دائـــــرة الـصـــحـــة
DEPARTMENT OF HEALTH

استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي

المحتويات

1 مقدمة

1.1 تمهيد

أصبح التطوّر التقني أحد أهم ممكّنات الأعمال والصناعات والحكومات بالنسبة للاقتصادات العالمية. ويلعب هذا التطور التقني دورًا أساسيًا في القطاع الصحي، حيث إنه يعزّز فاعلية رعاية المرضى وسلامتهم. كما أصبحت الاتجاهات الرقمية الجديدة شائعة بشكل متزايد، مثل الأجهزة القابلة للارتداء التي تُمكّن المرضى من تعزيز سجلاتهم الصحية بالإضافة إلى الأجهزة المتصلة بالشبكة التي تتيح المراقبة عن بُعد ورعاية المرضى.

هذه الموارد والنظم مُعرّضة لعدد من مسارات التهديد؛ كتهديدات هجمات الدول القومية أو سعي مجرمي الإنترنت إلى سرقة المعلومات الصحية المحمية القيّمة (PHI) بغرض استغلال البيانات المتعلقة بالصحة لتحقيق مصالح خاصة أو بغرض الربح منها. لذا يجب على القطاع الصحي إعطاء الأولوية لأمن المعلومات والأمن السيبراني ضمن أجندته الرامية إلى تقليل مخاطر فقدان البيانات وتضرّر السمعة والخسائر المالية المحتملة.

يلزم بذل جهود متضافرة واتباع أسلوب منهجي لإدارة وحماية الوضع الأمني السيبراني، وذلك ليس لضمان سلامة المريض فحسب، بل أيضًا للحفاظ على الثقة في الخدمات الصحية. كما يلزم اتباع أسلوب منهجي للأمن السيبراني لوضع مجموعة من الأهداف والأولويات استنادًا إلى استراتيجية أمن المعلومات والأمن السيبراني.

1.2 الغرض

يتمثّل الغرض من استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في وضع نهج شامل لتطبيق إطار متّسق للأمن السيبراني؛ حيث تدعم هذه الاستراتيجية تحقيق أهداف وأولويات القطاع الصحي في أبوظبي وحمايته من التهديدات السيبرانية.

ستُوفر استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي استجابة متماسكة واستباقية للتحديات الحالية والمستقبلية التي قد تواجه الأمن السيبراني للقطاع الصحي في إمارة أبوظبي. كما أن هذه الاستراتيجية تدعم أهداف التحوّل الرقمي من خلال تمكين تبنّي التقنية والابتكار والذكاء الاصطناعي في القطاع الصحي في الإمارة. وتعمل الاستراتيجية على مواءمة مبادرات الأمن السيبراني للقطاع الصحي مع مبادرات الأمن السيبراني الوطنية لدولة الإمارات العربية المتحدة.

1.3 النطاق

تؤكد الاستراتيجية على سلسلة من الإجراءات الموصى بها. ستضمن دائرة الصحة تنفيذ استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي بشكل مُوحّد على مستوى القطاع في الإمارة.

يغطي نطاق هذه الاستراتيجية ما يلي:

- جميع جوانب أمن المعلومات والأمن السيبراني للقطاع الصحي وخدماته داخل إمارة أبوظبي.
- أخصائيي الرعاية الصحية، والمنشآت الصحية، وشركات التأمين، ومزودي الخدمات، والبائعين، والجهات الخارجية الذين لديهم إمكانية الوصول والمعالجة/إدارة/تخزين معلومات المرضى و يعملون داخل إمارة أبوظبي.

تُعتبر كل منشأة من منشآت القطاع الصحي مسؤولة عن معلوماتها ووضعها الأمني السيبراني. وستعمل دائرة الصحة، بصفتها الجهة المسؤولة عن هذه الاستراتيجية، على مواءمة قطاع الصحة في أبوظبي مع المهمة الوطنية المتمثلة في تعزيز الوضع الأمني العام. ومن خلال رؤية السنوات الخمس المقبلة، ستقود دائرة الصحة التنفيذ الناجح لمختلف مبادرات القطاع الصحي في أبوظبي.

تُعدّ الرؤية عنصرًا مهمًا في الاستراتيجية وتهدف إلى تحديد الغرض، والاتجاه الذي يسير فيه القطاع، والقيم التي توجّه هذه الرحلة. تمت صياغة الرؤية والرسالة بما يتماشى مع الأولويات المحددة في بيانات الرؤية والرسالة الأعمّ، وخاصةً بما يراعي أولويات كل من (1) دائرة الصحة – أبوظبي، و(2) هيئة أبوظبي الرقمية، و(3) استراتيجية الأمن السيبراني على مستوى دولة الإمارات.

