المدرسة في مجال إدارة عمليات الأمن المعلوماتي لديها، وما واجهته من مشكلات؛ للاستفادة منه في الخطط القادمة.	قبل الهيئات الإدارية الأعلى لمساعدة المدرسة في التغلب على مثل تلك العقبات عند إعداد الخطط المستقبلية؛ لإدارة عمليات الأمن المعلوماتي.		
ب. تشجيع المرؤوسين على المستويات كافة (المديرية، الإدارة، المدرسة) للمشاركة في صنع القرار، وبالتالي إبداء الرأي، في سبيل تحقيق إدارة فعالة للأمن المعلوماتي في	• دعوة المرؤوسين على المستويات كافة لحضور اجتماعات صنع القرار، المنعقدة للحصول على آرائهم، في إطار الحفاظ على الأمن المعلوماتي للمدرسة. • الأخذ بآراء المرؤوسين على المستويات كافة، خاصةً إن كانت أفكارًا جديدة ومتنوعة في مجال الحفاظ على أمن المعلومات.	• الحوارات والمناقشات واجتماعات العصف الذهني؛ لتوليد المزيد من الأفكار حول الحفاظ على أمن المعلومات في المدرسة الثانوية الصناعية.	• الأفكار الجديدة والمقترحات التي من شأنها الحفاظ على المعلومات الموجودة في المدرسة الثانوية الصناعية، والمثبتة بمحاضر الاجتماعات.	• مدير المدرسة مع مرؤوسيه. • مدير الإدارة التعليمية مع مديري المدارس الثانوية الصناعية. • مدير المديرية مع مديري الإدارات التعليمية. • وكيل الوزارة مع مديري المديريات	مستمر

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمنى المقترح
المدرسة.				التعليمية.	
ج. إلحاق المسئولين عن حفظ المعلومات في المدرسة الثانوية الصناعية ببرامج تدريبية، تمكنهم من تصنيف المعلومات، ومعرفة درجة حساسيتها، ومن ثم التخطيط لاستخدامها وتخزينها في ضوء ذلك.	• تحديد الاحتياجات التدريبية للمسئولين عن البيانات والمعلومات في المدرسة الثانوية الصناعية؛ لمعرفة أولويات الموضوعات التي يريدون التدرب عليها. • إجراء عدد من البرامج التدريبية لهم داخل المدرسة مع الاستعانة بخبرات وحدة التدريب والتقويم والجودة الموجودة في المدرسة. • ترشيحهم للحصول على دورات تدريبية موسعة بهيئات خارجية في: المصانع، والشركات؛ لاستغلال إمكانياتها المادية لإنجاح التدريب. • التركيز في برامج التدريب ـــ المقدمة لمسئولي المعلومات ـ على ضرورة تقدير حساسية المعلومات وتصنيفها وفقًا لذلك.	• البرامج التدريبية المختلفة التي يقرها التحليل الإحصائي لاستمارات تحديد الاحتياجات التدريبية، سواء داخل وحدة التدريب والتقويم والجودة في المدرسة أو في الهيئات الخارجية. • قاعدة بيانات بأهم الهيئات والمؤسسات التي من الممكن استغلالها لتقديم البرامج التدريبية خارج المدرسة. • وضع بعض البرامج التدريبية الإضافية للعاملين، حتى وإن لم يتخيروها، مثل تلك المختصة بتصنيف خطورة المعلومات وحساسيتها.	• استمارات تحديد الاحتياجات التدريبية للمتدربين. • نتائج التحليل الإحصائي لاستمارات تحديد الاحتياجات التدريبية. • توافر الحقائب التدريبية الخاصة بالموضوعات المختارة. • توافر قاعدة بيانات عن الهيئات والمؤسسات التي من الممكن الاستعانة بها، لتقديم البرامج، على أجهزة المدرسة، وعمل نسخ احتياطية منها على وسائط تخزين خارجية، مثل: أقراص صلبة خارجية، أو أقراص مدمجة.	• المسئولون عن وحدة التدريب والتقويم والجودة في المدرسة. • المختصون في تقديم البرامج التدريبية التي تتلاءم والموضوعات المختارة. • المسئولون عن إنشاء قواعد البيانات في المدرسة، وحفظها من التلف أو السرقة.	مستمر

الغاية الثانية . (العمل على تنمية قدرات الإمكانات البشرية في المدرسة الثانوية الصناعية، الأمر الذي يمكنهم من الحفاظ على المعلومات التي تمتلكها المدرسة، واستخدامها وقت الحاجة إليها).

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
أ. تدريب العاملين في المدرسة الثانوية الصناعية على استخدام وسائل التكنولوجيا الحديثة والحفاظ عليها، وذلك بناء على احتياجاتهم التدريبية.	• تصميم برامج تدريبية متخصصة في تمكين العاملين من استخدام الوسائل التكنولوجية الحديثة، داخل المدرسة، وبالمصانع والشركات، ومراكز التدريب المتخصصة، وعبر قاعات الفيديو كونفرانس؛ لتوسيع نطاق التدريب. • عقد ورش عمل متخصصة ملحقة بكل برنامج تدريبي للتأكد من ربط الجانب النظري بالجانب التطبيقي.	• تجهيز الحقائب التدريبية. • البرامج التدريبية المتخصصة. • ورش العمل لربط النظرية بالتطبيق.	• التحاق العاملين في البرامج التدريبية التي تركز على استخدام التكنولوجيا المتطورة. • التمكن من تطبيق ما تم الحصول عليه بشكل نظري عمليًا بالمعامل والوحدات المدرسية. • تلاشي الفجوة بين النظرية والتطبيق، وتحقيق التكامل بين الجانبين.	• المسئولون عن وحدة التدريب والتقويم والجودة في المدرسة. • المتخصصون في تقديم موضوعات التدريب من داخل المدرسة، وخارجها. • مركز التطوير التكنولوجي في وزارة التربية والتعليم. • الإدارة العامة لمركز تطوير التعليم الفني.	مستمر
ب. الاهتمام بالحصول على برمجيات حديثة وأصلية تساعد العاملين على إدارة عمليات	• التعاقد مع شركات الكمبيوتر لتوريد برامج أصلية للمدرسة الثانوية الصناعية؛ لمساعدتها على حماية الأجهزة من الفيروسات، وإنشاء قواعد البيانات، وحفظ المعلومات، وتجهيزها، واسترجاعها	• إبرام عقود الشراكة بين المدرسة الثانوية الصناعية، وشركات الكمبيوتر، وذلك لـ: – توفير البرمجيات.	• وجود عقود الشراكة بين المدرسة الثانوية الصناعية والشركات المقصودة. • تصميم البرامج التدريبية اللازمة؛ لتمكين العاملين	• مدير المدرسة والوكلاء. • المسئولون عن إدارة شركات الكمبيوتر. • المسئولون عن	مستمر