تتمثل رؤية أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي فيما يلي:

تمكين التحوّل الرقمي الآمن سيبرانيًا للخدمات الصحية وتوفير ضمان كافٍ بشأن أمن المعلومات، مع تحسين تجربة المتعاملين في الحصول على الرعاية الصحية في ذات الوقت.

من ناحية أخرى، تُقدم الرسالة بيانات عامة حول كيفية تحقيق القطاع للرؤية المحددة بعبارات عملية أكثر وتجمع بين التفكير المستقبلي والأهداف الحالية.

تتمثل رسالة أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي فيما يلي:

التمكين من تقديم خدمات صحية رقمية آمنة ومستدامة من خلال:

- وضع آلية إشراف قيادي على قطاع الصحة.
- تمكين بُنية تحتية قادرة على التكيّف من أجل الاستجابة والتعافي السريعيْن.
- تطوير وتمكين قوى عاملة ذات كفاءة في مجال الأمن السيبراني.
- وضع منهجية لإدارة المخاطر على مستوى القطاع.
- تحسين سياسات ومعايير القطاع الصحي.
- تهيئة بيئة تعمل على تعزيز الشراكة والابتكار في مجال الأمن السيبراني.

فيما يتعلق بالخطوات التالية، فإن النهج الشامل الموضّح في الرؤية والرسالة يتيح تحديد الحالة المستهدفة المناسبة ومتابعة أهداف وأولويات القطاع التي ينبغي تحقيقها ضمن إطار زمني محدد.

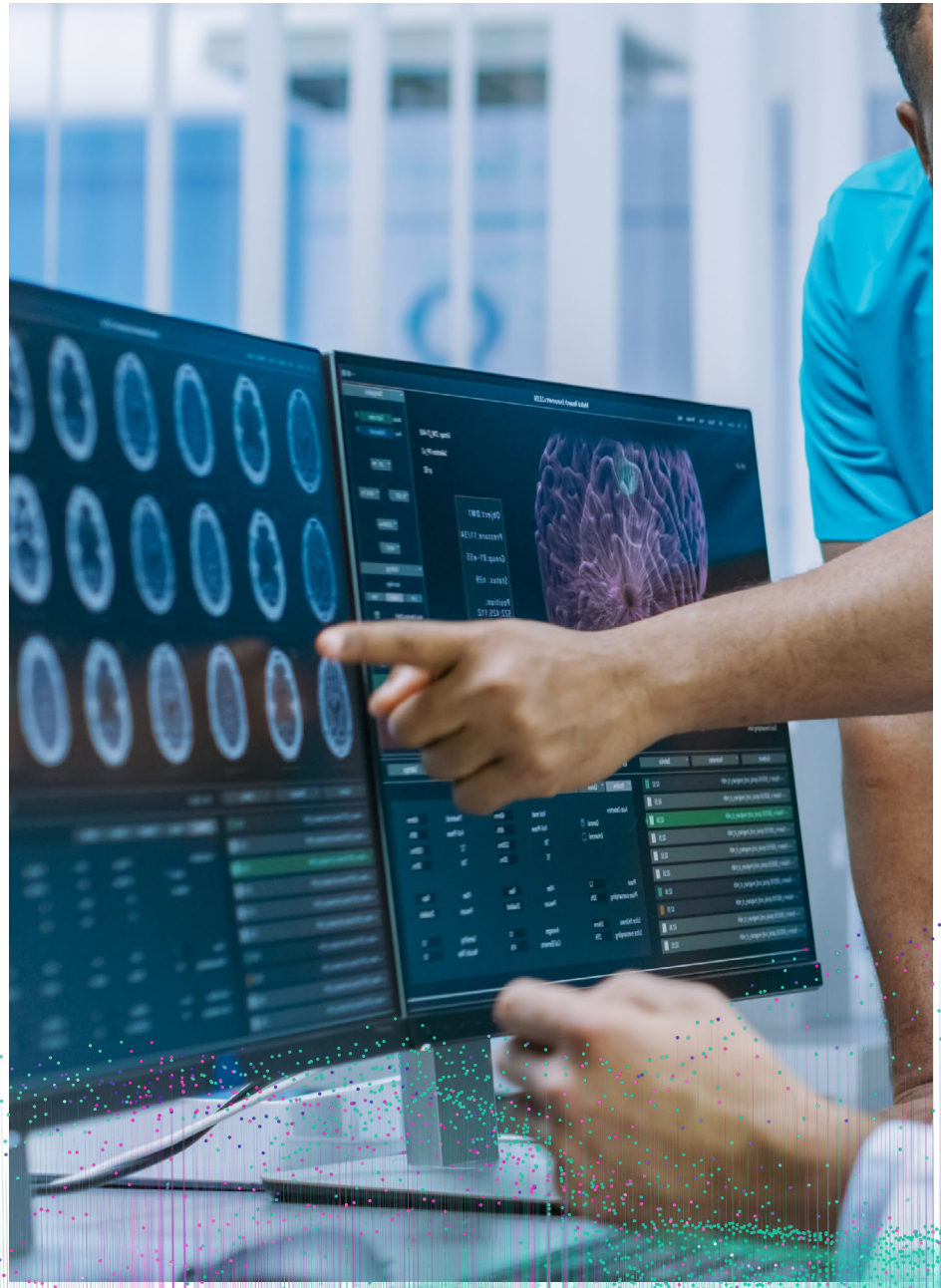
3 الحالة المستهدفة للقطاع الصحي في أبوظبي