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
الأمن المعلوماتي في المدرسة الثانوية الصناعية، وتدريب العاملين على استخدامها، وتشفيرها، واسترجاعها وقت الحاجة.	وقت الحاجة. • تقديم شركة الكمبيوتر ـ التي تم التعاقد معها ـ عدد من برامج التدريب للعاملين الذين سيقومون بالتعامل مع هذه البرامج؛ لتمكينهم من التعامل معها وتحديثها.	– عقد برامج تدريبية للعاملين. • عقد عدد من اللقاءات بين المدرسة الثانوية الصناعية، وتلك الشركات؛ للبحث عن سبل تفعيل الشراكات.	من استخدام تلك البرمجيات. • تنفيذ البرامج التدريبية اللازمة لتمكين العاملين من استخدام تلك البرمجيات.	الوحدات المدرسية، حيث إنهم من سيتلقون تلك البرامج التدريبية.	
ج. الاستفادة من خبرات العاملين الحاصلين على تدريب في مراكز التدريب الرسمية لتدريب زملائهم، وتعميم أثر التدريب على عدد أكبر من العاملين، وذلك داخل وحدة التدريب في المدرسة الثانوية الصناعية.	• قيام وحدة التدريب بعمل حصر بأسماء العاملين الحاصلين على برامج التدريب في مجال الحفاظ على البيانات والمعلومات. • عمل حصر بأهم المهارات التي حصل عليها هؤلاء المتدربون؛ لمعرفة مجال الفائدة التي يمكن أن يبرعوا فيه. • تصميم بعض البرامج التدريبية المنبثقة من البرامج التي حصل عليها المتدربون لتقديمها للعاملين من غير الحاصلين على البرامج التدريبية. • تنفيذ البرامج التدريبية بوحدة التدريب. • قياس أثر التدريب بعد انتهاء البرنامج؛	• توفير الحوافز المادية والمعنوية للمدربين؛ لتشجيعهم على القيام بالمهمة على الوجه الأكمل. • قيام القائمين على التدريب بعمل تقارير عن كل برنامج يقومون بتقديمه، ومدى اتفاقه مع الهدف العام الخاص بالتمكن من مهارات الحفاظ على البيانات والمعلومات. • إبداء رأي المتدربين حول	• وجود قائمة بالأفراد الحاصلين على التدريب والمهارات التي تمكنوا منها. • عمل حصر بالأفراد الذين حصلوا على التدريب على يد زملائهم المتدربين بجهات خارجية، وتحديد أهم المهارات التي تمكنوا منها. • قياس رضا العاملين عن تلك البرامج، ومعرفة ما إذا كانت تتفق واحتياجاتهم التدريبية.	• العاملون الحاصلون على تدريب بمراكز التدريب المختلفة. • المسئولون بوحدة التدريب والتقويم والجودة في المدرسة.	عام واحد

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
	للتأكد من فاعلية هذا البرنامج، وللتأكد من تعميم الفائدة على عدد أكبر من العاملين.	البرنامج التدريبي الذي حصلوا عليه؛ لمعرفة جوانب القوة والضعف فيه، لتدعيم جوانب القوة، والتغلب على جوانب الضعف، ومن ثم تنقيح البرنامج المقدم.			
د. الاهتمام بقياس أثر التدريب بعد انتهاء البرنامج للتأكد من انعكاس ما تم الحصول عليه في البرنامج التدريبي على الممارسات الفعلية للعاملين في الحفاظ على أمن المعلومات.	• تقويم البرامج التدريبية المقدمة للعاملين. • تعديل البرامج التدريبية المقدمة للعاملين وفقًا لأهداف تلك البرامج، ووفقًا لتوقعات العاملين منها. • وضع معايير ثابتة لتقويم البرامج التدريبية، التي يتم على أساسها الحكم على تلك البرامج.	• عمل مقاييس من شأنها قياس أثر كل برنامج تدريبي بعد انتهائه. • ملاحظة أداء العاملين بعد عودتهم من البرنامج التدريبي؛ لمعرفة مدى قدرتهم على تطبيق ما تم الحصول عليه في البرنامج التدريبي في ممارساتهم اليومية. • استطلاع رأي المتدربين حول البرنامج الذي حصلوا عليه، وذلك للحكم على مدى جودته من وجهة	• وجود مقاييس من شأنها الحكم على جودة البرامج التدريبية المقدمة. • وجود مقاييس أخرى للحكم على جودة أداء المتدربين بعد حصولهم على البرنامج.	• المسئولون بوحدة التدريب والتقويم والجودة.	شهر بعد انتهاء البرنامج التدريبي لتطبيق المقاييس والحكم على أداء الأفراد.

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
		نظرهم.			
هـ. التركيز على ضرورة تحديث قواعد البيانات الموجودة في المدرسة والتدقيق فيما تحويه من بيانات، وتحديثها باستمرار، وذلك لضمان رشد القرار الذي سيتم اتخاذه بناء عليها.	• عمل قواعد بيانات دقيقة تحتوي على بيانات حديثة. • الاعتماد على ما يوجد بتلك القواعد من بيانات ومعلومات للحصول على قرار رشيد.	• استخدام برامج إلكترونية خاصة لإنشاء قواعد البيانات؛ وذلك للمحافظة على البيانات التي تمتلكها المدرسة. • التمكن من استرجاع المعلومات وقت الحاجة إليها للتمكن من اتخاذ القرار الرشيد بناءً عليها.	• وجود قواعد بيانات دقيقة ومحدثة تحوي البيانات والمعلومات التي تمتلكها المدرسة. • قدرة العاملين على استرجاع المعلومات وقت الحاجة إليها. • رشد القرارات التي تتخذها إدارة المدرسة بناء على المعلومات التي تمتلكها. • عدد القرارات التي تتخذها إدارة المدرسة وقت الحاجة، ومدى ملاءمتها لظروف المدرسة وإمكاناتها.	• المسئولون عن حفظ البيانات والمعلومات واسترجاعها وقت الحاجة في الوحدات المختلفة في المدرسة الثانوية الصناعية. • مدير المدرسة والوكلاء.	مستمر

الغاية الثالثة: (العمل على إعداد خطة شاملة، تركز على التنسيق الدائم بين وزارة التربية والتعليم والوزارات الأخرى، والهيئات المعنية، والشركات، والمصانع؛ من أجل المساهمة في تحقيق إدارة فعالة لعمليات الأمن المعلوماتي)

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
أ. الاهتمام بعمل عقود شراكة، وبرتوكولات تعاون بين وزارة التربية والتعليم والجهات المعنية الأخرى وخاصةً تلك التي تمتلك إمكانات مادية تسهم في تجهيز المدارس، وتوفير عقود الصيانة، وبرامج التدريب، وتجهيز قاعات التدريب بما تحتاجه من	• الاهتمام بالاستغلال الأمثل للإمكانيات المادية التي تمتلكها الوزارة، والمصانع، والشركات؛ من أجل تجهيز المدارس، وتوفير البرامج التدريبية وتنفيذها.	• عمل قواعد بيانات تهتم بحصر الإمكانات المادية والبشرية التي يمكن الاستعانة بها لتجهيز المدارس، وتدريب العاملين. • إعطاء المدرسة بعض المميزات للشركات المنوط بها إبرام الشراكة معها، مثل الإعلان المجاني عن منتجاتها للعملاء من أولياء	• الاعتماد على الإمكانات البشرية المؤهلة والمدربة، التي من شأنها المساهمة في تحقيق أهداف الخطة الشاملة لأمن المعلومات للمدرسة. • وجود قواعد بيانات تحدد أسماء الشركات	• وزارة التربية والتعليم. • شركات الكمبيوتر المعنية. • الهيئات والمؤسسات القادرة على تقديم الدعم للمدارس سواء بالتجهيزات، أو من خلال تقديم برامج التدريب مثل مؤسسات المجتمع المدني.	**مستمر**

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
إمكانيات.	• تحديد أهم الشركات التي يمكن التعاون معها، والاستعانة بها لصيانة الأجهزة الموجودة في المدرسة. • تحديد مجالات الاستفادة المتبادلة التي ستحصل عليها كل من المدارس والشركات في حالة وجود عقود الشراكة بينهما. • إحداث قدر من التكامل والتنسيق بين الهيئات كافة؛ وذلك لتلاشي الانفصال بين الجهود المختلفة.	الأمور، والطلاب، والمعلمين، والعاملين أيضًا. • التحديد الدقيق لبنود الشراكة، بحيث يتم تحديد مجالات الإفادة والاستفادة لكل طرف، ومن ثم ضمان التزام كل منهم تجاه الآخر. • إجراء مسوحات لاستطلاع رأي تلك الشركات والهيئات؛ لمعرفة رغباتها، واحتياجاتها، ومحاولة تضمينها بعقود الشراكة. • رقابة وزارة التربية والتعليم على سير تلك الشراكات ومدى جودتها، وإزالة كافة العوائق أمام تنفيذها.	التي يمكن عمل الشراكات وبروتوكولات التعاون معها. • وجود معايير محددة للمفاضلة بين تلك الشركات لمعرفة أفضلها لعقد البروتوكول. • وجود قوانين وتشريعات يتم على أساسها ضمان تحقيق الفائدة لأطراف الشراكة.		

الغاية الرابعة (الاستثمار الأمثل لإمكانيات المدرسة الثانوية الصناعية بما يسهم في إدارة عمليات الأمن المعلوماتي بها)

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
• التنسيق بين الوحدات المدرسية المختلفة، مثل وحدة إدارة الأزمات في المدرسة الثانوية الصناعية، وذلك لما لها من دور في جمع البيانات والمعلومات التي من شأنها التنبؤ بالمشكلات والأزمات قبل حدوثها، ووحدة المعلومات والإحصاء باعتبارها	• التكامل في الأداء بين الوحدات المدرسية المستحدثة. • التنسيق بين العاملين في تلك الوحدات؛ لتحقيق أهداف الحفاظ على المعلومات واسترجاعها وقت الحاجة إليها. • الاستعداد للمشكلات والأزمات قبل حدوثها، عن طريق المعلومات التي تملكها المدرسة؛ على اعتبار أنها الوسيلة المثلى لاتخاذ القرار الرشيد.	• تفعيل القوانين والتشريعات التي تدعو إلى تمكين العاملين، وحريتهم واستقلالهم، ودعم مشاركتهم في صنع القرار. • وضع خطة للاستعداد للمشكلات والأزمات المتوقع أن تواجهها المدرسة بناء على واقعها وظروفها الحالية، وذلك بالتعاون والتنسيق بين الوحدات المسئولة عن حفظ المعلومات في المدرسة. • عقد اجتماعات دورية بين هؤلاء المسئولين؛ لتبادل الخبرة، والاستعداد	• زيادة عدد المشاركين في صنع القرارات المدرسية. • وجود تقارير مستمرة توضح التوقعات عن حالة المدرسة الثانوية الصناعية بناءً على المعلومات المتاحة. • وجود عدد من الخطط الجاهزة للتنفيذ لمواجهة المشكلات والأزمات التي قد تواجه المدرسة، وتحديد سبل متابعتها. • العمل على تقويم تلك الخطط باستمرار؛ للوقوف على نقاط القوة والضعف فيها، وتصحيحها بما يتوافق مع	• وزارة التربية والتعليم. • مدير المدرسة. • المسئولون بوحدة إدارة الأزمات في المدرسة الثانوية الصناعية. • المسئولون عن وحدة المعلومات والإحصاء في المدرسة.	مستمر

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
المكان المسئول عن حفظ المعلومات التي تمتلكها المدرسة كافة.	• إعطاء مزيد من الحرية والاستقلالية للعاملين بشكل عام، والعاملين بالوحدات المسئولة عن حفظ البيانات والمعلومات للمشاركة في صنع القرار؛ حيث إنهم أقرب الفئات للواقع، والأقدر على توقع مستقبله.	للمشكلات. • وضع تقارير عن الأنشطة التي قام بها المسئولون للاسترشاد بها في صنع القرارات واتخاذها.	احتياجات المدرسة، وبما يتلاءم مع شكل المعلومات الموجودة في المدرسة، ودرجة حساسيتها.		
• استغلال الوحدات المدرسية الأخرى الموجودة في المدرسة ـ التي تمتلك بعض الأجهزة التكنولوجية، مثل: وحدة تيسير الانتقال لسوق العمل، ووحدة الإرشاد المهني، ووحدة ريادة الأعمال ـ في تقديم	• استثمار القدرات التكنولوجية في الوحدات المدرسية في تنفيذ برامج لتدريب العاملين بالفعل على التمكن من استخدام الأجهزة التكنولوجية الحديثة، وحفظ المعلومات، واستغلالها وقت الحاجة. • إمداد الأجهزة الموجودة في تلك الوحدات في البرامج الحديثة المسئولة عن حفظ البيانات، وتحديثها	• عمل حصر بعدد الأجهزة الموجودة في الوحدات المدرسية المستحدثة في المدرسة. • عمل حصر بالإمكانات الحالية للأجهزة الموجودة بتلك الوحدات. • تحديث الأجهزة الموجودة فيتلك الوحدات، للاستفادة المثلى منها أثناء تنفيذ التدريب. • إمداد الأجهزة بالبرامج اللازمة	• توافر عدد كاف من أجهزة الكمبيوتر الصالحة لإجراء برامج التدريب عليها. • توافر البرمجيات الحديث اللازمة للتدريب على الأجهزة الموجودة بالوحدات. • تنفيذ خطة التدريب المعدة مسبقًا. • وجود حصر بعدد المتدربين بالوحدات والمهارات التي حصلوا عليها. • وجود رضا عن محتوى البرامج	• وزارة التربية والتعليم • مدير المدرسة. • الشركات المسئولة عن تجهيز المدرسة بما تحتاجه من تجهيزات تكنولوجية • منظمات المجتمع المدني.	مستمر