يتمثّل الهدف من استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي في توفير استجابة قوية ومتماسكة واستباقية للتحديات الحالية والمستقبلية التي قد تواجه الأمن السيبراني للقطاع في الإمارة.

استنادًا إلى التحليل والمقارنة مع نماذج نضج الأمن السيبراني العالمية، يمكن تحديد الحالة المستهدفة لنضج الأمن السيبراني للقطاع الصحي على النحو التالي:

- حوكمة الأمن السيبراني المستدامة، وترسيخ الاستراتيجية والإجراءات المرتبطة بها مع الإشراف المناسب عليها.
- الوعي المستدام لجميع الأطراف المعنية بالأمن السيبراني، كلٌّ حسب دوره، مما يؤدي إلى زيادة التركيز على المبادرات الأمنية.
- الجاهزية للتعامل مع الحوادث المتعلقة بالأمن السيبراني بتوفير قدرات الاستجابة والتعافي السريعيْن.
- توفُّر الموارد البشرية الماهرة والإجراءات المتعلقة بالأمن السيبراني لضمان نجاح المبادرات الأمنية.
- ممارسات مترابطة بين المورّدين والشركاء في القطاع الصحي من أجل التعاون على التخفيف من التهديدات وتقليل نقاط الضعف الأمنية السيبرانية.
- تبنّي التوجّهات التقنية العالمية في القطاع الصحي في أبوظبي ضمن حدود المخاطر المقبولة.

ينبغي أن تتمثّل الاعتبارات الرئيسية لتحقيق الحالة المستهدفة في التقليل من التحديات الحالية التي تواجه القطاع الصحي ومجالات المخاطر المحتملة في المستقبل.



4

لتمكين تحقيق الرؤية المتعلقة بأمن المعلومات والأمن السيبراني للقطاع الصحي، أخذت دائرة الصحة زمام المبادرة في وضع استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في إمارة أبوظبي.

يتطلب وضع الاستراتيجية فهمًا واضحًا لما حقّقه الرائدون عالميًا في مجال الأمن السيبراني للقطاع الصحي. لذا عملت دائرة الصحة وفق نهج تعاوني مع مختلف الجهات المعنية لتحديد ووضع هذه الاستراتيجية.

بدأت عملية المقارنة المعيارية بتحديد الدول التي تُظهر حاليًا قدرًا عاليًا من النضج الأمني السيبراني في القطاع الصحي والمصنفة بأعلى المراتب في هذا المجال. كما تم جمع المدخلات من مصادر مختلفة، بما فيها مؤشر الأمن السيبراني العالمي (GCI)، والدول النظيرة جغرافيًا، ومتصدّري العناوين والرُوّاد في هذا المجال.

تم إجراء تقييم نضج شامل للقطاع الصحي في أبوظبي وفقًا للممارسات الرائدة ولوائح الامتثال لمعايير أمن المعلومات والخصوصية، وتم تحديد المجالات التي يجب التركيز عليها والأهداف الرئيسية للجهات المعنية الداخلية والخارجية.

كما تمت المواءمة مع الاستراتيجية الشاملة لدائرة الصحة ومبادرات التحوّل الرقمي الأخرى لتحديد رؤية ورسالة وتوجيهات الأمن السيبراني للقطاع الصحي.

لتحقيق الحالة المستهدفة للقطاع الصحي في أبوظبي، وضعت دائرة الصحة استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي استنادًا إلى ستّة ركائز.

حوكمة الأمن السيبراني

تعزيز الرقابة القيادية عن طريق وضع إطار عمل مخصص لحوكمة الأمن السيبراني.

مرونة الأمن السيبراني

التأكد من القدرة على الاستجابة للتهديدات السيبرانية والتعافي منها.

قدرات الأمن السيبراني

تطوير المعارف والمهارات والقدرات ذات الصلة لتأمين البيئة السيرانية.

شراكات الأمن السيبراني

ضمان التعاون من خلال شراكات متعددة الأطراف لتحسين الفضاء السيبراني.