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
البرامج التدريبية الخاصة بتدريب العاملين على استخدام الأجهزة التكنولوجية الحديثة، واستخدام برامج إنشاء قواعد البيانات وتشفيرها واسترجاع ما بها من بيانات ومعلومات عند الحاجة.	باستمرار؛ لضمان تدريب العاملين على أحدث شكل لتلك البرامج. ● تدريب العاملين على السبيل الأمثل لتشفير البيانات والمعلومات، وفك تلك الشفرة عند الحاجة لذلك.	عند التدريب، كبرامج إنشاء قواعد البيانات، والتشفير، واسترجاع البيانات، وتصنيف البيانات والمعلومات وفقًا لدرجة حساسيتها. ● عمل خطة للتدريب على تلك الموضوعات تحدد أولويات تقديم الموضوعات حسب الاحتياجات التدريبية للمتدربين.	التدريبية التي حصل عليها العاملون. ● تقليل الفجوة بين الاحتياجات التدريبية للمتدربين، وبين ما يحصلون عليه من برامج تدريب فعلية.		

الغاية الخامسة:(دعم الثقافة التنظيمية للعاملين في المدرسة الثانوية الصناعية عن أهمية المعلومات، ومن ثم إدارة عمليات الأمن المعلوماتي)

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
أ. توعية العاملين بأهمية المعلومات للمدرسة الثانوية الصناعية، وخاصةً لمتخذي	● توفير فرص للمناقشة والحوار بين مدير المدرسة والعاملين على كل المستويات، بحيث تدور تلك والمناقشات حول الثروة المعلوماتية التي تمتلكها المدرسة، وكيفية استخدامها.	● عمل ندوات ولقاءات مستمرة للعاملين توضح لهم أهمية المعلومات، ومدى تأثيرها على قدرة المدرسة لاستعادة نشاطها.	● تعامل العاملين في المدرسة الثانوية الصناعية مع المعلومات بقدر من	● مدير المدرسة. ● الوكلاء. ● المسئولون	

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
القرار، وفي الأوقات التي تحتاج المدرسة فيها لاستعادة نشاطها.	• توضيح الإجراءات التي على كل عامل في المدرسة اتباعها؛ للحفاظ على البيانات والمعلومات التي تقع في نطاق مسئوليته. • الاستفادة من الخبرات الناجحة في هذا المجال، الأمر الذي يعظم من دور المعلومات فعليًا، ويقنع العاملين عمليًا بضرورة حماية المعلومات السرية، التي لا يمكن للجميع الاطلاع عليها. • عرض الخبرات السلبية التي أهملت الحفاظ على المعلومات، ومن ثم افقدت المنظمة قدرتها على استعادة نشاطها، وتعافيها من أزماتها.	• عرض بعض التجارب الناجحة للمدارس التي استعادت نشاطها وتعافت سريعًا بعد مرورها بأزمة أو أكثر اعتمادًا على المعلومات. • تزويد العاملين بكتيبات إرشادية توضح لهم درجات تصنيف المعلومات وفق خطورتها. • رفع درجة المحاسبية للعاملين غير القادرين على حفظ البيانات والمعلومات في مأمن من السرقة أو التلف، وتعريضهم للعقاب لإخلالهم بواجبات وظيفتهم.	الحذر، واستخدام معايير ثابتة للحكم على مدى حساسيتها وخطورتها، وبالتالي عدم نشر المعلومات الحساسة والخطرة التي قد تعرض المدرسة للمشكلات. • الإقبال على حضور الندوات التثقيفية واللقاءات التي تدور حول رفع وعي العاملين بأهمية المعلومات ودورها في الحفاظ على حياة المدرسة.	عن الوحدات المدرسية المستحدثة.	مستمر
ب. دعم ولاء العاملين وانتمائهم للمدرسة الثانوية	• تمكين العاملين في المدرسة في عمليات صنع القرار، وبالتالي شعورهم بالمسئولية تجاه المدرسة. • تفعيل الاجتماعات المدرسية بالقدر الذي يتيح	• تشريع القوانين التي من شأنها تفعيل قدرة العامل ـ على المستويات كافة ـــ على المشاركة الفعالة في صنع	• زيادة مشاركة العاملين في صنع القرارات التي من شأنها الإدارة	• وزارة التربية والتعليم • المسئولون في	

الأهداف الإستراتيجية	الأهداف الإجرائية	أنشطة التنفيذ	مؤشرات الإنجاز	مسئولية التنفيذ	المدى الزمني المقترح
الصناعية، من خلال إشراكهم في صنع القرار، والأخذ بآرائهم المختلفة لحل مشكلات المدرسة، وبالتالي الشعور بمسئولياتهم تجاه ما يتم اتخاذه من قرارات تخص المدرسة.	لجميع العاملين إبداء الرأي. • تشجيع العاملين على كتابة المقترحات اللازمة للحفاظ على الأمن المعلوماتي في المدرسة، الأمر الذي يشعرهم بمزيد من الانتماء للمدرسة.	القرار. • إحكام الرقابة من الجهات الإدارية العليا من الإدارة والمديرية، للتأكد من عدم صورية الاجتماعات المدرسية، وأنها عقدت للاستفادة من آراء العاملين. • النظر في مقترحات العاملين باستمرار، ومحاولة تنفيذ ما يصلح منها في شكل مشروعات ومبادرات يقوم بها العاملون من أجل تحقيق الصالح العام للمدرسة. • تخصيص جوائز لأفضل المقترحات والمشاركات التي يقدمها العاملون عن أفضل السبل لإدارة عمليات الأمن المعلوماتي في المدرسة.	الفعالة للأمن المعلوماتي في المدرسة. • الزيارات المتتالية من قبل المسئولين في المديرية والإدارة لمعرفة جدوى الممارسات الديمقراطية في المدرسة، ومدى جديتها، وما تم تنفيذه منها. • المنافسة المستمرة بين العاملين؛ لتقديم أفضل الأفكار باستمرار للحصول على الجوائز نتيجة ما يقدمونه من أفكار ومقترحات.	المديريات التعليمية والإدارات. • مدير المدرسة • العاملون على مختلف المستويات.	مستمر

6. متطلبات تنفيذ الإستراتيجية المقترحة.