نضج الأمن السيبراني

تعزيز الوعي بالأمن السيبراني وأطر الإدارة الملائمة للتهديدات السيبرانية.

الابتكار في الأمن السيبراني

ترسيخ الابتكار المستدام باعتباره أحد ممكنات الأمن السيبراني.

الأهداف

المبادرات

النتائج

تم تحديد الأهداف والمبادرات الرئيسية والنتائج لكل ركيزة من الركائز استنادًا إلى المدخلات المقدمة من الجهات المعنية بالرعاية الصحية.

5

استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي في أبوظبي

5.1 الركيزة الأولى: حوكمة الأمن السيبراني

تُعنى هذه الركيزة بوضع إطار حوكمة لأمن المعلومات والأمن السيبراني للقطاع الصحي؛ حيث لن يعمل هذا الإطار على ترسيخ قيادة مُخصّصة وهيكل تنظيمي مناسب فحسب، بل أيضًا على ترسيخ إجراءات شاملة لتحقيق الأهداف الاستراتيجية واستدامتها.

5.1.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

إنشاء إطار قوي لحوكمة أمن المعلومات والأمن السيبراني يضمّ مجموعة واضحة من أوجه المساءلة والمسؤوليات.

المبادرات

- إنشاء هياكل داخلية مناسبة لضمان كفاءة العمليات وتنفيذ المسؤوليات الموكلة.
- تشكيل اللجان والمنتديات اللازمة لإدارة الاتصالات الداخلية والخارجية والعمليات والامتثال، ولمناقشة القضايا والتحسينات.
- إعداد أدوات وتقنيات مناسبة للتنفيذ الفعّال لإطار حوكمة أمن المعلومات والأمن السيبراني.
- وضع إجراءات رصد وإبلاغ تتسم بالكفاءة والفاعلية، بالإضافة إلى مؤشرات أداء رئيسية للمتطلبات الحالية والمستقبلية.

5.1.2 النتائج المرجوّة

- المشاركة على مستوى القطاع في اجتماعات الحوكمة، في مواعيد محددة، لمراجعة أداء الأمن السيبراني.
- تحديد ووضع الشروط المرجعية إلى جانب أوجه المساءلة والمسؤوليات لتنفيذ حوكمة القطاع والحوكمة الداخلية على النحو الملائم.
- تطبيق وتشغيل أدوات وتقنيات الرصد على مستوى القطاع لدعم إطار حوكمة الأمن السيبراني.
- تحديد ووضع معايير الرصد والإبلاغ عن أمن المعلومات والأمن السيبراني على مستوى القطاع من أجل تنفيذ آلية الإشراف القيادي والتحسينات.

5.2 الركيزة الثانية: مرونة الأمن السيبراني

تُعنى هذه الركيزة بضمان تهيئة بيئة قوية للقطاع الصحي في أبوظبي قادرة على مواجهة التهديدات السيبرانية والتكيّف مع الظروف المتغيرة، بما يشمل القدرة على تحمل جميع أنواع الهجمات، والتعافي السريع من الآثار السلبية، والحدّ من أضرار الهجمات على المنشآت الصحية والأفراد والمجتمع.

5.2.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

إنشاء إطار استجابة سيبرانية للقطاع الصحي مع إدارة تهديدات ومخاطر حوادث الأمن السيبراني.

المبادرات

- إعداد الممارسات الرائدة والمبادئ التوجيهية وخطط العمل بحيث تشمل الجانب المتعلق بإدارة حوادث الأمن السيبراني ونقاط الضعف في القطاع الصحي.
- تشكيل فريق متقدم لإدارة الحوادث يتمتع بمجموعة المهارات المناسبة للتعامل مع حوادث الأمن السيبراني.
- تعزيز الوعي الظرفي لاكتشاف الحوادث والاستجابة المناسبة لها من خلال تمكين تبادل معلومات التهديدات آنيًا بين منشآت القطاع الصحي.
- تعزيز تبادل المعلومات بين مركز استخبارات التهديد السيبراني في أبوظبي (CTIC) وفريق الاستجابة لطوارئ الحاسب الآلي (CERT) للقطاع الصحي في أبوظبي بشأن معلومات التهديدات السيبرانية الخاصة بالقطاع.

الهدف الثاني

تقليل المشاكل ونقاط الضعف المحددة في النظم والتطبيقات والبنية التحتية وذلك باتباع نهج قائم على إدارة المخاطر.

المبادرات

- تحسين المعايير والممارسات الرائدة لإدارة المخاطر المتعلقة بالأجهزة الطبية والخدمات الصحية.
- التعاون مع الهيئات والجهات المعنية لإعداد لوائح وإجراءات تعزيز الأمن السيبراني الملائمة لضمان أمن بيئة القطاع الصحي من ناحية البنية التحتية لتقنية المعلومات وشبكة تقنية المعلومات والأجهزة الطبية.
- وضع أسلوب منهجي للنظم والتطبيقات والبنية التحتية القديمة والجديدة فيما يتعلق بدورة حياة الأمن السيبراني الخاصة بها (مثل التصحيح، وتطبيق ضوابط رقابية بديلة، والتجزئة، والاستبدال).

الهدف الثالث

وضع خطة استمرارية للأمن السيبراني على مستوى القطاع.

المبادرات

- وضع سياسات الاستمرارية للقطاع الصحي وفقًا للمبادئ التوجيهية لمعيار إدارة استمرارية الأعمال (معيار "NCEMA 7000" للهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث).
- التحقق من خطط الاستمرارية من خلال اختبار التشغيل التلقائي للتجهيزات الاحتياطية والتدرب على تلك الخطط بشكل متكرر.

5.2.2 النتائج المرجوّة

- الالتزام على مستوى القطاع بإطار الاستجابة السيبرانية لإدارة حوادث الأمن السيبراني.
- تشكيل فريق لإدارة الحوادث يتمتع بالمهارات الملائمة وتحديد الممارسات الرائدة والمقاييس والمبادئ التوجيهية للتعامل مع حوادث الأمن السيبراني.
- نشر معلومات التهديدات الآنية والظرفية فيما بين منشآت القطاع الصحي.
- ترسيخ الاتصال والتعاون مع الجهات الاتحادية الأخرى لمشاركة معلومات التهديدات السيبرانية.
- تعزيز المعايير والأطر المُطبقة على القطاع الصحي.
- تطوير لوائح تعزيز الأمن السيبراني.
- وضع وترسيخ أسلوب منهجي للنظم والتطبيقات والبنية التحتية القديمة والجديدة فيما يتعلق بدورة حياة الأمن السيبراني الخاصة بها.
- وضع سياسات وخطط الاستمرارية المحددة للأمن السيبراني مع تعيين الأدوار والمسؤوليات.
- وضع خطة دورية للأمن السيبراني فيما يتعلق باختبار خطط استمرارية الأعمال والتعافي من الكوارث.

5.3 الركيزة الثالثة: قدرات الأمن السيبراني

تُعنى هذه الركيزة بتطوير المعارف والمهارات والقدرات ذات الصلة بتعزيز القدرة على مواجهة مخاطر وتهديدات الأمن السيبراني، بما يشمل تطوير الوظائف والقدرات لتيسير الابتكار التقني في تقديم الرعاية وصحة المرضى.

5.3.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

تهيئة بيئة تقنية تدعم المنصات التقنية الآمنة والتحوّل الرقمي الآمن للمنشآت الصحية.

المبادرات

- تعزيز الأمن السيبراني باعتباره خاصية أساسية لتصميم الخدمات واستخدام التفكير التصميمي لبناء تجارب آمنة ومريحة للمتعاملين.
- تعزيز تقنية الأتمتة والتنسيق لتقليل إهدار الوقت والتأخير في الإجراءات والتفاعلات الأمنية بهدف تحسين التعرّف على التهديدات السيبرانية والاستجابة لها.
- تمكين تبادل المعلومات الصحية الخاصة بالمرضى بين منشآت القطاع الصحي وشركات التأمين والمرضى بصورة آمنة وملائمة.

الهدف الثاني

رفع الوعي بأمن المعلومات والأمن السيبراني ضمن القطاع الصحي من خلال إرساء فهم الآثار المترتبة على الأفراد والإجراءات والتقنيات.

المبادرات

- إعداد برامج تثقيفية وتوعوية بالأمن السيبراني تستهدف جميع قادة وموظفي القطاع الصحي لضمان الوعي الكافي وزيادة التركيز على المبادرات الأمنية.
- تنظيم وإجراء ورش عمل وحملات للتوعية بالأمن السيبراني لجميع الأطراف المعنية بمن فيهم المرضى والموظفين كلٌّ حسب دوره.
- تعزيز مهارات موظفي القطاع الصحي بمختلف الطرق وذلك من خلال التعاون بين القطاع والمعاهد الأكاديمية.

5.3.2 النتائج المرجوّة

- توحيد الممارسات والمبادئ التوجيهية الأمنية خلال عملية دورة حياة تطوير البرامج/ التطبيقات/ النظم واستخدامها.
- تعزيز قدرات التعرّف على التهديدات السيبرانية والتعافي منها نتيجة استخدام تقنيات الأتمتة والتنسيق.
- وضع مبادئ توجيهية وإنشاء منصة متطورة لتبادل المعلومات الصحية بين منشآت القطاع الصحي وشركات التأمين والمرضى بصورة آمنة وملائمة.
- تعزيز وعي قيادات القطاع الصحي بالأمن السيبراني وتركيزهم عليه، مما يؤدي بدوره إلى تحسين دعم الإدارة لمبادرات الأمن السيبراني الهامة.
- تعزيز وعي جميع الأطراف المعنية، كلٌّ حسب دوره، بشأن التهديدات السيبرانية والممارسات السيبرانية الجيدة، وتحسين القدرة على التعرّف على حوادث الأمن السيبراني والاستجابة لها وتقليل زمن التعافي منها.
- تنظيم ندوات وجلسات تدريبية لموظفي القطاع الصحي لتعزيز مهاراتهم في الأمن السيبراني.