إن ثمة متطلبات ينبغي توفرها ـ تتضح من خلال الدراسة النظرية والميدانية ـ لتطبيق الإستراتيجية لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في مصر، وربما يكون من أهم تلك المتطلبات ما يلي:

- توفير التمويل اللازم لتجهيز مدارس التعليم الثانوي الصناعي بما تحتاج إليه من تجهيزات، وأجهزة، وبرمجيات حديثة.
- التخفيف من حدة المركزية التي تعاني منها إدارة التعليم بشكل عام، ومن ثم إعطاء مزيد من الحرية لمدير المدرسة، ومرؤوسيه للمشاركة، والاستقلالية في التخطيط، وصناعة القرارات التي تخص الحفاظ على المعلومات التي تمتلكها المدرسة.
- وعي مدير المدرسة الثانوية الصناعية، والمعلمين والإداريين بأهمية المعلومات، وأمنها، والحفاظ عليها، واستخدامها في استعادة نشاط المدرسة بعد تعرضها للمشكلات والأزمات.
- ضرورة توفير البنية التحتية اللازمة للحفاظ على المعلومات، والتنويع بين سياسات الحفاظ على أمن المعلومات لتوفير أكثر من فرصة وأكثر من طريقة للحفاظ على المعلومات واستخدامها وقت الحاجة.
- حث المرؤوسين على المشاركة في عمليات التخطيط للأمن المعلوماتي، وصنع القرارات التي تخص المدرسة؛ بما يشعرهم بالانتماء للمدرسة، والعمل من أجل صالحها العام.
- إعداد قاعدة بيانات شاملة عن أهم الجهات التي يمكن التواصل معها أثناء حدوث الأزمات؛ وذلك استعدادًا للأزمات قبل حدوثها، على أن يتم مراجعة تلك البيانات، والالتزام بتحديثها باستمرار.
- توافر بطاقات توصيف وظيفي دقيقة تحدد للعاملين بالوحدات المدرسية المستحدثة ـ خاصةً تلك التي تتعامل مع المعلومات وتلتزم بالحفاظ عليها ـ ما يجب عليهم القيام به عند القيام بحفظ البيانات والمعلومات وتخزينها تخزينًا آمنًا يحميها من السرقة أو التلف.

- التدريب المستمر للعاملين في قطاع المعلومات على تصنيف المعلومات وفقًا لخطورتها، ومعرفة أي المعلومات يمكن الإفصاح عنه، وأيها يجب تخزينه والاحتفاظ به لحين حاجة المدرسة إليه.
- تدريب العاملين في قطاع المعلومات على التعامل مع البرمجيات الحديثة التي تتعامل مع حفظ المعلومات، وتشفيرها، واستعادتها وقت الحاجة إليها.
- تفعيل عمليات محاسبة العاملين في قطاع المعلومات، خاصةً المقصرين في الحفاظ على أمن المعلومات، وفي حالة تسرب المعلومات التي تقع في نطاق مسئولياتهم.
- تقويم قدرة المدرسة باستمرار على الحفاظ على أمنها المعلوماتي بناءً على معايير ثابتة، وبناءً على مقارنة قدراتها في هذا الإطار بممارسات المدارس الأفضل التي استطاعت الحفاظ على أمنها المعلوماتي محليًا ودوليًا.
- الاهتمام بالتنسيق المستمر بين وزارة التربية والتعليم وباقي الوزارات والقطاعات الاقتصادية، والهيئات المعنية؛ لتحقيق إدارة فعالة للأمن المعلوماتي.

سابعًا- معوقات تنفيذ الإستراتيجية المقترحة وسبل مواجهتها:

توصلت الدراسة النظرية والميدانية لعدد من الصعوبات التي قد تعوق تنفيذ الإستراتيجية المقترحة، والتي يجب أن تؤخذ بعين الاعتبار أثناء التنفيذ، وهي كما يلي:

- ضعف البنية التحتية والتجهيزات الموجودة في المدرسة الثانوية الصناعية، **وللتغلب على ذلك** يمكن الاستعانة بمصادر تمويل إضافية، مثل: المساعدات التي تقدمها القطاعات الاقتصادية كالشركات والمصانع، في هيئة برامج تدريبية وتجهيزات للمدرسة، وشركات الكمبيوتر في هيئة أجهزة وبرمجيات، الأمر الذي يتطلب مزيدًا من التنسيق بين تلك الجهات وبعضها.
- تزايد حدة المركزية على المستويات الإدارية كافة، الأمر الذي يحد من فرصة مدير المدرسة والمرؤوسين على المشاركة، **وللتغلب على ذلك**، يمكن وضع عدد من التشريعات التي تعطي لمدير المدرسة ومرؤوسيه فرصة لإدارة مدرستهم ذاتيًا، الأمر الذي يتيح لهم الفرصة على المشاركة وإشراك العاملين في صنع القرار، ومن ثم التغلب على المشكلات التي تواجه المدرسة، عن طريق الحفاظ على البيانات والمعلومات.