5.4 الركيزة الرابعة: شراكات الأمن السيبراني

تُعنى هذه الركيزة بضمان التعاون من خلال شراكات متعددة الأطراف لتعزيز الأمن السيبراني للقطاع الصحي؛ وذلك بهدف الحماية من التهديدات السيبرانية، وزيادة تبادل المعلومات المتعلقة بمسارات التهديد، واتخاذ إجراءات ضد أطراف التهديد السيبراني المختلفة.

5.4.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

إقامة اتحادات محلية ودولية لتحسين التعاون بين مجتمع الأمن السيبراني.

المبادرات

- إقامة اتحادات إقليمية ودولية لمشاركة ومناقشة وإدارة قضايا ومخاطر الأمن السيبراني في القطاع الصحي مع القطاعات الأخرى.
- التعاون مع فِرق الطب الحيوي لترسيخ الممارسات السيبرانية الجيدة ووضع قوائم التحقق من جودة الأجهزة الطبية الحيوية.
- التعاون مع المورّدين والشركاء والجهات المعنية لتعزيز مبادئ التصميم الآمن في تطوير المنتجات.

الهدف الثاني

تعزيز منصات ومنتديات استخبارات التهديد السيبراني لمشاركة معلومات التهديدات السيبرانية الخاصة بالقطاع الصحي.

المبادرات

- زيادة التوعية والمشاركة في الأمن السيبراني على مستوى القطاع الصحي والقطاعات الأخرى لتبادل المعرفة والمعلومات.
- إعداد وترويج دليل معرفي أساسي لتقنية المعلومات الطبية/الأجهزة الطبية، بهدف تجميع نقاط الضعف المحددة والتصحيحات والمشاكل الشائعة وكيفية حلّها.

5.4.2 النتائج المرجوّة

- الترويج لإمارة أبوظبي بوصفها رائدة عالميًا في القطاع الصحي الآمن سيبرانيًا من خلال إقامة اتحادات وشراكات وثيقة والتعاون في التخفيف من تهديدات ومخاطر الأمن السيبراني على القطاع الصحي.
- إعداد قائمة مرجعية ومبادئ توجيهية لفرق الطب الحيوي للتحقق من جودة الأجهزة الطبية وتقييم أمنها السيبراني.
- إقامة شراكة وثيقة مع المورّدين والشركاء لترسيخ الأمن السيبراني باعتباره مسؤولية مشتركة.
- إنشاء منصات تبادل المعلومات والمعارف الاستخباراتية حول التهديدات السيبرانية لمختلف الجهات المعنية والقطاعات.
- نشر دليل معرفي حول نقاط الضعف المحددة والتصحيحات للأجهزة والمشاكل الشائعة.

5.5 الركيزة الخامسة: نضج الأمن السيبراني

تُعنى هذه الركيزة بتحسين نضج الممارسات والإجراءات المتعلقة بالأمن السيبراني؛ حيث إنه من الضروري وضع إجراءات لتقييم فاعلية الضوابط والأطر الأمنية بشكل مستمر. ومع تطور مشهد التهديدات السيبرانية، ينبغي التكليف بوضع إطار أمني سيبراني ناضج ومتطوّر لتعزيز القدرات.

5.5.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

تعزيز إطار أمن المعلومات والأمن السيبراني للقطاع الصحي بوضع التشريعات اللازمة واستحداث مقاييس الالتزام بها، وتحديد متطلبات هذا المجال من ناحية الأفراد والإجراءات والتقنيات.

المبادرات

- تطوير برنامج تدقيق ومراقبة للقطاع الصحي بهدف تقييم حالة تطبيق معايير وسياسات القطاع الصحي ومدى الالتزام بها.
- إجراء تقييمات سنوية لمعايير أمن المعلومات والأمن السيبراني الحالية بالمقارنة مع الممارسات الرائدة عالميًا واتجاهات التقنية المستجدة.
- استكمال إطار أمن المعلومات والأمن السيبراني للقطاع الصحي بالسياسات والمعايير والمبادئ التوجيهية المطلوبة بالإضافة إلى قوائم التحقق لتغطية كافة أوجه الأمن المعلوماتي والسيبراني من أفراد وإجراءات وتقنيات.