- ضعف دراية العاملين بأهمية المعلومات وأهمية الحفاظ عليها؛ مما يجعلها عرضة للتلف أو السرقة، **ويمكن التغلب على ذلك** من خلال تقديم عدد من برامج التوعية، والندوات التثقيفية الموجهة للعاملين لتوعيتهم بأهمية المعلومات، ومخاطر تسربها.
- ضعف قدرة قواعد البيانات الموجودة في المدرسة عن أهم الهيئات وجهات الاتصال التي يمكن الاستعانة بها وقت الأزمات، **ويمكن التغلب على ذلك** من خلال الاهتمام بالحصول على برمجيات إنشاء قواعد البيانات، وتدريب العاملين على استخدامها، وحفظ المعلومات بها، وتحديث ما بها من بيانات ومعلومات باستمرار.
- ضعف الحماية والتأمين اللازمين للبيانات والمعلومات الخاصة في المدرسة من السرقة، **ويمكن التغلب على ذلك** من خلال تأمين الحجرات التي تحوي الأجهزة التي تضم المعلومات المدرسية، مع الاهتمام بتخصيص أماكن لها بعيدًا عن الورش والمعامل المعرضة للحوادث، بالإضافة إلى تدريب العاملين على تشفير تلك البيانات والمعلومات، والاحتفاظ بنسخ احتياطية منها في أماكن آمنة لحين الحاجة إليها.
- تركيز معظم برامج التدريب الموجهة للعاملين في المدرسة الثانوية الصناعية على الجوانب النظرية، دون الاهتمام بربط النظرية بالتطبيق، **ويمكن التغلب على ذلك** من خلال عقد العديد من ورش العمل للمتدربين لتطبيق ما تم الحصول عليه بشكل نظري عمليًا؛ وذلك لتشجيعهم على التنفيذ الفعلي لما ورد في البرنامج التدريبي بعد العودة إلى المدرسة، لأداء مهامهم الوظيفية.
- ضعف قدرة المسئولين في المدرسة الثانوية الصناعية على التنبؤ بالمشكلات قبل حدوثها، الأمر الذي يؤدي إلى تصاعدها بشدة، وتحولها إلى أزمة بشكل سريع، **ويمكن التغلب على ذلك** من خلال التنسيق المستمر بين أداء وحدة الأزمات من ناحية، ووحدة المعلومات والإحصاء من ناحية أخرى، لإحداث التكامل الذي يؤدي إلى توقع أفضل للمشكلات، وتلافي الأزمات التي قد تهدد قدرة المدرسة على تقديم خدماتها التعليمية.
- قلة عقود الصيانة الموجودة بين المدارس الثانوية الصناعية والشركات التي من شأنها صيانة الأجهزة، الأمر الذي يوضح أن تعطلها قد يودي بحياة

المعلومات، ويؤدي إلى فسادها، **ويمكن التغلب على ذلك** من خلال عقد مزيد من عقود الشراكة بين المدارس الثانوية الصناعية، والشركات المنوط بها تقديم خدمة الصيانة للمدارس، أو المساهمة في تقديم التجهيزات، أو برامج التدريب، مع توضيح مجالات الاستفادة التي سيحظى بها الطرفان، الأمر الذي يثير حماسة كل طرف في تنفيذ بنود الشراكة.

خلاصة:

في إطار البحث الحالي تم التوصل إلى إستراتيجية مقترحة لإدارة عمليات الأمن المعلوماتي في المدرسة الثانوية الصناعية في جمهورية مصر العربية، وذلك باستخدام أسلوب التحليل الرباعي، الذي اعتمد على تحليل البيئة الداخلية، ومعرفة نقاط القوة والضعف، وتحليل البيئة الخارجية من خلال معرفة الفرص والتهديدات؛ وذلك للتوصل لإدارة فعالة لعمليات الأمن المعلوماتي، والقدرة على استغلال المعلومات وقت الحاجة إليها، على اعتبار أنها المخزون الذي تستطيع المدرسة الاعتماد عليه، خاصةً وقت تعافيها من الأزمات التي قد تتعرض لها.

مراجع البحث

(1) Ministry of Public Safety and Solicitor General, (2006), Disaster Recovery: Provincial Emergency Program, British Colombia, Ministry of Public Safety and Solicitor General, P. 1.1.

(2) Michael K.Lindell, (2013), Recovery and Reconstruction after Disaster, In, P.T. Bobrowsky, Encyclopedia of Natural Hazards, Vol., XLI England, Springer Publications, P.812.

(3) وزارة التربية والتعليم، (2014) الخطة الإستراتيجية للتعليم قبل الجامعي 2014-2030، القاهرة، وزارة التربية والتعليم، ص 79.

(4) وزارة التربية والتعليم، (2013)، برنامج تطوير التعليم الفني بالتعاون مع وزارة الاتصالات، القاهرة، وزارة التربية والتعليم، ص 2.

(5) وزارة التربية والتعليم، (2013)، برنامج تطوير التعليم الفني بالتعاون مع وزارة الاتصالات، القاهرة، وزارة التربية والتعليم، ص 4.

(6) وزارة التربية والتعليم، (2014)، قرار وزاري رقم 262 لعام 2014، بشأن إنشاء وحدة إدارة الأزمات بالمدارس، القاهرة، وزارة التربية والتعليم.

(7) رئاسة الجمهورية، (2013)، تقرير المجلس القومي للتعليم والبحث العلمي والتكنولوجيا، الدورة الأربعون، القاهرة، المجالس القومية المتخصصة، ص 21.

(8) وزارة الاتصالات وتكنولوجيا المعلومات، (2012) الإستراتيجية القومية للاتصالات وتكنولوجيا المعلومات 2012-2017: المجتمع المصري الرقمي في ظل اقتصاد المعرفة، جمهورية مصر العربية، الإدارة المركزية للبحوث والسياسات والتخطيط الاستراتيجي، ص 48.

(9) محمد جمال الدين درويش، (2009) مصر ومجتمع المعلومات، القاهرة، اللجنة القومية للمعلومات بجامعة القاهرة، ص 23.

(10) المرجع السابق، ص 23

(11) عماد ثروت محمد رضوان، (2009) السلوك القيادي لمديري المدارس الثانوية الصناعية بمصر في التعامل مع الأزمات المدرسية: تصور مقترح، رسالة دكتوراه مقدمة إلى مركز النظم العالمية، ص 22.

(12) نهلة عبد القادر هاشم، وإيمان زغلول راغب، (2007) "الإدارة المفتوحة مدخل لتمكين المعلمين بالمدرسة الثانوية الفنية الصناعية في جمهورية مصر العربية"، مجلة التربية والتنمية، المكتب الاستشاري للخدمات التربوية، العدد 42، السنة ال 15، ص 69.

([13]) RamziKamelHannaallah, Michael Takla, (1998) Dictionary of the Terms of Education, Beiruit, Librairie du Liban Publishers, P.211.

([14]) Richard Kissel, (2013), Glossary of Key Information Security Terms, U.S.A, National Institute of Standards and Technology, P.94.

([15]) Information Systems Audit and Control Association, (2015) ISACA Glossary of Terms, U.S.A, Information Systems Audit and Control Association, P.49.

(16) Tom Carlson, Information Security Management, (2002), USA, International Network Services Inc, P.9.

(17) Prasanna Ramakrishnan, (2003) Information Security Management Systems, North America, Federal Energy Regulatory commission, P.1.

(18) Gary R. Lomprey,(2008) Critical Elements of an Information Security Management Strategy, Presented to the Interdisciplinary Studies Program: Applied Information Management and the Graduate School of the University of Oregon in Partial Fulfillment of the Requirement for the

Degree of Master of Science, Portland, University of Oregon, Applied Information Management Program, P.18.

(19) RadhaBalamuralikrishna, and JhonC.Dugger,(2003) SWOT Analysis: A Managing Tool for Imitating New Programs in Vocational Schools, London, Person Education Limited, P.P. 185-187.

(20) Board of Studies, Industrial Technology, (2003), New South Wales, Board of Studies, P.11.

(21) Jethro Perkins, (2014) Information Security Policy, London: London School of Economics & Political Science IT Services, P.2.

(22) Ibid, P.P.17-18

(23) Education Bureau, (2007) the Government of the HKSAR: Information Technology in Education Project, IT Security In Schools, (HK, Education Bureau P.P.23-26.

(24) Janet Reno and Others, (2008) The Appropriate and Effective Use of Security Technologies in U.S. Schools: A Guide for Schools and Law Enforcement Agencies, Washington, U.S. Department of Justice, P.26.

(25) John N. Stewart, (2013), School Information Security, New Jerrcy, Executive Thought Leadership Center, P.2.

(26) DanchoDanchev, (2003), Building and Implementing a Successful Information Security Policy, Windows Security Resource for IT Admins, London, Internet Software Marketing, P.P.12-15

(27) Jethro Perkins, (2013) Policy Electronic Messaging Policy, London, London School of Economics & Political Science IT Services, P.P.9-12.

(28) BundesamtfürSicherheit in der Information stechnik,(2008), Information Security Management System ,Version 1.5 Bonn, BundesamtfürSicherheit in der Informationstechnik, P.P.16-17.

(29) Ibid, P.P 18-19.

(30) Geoff Whitty, (2013), Information Security Management Policy, London, London Institute of Education, P.10.

(31) Moses Moyo, (2014), Information Security Risk Management in Small--Scale Organizations: A Case Study of Secondary Schools‟ Computerized Information System, submitted in Accordance with the Requirements for the Degree of MA, at University of South Africa, P.51.

(32) Malik Saleh, (2011), "The Three Dimensions of Security", In International Journal of Security, Volume 5, Issue 2, P.P.87-88.

(33) T Grobler, and Von Solms, (2005), Assessing the Policy Dimension, Johannesburg: Standard Bank Academy of Information Technology, P.6.

(34) Ibid, P.8.

(35) Ibid, P.6.

(36) Malik Saleh, Op.Cit, P.P.88, 90.

(37) At. Kearaney, (2015), Information Technology: It's all about Trust, Koera, At Kearaney Organization, P.P.5-6.

(38) Ali Maqousi and Others, (2013), An Effective Method for Information Security Awareness Raising Initiatives, International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 2, P.65.

(39) Hussain A.H. Awad and Fadi M. Battah,(2011), Enhancing Information Systems Security in EducationalHl Organizations in KSA throughproposing security model, International Journal of ComputerScience Issues, Vol. 8, Issue 5, No 3, P.356.

(40) Jason Taule and Others, (2014), Building an Information Security Organization, Dave Summit, Chief Information Security Officer, University of Alabama at Birmingham Health System, Building Security Program, P.6.

(41) Kenneth Høstland and Others, (2010) Information Security Policy: Best Practice Document, Norway, UNINETT led Working Group, P.P 24-25.

(42) Alex Fagerström, (2013), Creating, Maintaining and Managing an Information Security Culture, Degree Thesis, Information and Media Technology Department, Arcada, P.14.

(43) Information Systems Audit and Control Association,(2005), Critical Elements of Information Security Program Success, United States of America, Information Systems Audit and Control Association, P. 8.

(44) Ibid, P. 9.

(45) Information Security Policy Council, (2010), The First National Strategy on Information Security, Tokyo: Information Security Policy Council, P.P. 32-33.

(46) Information Security Board of Review Members,(2011), Information Security Plan, Michigan Technological University, Michigan, Michigan Technological University,P.P 23-25

(47) Virginia Department of Education, (2012), Model School Crisis Management Plan, Virginia: Division of Special Education and Student Services, P.71.

(48) Ibid, P. 74

(49) W. Timothy Coombs,(2007), Crisis Management and Communication, PhD Presented at Faculty of Education, Department of Education Foundation, Boston University, P.14.

(50) Massachusetts Department of Elementary and Secondary Education, Career/Vocational Technical Education,(2016), Massachusetts, Massachusetts Department of Elementary and Secondary Education, P.P 31-35

(51) AliMaqousi and Others, (2013), An Effective Method for Information Security Awareness Raising Initiative, International Journal of Computer Science & Information Technology (IJCSIT) Vol.,5, No 2, P.67.

(52) Information System Security Association (ISSA), Available:www.issa.org, (Accessed: 14-2-2016)

(53) The Information Systems Audit and Control Association (ISACA) Available: http://www.isaca.org (Accessed: 7-10-2016)

(54) The System Administration, Networking, and Security Institute (SANS), Available: http:// www.sans.org (Accessed: 7-10- 2016)

(55) Frost & Sullivan, (2011), The 2011 Global Information Security Workforce Study, Geneva: A Frost& Sullivan Market Survey, P.20.

(56) Security Awareness Program, (2014) Information Supplement: Best Practices for Implementing a Security Awareness Program, Special Interest Group PCI Security Standards Council, P.7.

(57) Joint Universities Computer Centre Limited ("JUCC"), (2009) Information Security-Perspective for Management Information Security Management Program –Concept and Implementation, Information Security Awareness Training-Session One, Hong Kong, P.8.

(58) Gary R. Lomprey,(2008), Critical Elements of an Information Security Management Strategy, Presented to the Interdisciplinary Studies Program: Applied Information Management and the Graduate School of the University of Oregon in partial fulfillment of the requirement for the degree of Master of Science, P.66.

(59) Benjamin Wright, (2009),” Employment, Trends, and Training in Information Security”, Occupational Outlook Quarterly, P.P. 37-38

(60) Eric Henault, (2016), Master Class Cycle on Information Security Management, EU: European Technical School Union, P.P.2-3.

(61) Kathryn Parsons and Others, (2013), Human Factors and Information Security: Individual, Culture and Security Environment, Australia, Defense Science Technology Organization, P.35.

(62) Alex Fagerström, Creating, Maintaining and Managing an Information Security Culture, Op.Cit, p.20

(63) Tom Carlson, (2001), Information Security Management: Understanding ISO 17799, London, International Network Services,P.P.8-10

(64) Tom Carlson, (2002) Information Security Management: Understanding ISO 17799, Washington: International Network Services, P.P.7-9

(65) Ohio Department of Education, (2013), Information Technology Career Field Technical Content Standard, Ohio, Department of Education, P.P. 20-25.