الهدف الثاني

تعزيز حماية المعلومات الصحية من الوصول غير المصرح به من خلال استحداث آلية الأمن اللازمة للبنية التحتية الرقمية.

المبادرات

- إعداد الهياكل والضوابط الرقابية الداخلية لإدارة خصوصية البيانات بما يتماشى مع التشريعات واللوائح المعمول بها.
- العمل مع المنشآت الصحية لإنشاء عملية توثيق/اعتماد للنظم التي تعالج البيانات الصحية وتتعامل مع الأجهزة الطبية المتصلة بالشبكة.
- وضع وترسيخ ممارسات وبروتوكولات محددة بالإضافة إلى المواصفات الفنية للتبادل الآمن لسجلات المرضى وإدارتها.

5.5.2 النتائج المرجوّة

- الامتثال على مستوى القطاع لتشريعات، ومعايير، وإطار إدارة مخاطر الأمن السيبراني.
- تحديث معايير أمن المعلومات والأمن السيبراني استنادًا إلى نتائج المراجعة، ومعالجة متطلبات القطاع والمتطلبات التشريعية سنويًا.
- وضع السياسات والمعايير والمبادئ التوجيهية الداعمة والحفاظ عليها.
- تحديد الأدوار والمسؤوليات في القطاع الصحي لإدارة ومعالجة متطلبات تشريعات ومعايير خصوصية البيانات.
- الامتثال على نطاق واسع للأنظمة الصحية والأجهزة الطبية المتصلة بالأمن الإلكتروني في أبو ظبي وخصوصية البيانات وغيرها من المتطلبات القانونية والتنظيمية.
- وضع آلية للتبادل الآمن للمعلومات الصحية تحقيقًا لرؤية دائرة الصحة المتمثلة في "أبوظبي مجتمع معافى يتمتع بحياة صحية وسليمة."

5.6 الركيزة السادسة: الابتكار في الأمن السيبراني

تُعنى هذه الركيزة بتقديم الابتكار المستدام باعتباره أحد ممكّنات الأمن السيبراني، من خلال تبنّي الاتجاهات السائدة للتقنيات المستخدمة في القطاع الصحي على أمل تقديم رعاية صحية أفضل في المستقبل ضمن بيئة تشهد أقل قدر ممكن من التهديدات السيبرانية. ولا يشمل ذلك مجال التقنية فحسب، بل يشمل أيضًا جانبَي الأفراد والإجراءات.

5.6.1 الأهداف والمبادرات الاستراتيجية

الهدف الأول

تنظيم وتمكين منظومة الابتكار في القطاع الصحي من أجل تحقيق التحوّل الآمن سيبرانيًا.

المبادرات

- وضع اللوائح والمعايير والسياسات لدعم تبنّي الابتكار الآمن.
- تحسين عملية إدارة التغيير من خلال تبنّي الابتكار الآمن أثناء إجراء التغييرات.

الهدف الثاني

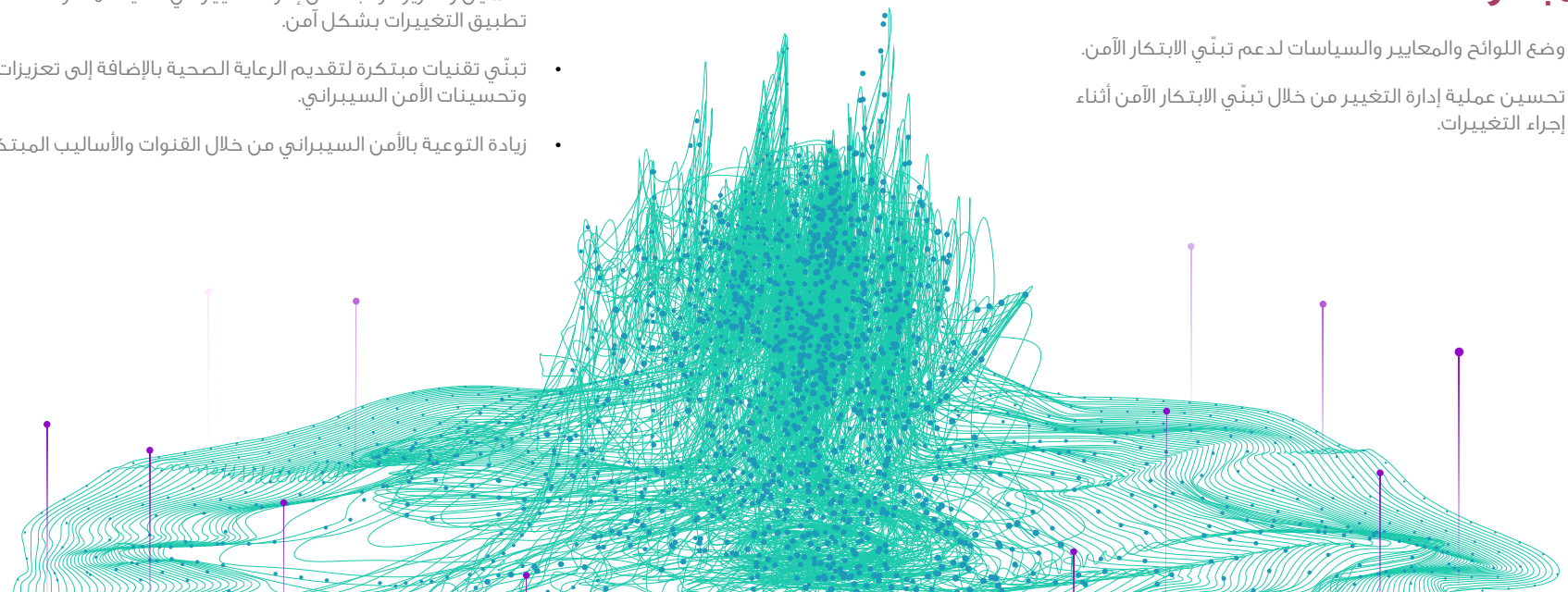
تشجيع الابتكار الآمن مع تحسين الرعاية الصحية المقدمة، وتعزيز نضج الأمن السيبراني للقطاع الصحي في ذات الوقت.