(66) وزارة التربية والتعليم، الرؤية المستقبلية لسياسة التعليم قبل الجامعي Available: http://knowledge.moe.gov.eg/arabic/ (Accessed: 13-8-2016)

(67) وزارة التربية والتعليم، قطاع التعليم الفني، الأهداف العامة للتعليم الفني، Available:

http://portal.moe.gov.eg/Aboutministery/Departments/technical/pages/aims.aspsx (Accessed: 13-8-2016)

(68) هناء شحتة السيد مندور، (2010) " تطوير النمط القيادي لمديري المدارس الثانوية الفنية بمصر في ضوء مبادئ الإدارة المفتوحة"، رسالة ماجستير غير منشورة، مقدمة إلى قسم التربية المقارنة والإدارة التعليمية، كلية التربية، جامعة عين شمس، ص 131.

(69) وزارة التربية والتعليم، الخطة الاستراتيجية للتعليم قبل الجامعي 2014-2030، (2014) جمهورية مصر العربية، وزارة التربية والتعليم، ص ص 77-78.

(70) البوابة المصرية للتعليم الفني، مشروع تطوير التعليم الفني باستخدام تكنولوجيا المعلومات والاتصالات :Available

http:fany.moe.gov.eg/forums Accessed (13-7-2016)

(71) وزارة التربية والتعليم، (2002)، قرار وزاري رقم 99 بتاريخ 6/8/ 2002، بشأن إنشاء وحدة الإحصاء والمعلومات بالمدارس، القاهرة، مكتب الوزير، مادة 1.

(72) المرجع السابق، مادة 2.

(73) المرجع السابق، مادة 3.

(74) وزارة التربية والتعليم، (2014)، قرار وزاري رقم 283 بتاريخ 6/26/ 2014، بشأن تحديد الوصف الوظيفي لمسئول معلومات سوق العمل بالمدرسة الثانوية الفنية، القاهرة، مكتب الوزير، مادة 1، 2

(75) وزارة التربية والتعليم، (2014)، قرار وزاري رقم 283 بتاريخ 6/26/ 2014، بشأن تحديد الوصف الوظيفي لمسئول التوظيف بالمدرسة الثانوية الفنية، القاهرة، مكتب الوزير، مادة 1.

(76) وزارة التربية والتعليم، (2014)، قرار وزاري رقم 283 بتاريخ 6/26/ 2014، بشأن تحديد الوصف الوظيفي لمسئول ريادة الأعمال بالمدرسة الثانوية الفنية، القاهرة، مكتب الوزير، مادة 1، 2.

(77) وزارة التربية والتعليم، (2014)، قرار وزاري رقم 283 بتاريخ 6/26/ 2014، بشأن تحديد الوصف الوظيفي لمسئول الإرشاد والتوجيه المهني بالمدرسة الثانوية الفنية، القاهرة، مكتب الوزير، مادة 1، 2.

(78) يسري طه دنيور، (2015)، آليات التوسع في التعليم الفني في ضوء احتياجات سوق العمل (تصور مقترح)، القاهرة، المركز القومي للبحوث التربوية والتنمية، ص 16.

(79) يسرى طه دنيور، (2014)، تقويم البرامج التدريبية لمعلمي التعليم الفني في مصر على ضوء الاتجاهات العالمية المعاصرة، القاهرة، المركز القومي للبحوث التربوية والتنمية: شعبة التعليم الفني، ص ص 40، 41.

(80) يسري طه دنيور، (2014)، مشكلات بعض المدارس الثانوية الفنية في مصر ومقترحات حلها، القاهرة، المركز القومي للبحوث التربوية والتنمية: شعبة التعليم الفني، ص25، 37، 38، 41.

(81) ناجي شنودة نخلة، (2013) تفعيل جهود الجهات الداعمة للتعليم الفني " دراسة ميدانية"، القاهرة، المركز القومي للبحوث التربوية والتنمية: شعبة التعليم الفني، ص ص 18–19.

(82) البوابة المصرية للتعليم الفني، تجارب ناجحة :Available http:fany.moe.gov.eg/sucessfulExperiments Accessed (13-7-2016)

(83) وزارة الاتصالات وتكنولوجيا المعلومات، مرجع سابق، ص 19.

(84) المرجع السابق، ص 19

(85) رئاسة مجلس الوزراء قانون جهاز أمن المعلومات ومكافحة جرائم الاتصالات، (2015)، جمهورية مصر العربية، وزارة الاتصالات، المادة السادسة.

(86) معهد اليونسكو للإحصاء، منظمة الأمم المتحدة للتربية والثقافة والعلوم، (2011)، دليل لقياس تكنولوجيا المعلومات والاتصالات في التعليم، مونتريال، معهد اليونسكو للإحصاء، ص ص 89 -92.

(87) وزارة التربية والتعليم، قطاع التعليم الفني، الأهداف العامة للتعليم الفني، Available:

http://portal.moe.gov.eg/Aboutministery/Departments/technical/pages/conferences.aspx (Accessed: 13-8-2016)

(88) وزارة التربية والتعليم، قطاع التعليم الفني، الأهداف العامة للتعليم الفني، Available: http://portal.moe.gov.eg/Aboutministery/Departments/technical/pages/techconf2.aspx (Accessed: 13-8-2016)

(89) اليونسكو، تقرير التعليم للجميع في مصر (2000-2015)، (2014)، القاهرة، مكتب اليونسكو بالقاهرة، ص 96.

(90) المرجع السابق، ص ص 106-107.

(91) يسري طه دنيور، مرجع سابق، ص 18.

(92) عبد الخالق يوسف سعد، (2009)، استخدام تكنولوجيا المعلومات والاتصالات في التنمية المهنية للمعلم، القاهرة، دار العين للنشر، ص 101.

(93) يسري طه دنيور، تقويم البرامج التدريبية لمعلمي التعليم الفني في مصر على ضوء الاتجاهات العالمية المعاصرة، مرجع سابق، ص 24.

(94) محمد جمال الدين درويش، مرجع سابق، ص 21.

(95) يسري طه دنيور، مرجع سابق، ص ص 16-17.

(96) السيد أحمد عبد الغفار، (2010)، دور التعليم الثانوي الفني في مواجهة تحديات بناء الاقتصاد المعرفي، القاهرة، المركز القومي للبحوث التربوية والتنمية: شعبة التعليم الفني، ص 28.

(100) محمود محمد الهادي (1995)، أساليب إعداد وتوثيق البحوث العلمية، القاهرة، المكتبة الأكاديمية، ص 185.

(101) Milorad M. Novicevic et al (2004): Dual Perspective SWOT: a Synthesis of Marketing Intelligence and Planning. Marketing Intelligence and Planning, Vol. 22, No. 1, p. 89.