المبادرات

- تحديد وتبنّي التقنيات المستجدة في مختلف القطاعات والدول النظيرة عالميًا لتحسين الوضع الأمني للقطاع الصحي.
- تعزيز وتشجيع الابتكار في رفع الوعي حول تهديدات ومخاطر الأمن السيبراني للقطاع الصحي والاحتياطات الواجب اتخاذها.

5.6.2 النتائج المرجوّة

- ترسيخ ممارسات آمنة لتبنّي الابتكار من خلال اللوائح والمعاييروالسياسات والمبادئ التوجيهية اللازمة.
- تحسين وتعزيز الرقابة على إدارة التغيير في تقنية المعلومات لضمان تطبيق التغييرات بشكل آمن.
- تبنّي تقنيات مبتكرة لتقديم الرعاية الصحية بالإضافة إلى تعزيزات وتحسينات الأمن السيبراني.
- زيادة التوعية بالأمن السيبراني من خلال القنوات والأساليب المبتكرة.



6 سُبل المضي قدمًا

تتمثل رؤية القيادة الوطنية في ضمان تنفيذ مبادرات الأمن السيبراني بصفتها من ممكّنات النمو بالإضافة إلى دورها في توفير الأمن العام واكتساب ثقة واطمئنان الجمهور. وعلى صعيد القطاع الصحي، فإن ثقة المريض بمُقدّم الرعاية الصحية وخدماته تُعدّ من أهم المبادئ التي يجب الحفاظ عليها. وفي هذا الصدد، تُركّز استراتيجية أمن المعلومات والأمن السيبراني على بناء الثقة في الخدمات الرقمية المقدمة.

ثمّة فرص كبيرة لتعزيز قدرات القطاع الصحي من خلال التحوّل الرقمي ولكنّ ذلك يتطلب التصدّي لبعض التحديات الفريدة. وعلى الصعيد العالمي، يُعد القطاع الصحي أحد أكثر القطاعات استهدافًا من حيث الجرائم والهجمات السيبرانية. وتتعرض إمارة أبوظبي، بسبب وضعها الجيوسياسي واقتصادها المزدهر، لتهديدات سيبرانية مستمرة تستهدف البنية التحتية والخدمات الحيوية لديها. لذا ينبغي تحديد جميع نقاط الضعف وتقليلها؛ وإلّا ستتمكن أطراف التهديد من استغلالها والتأثير على سلامة المرضى.

يُمثل إصدار استراتيجية أمن المعلومات والأمن السيبراني للقطاع الصحي مُنجزًا أوليًا أساسيًا ونقطة تحوّل مهمة في رحلة الأمن السيبراني المستمرة لإمارة أبوظبي. ويُعدّ تفعيل الخطة وتنفيذ المبادرات المختلفة بمثابة خطوة مقبلة مهمة لتحقيق النجاح في الاستراتيجية الشاملة والمبادرات الوطنية للأمن السيبراني.

يُعدّ الأمن السيبراني مجالًا ديناميكيًا ودائم التغيّر، لذا فإننا من خلال تبنّي المبادئ المُوضّحة في هذه الوثيقة، سننشئ قطاعًا صحيًا آمنًا بما يتماشى مع رؤية قيادة الإمارات المتمثلة في أن تكون أبوظبي آمنة سيبرانيًا.

https://doh.gov.ae/