الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الإطار الوطني لإدارة الحوادث السيبرانية

الإصدار العام

الإصدار 1.0

إخلاء مسؤولية

تم تطوير الإطار الوطني لإدارة الحوادث السيبرانية في دولة قطر من قبل الوكالة الوطنية للأمن السيبراني، وهي الجهة الوحيدة المسؤولة عن الإشراف على تطوير الإطار الوطني لإدارة الحوادث، وتحديثه، ونشره. وتحتفظ الوكالة الوطنية للأمن السيبراني بالحقّ في إجراء أي تغييرات أو تعديلات على الإطار الوطني وفق ما تقرره الوكالة الوطنية للأمن السيبراني.

لا يجوز نسخ هذه الوثيقة لأي غرض تجاري إلّا بتفويض كتابي من الوكالة الوطنية للأمن السيبراني. وتحتفظ الوكالة الوطنية للأمن السيبراني بالحقّ في تقييم مدى فعّالية وملاءمة كافة النسخ التي يتم إنشاؤها.

تلتزم الوكالة الوطنية للأمن السيبراني بتحسين الإطار الوطني وتعديله بشكل مستمر بما يتناسب مع الطبيعة المتغيّرة لتهديدات الأمن السيبراني. وتكون قرارات الوكالة الوطنية للأمن السيبراني الصادرة فيما يتعلّق بالإطار الوطني نهائية وملزمة. لمزيد من المعلومات والاستفسارات، يرجى التواصل مع الوكالة الوطنية للأمن السيبراني.

كلمة رئيس الوكالة الوطنية للأمن السيبراني

إن إصدار الإطار الوطني لإدارة الحوادث السيبرانية يعد خطوة هامة ورائدة في تنفيذ الاستراتيجية الوطنية للأمن السيبراني الثانية والمنبثقة من استراتيجية قطر الوطنية 2030، وقد تم تصميم الإطار الوطني لإدارة الحوادث السيبرانية لتلبية الاحتياجات والتحدّيات المُستجدة للدولة، من خلال تقديم نهج شامل ومُنسق لإدارة الحوادث السيبرانية ذات التأثير الوطني.

ويأتي هذا الإطار مُتماشياً مع أفضل الممارسات العالمية والدروس المستفادة، لضمان الجاهزية التامة للدولة لمواجهة أية تحديات في مجال الأمن السيبراني، كما يعمل الإطار على تزويد دولة قطر باستراتيجية صلبة لإدارة الحوادث المتعلقة بتكنولوجيا المعلومات والتكنولوجيا التشغيلية والتي قد تُهدد الأمن الوطني، كما يضمن استعادة التشغيل الموثوق للخدمات الحيوية خلال إدارة الحادثة السيبرانية، والاستجابة لها، والتعافي منها بكفاءة عالية.

ويعد الإطار الوطني لإدارة الحوادث السيبرانية بمثابة خطوة نوعية نحو حماية الفضاء السيبراني لدولة قطر مما يُعزز ثقة الجمهور في القدرات الوطنية في مجال الأمن السيبراني عبر الجهود المتظافرة لكافة الجهات المعنية، والتي يتعين عليها تطبيق مبادئ هذا الإطار الوطني لكونها مسؤولية مشتركة يتقاسمها الجميع.

وإننا على ثقة بأن التعاون المُشترك بين الجهات في دولة قطر له دور كبير في بناء وتعزيز منظومة الأمن السيبراني، مما سيُمكّن الدولة من الاستجابة الفعالة والتعافي من الحوادث السيبرانية.

سعادة المهندس/ عبدالرحمن بن علي الفراهيد المالكي

رئيس الوكالة الوطنية للأمن السيبراني

جدول المحتويات

قائمة الأشكال

01

المقدّمة

1. المقدّمة

1.1 نظرة عامة

يعمل الإطار الوطني لإدارة الحوادث السيبرانية على تعزيز أمن الفضاء السيبراني لدولة قطر عبر منهجية متكاملة لإدارة الحوادث السيبرانية ذات التأثير الوطني، وذلك من خلال تنسيق الجهود بين كافة الجهات المعنية. ويهدفُ الإطار الوطني لإدارة الحوادث السيبرانية إلى:

- إنشاء إطار شامل لإدارة الحوادث السيبرانية ذات التأثير الوطني، بما يضمن الاكتشاف السريع والاستجابة المنسّقة والاستعادة الفورية للخدمات الوطنية.
- صياغة استراتيجية شاملة ومتكاملة تحدّد أدوار ومسؤوليات كافة الجهات المعنية المُشاركة.
- تعزيز مفهوم العمليات والإجراءات التي تتبعها الوكالة الوطنية للأمن السيبراني لكافة الجهات المُشاركة وذلك للحدّ من آثار الحوادث السيبرانية.
- دمج التحسينات المستمدة من الدروس المستفادة لتعزيز قدرات الاستجابة في المستقبل.
- تعزيز أمن الفضاء السيبراني لدولة قطر عبر اتخاذ تدابير استباقية تضمن الاستجابة السريعة.

2.1 النطاق والجمهور المستهدف

يتناول الإطار إدارة الحوادث السيبرانية ذات التأثير الوطني ضمن الفضاء السيبراني لدولة قطر، ويسري على كافة الجهات داخل الدولة. ومن الجدير بالذكر أنّ هذا الإطار الوطني يركّز فقط على إدارة الحوادث السيبرانية، في حين تتم تغطية إدارة الأزمات السيبرانية في الإطار الوطني لإدارة الأزمات السيبرانية. وتتوقّف مشاركة الجهات المعنية وتحدد مسؤولياتها بناءً على طبيعة الحادثة التي يجري التعامل معها.

تم إصدار هذه النسخة من الإطار الوطني لإدارة الحوادث السيبرانية بغرض توزيعها على الجهات في كافة القطاعات في الدولة، وهي تستعرض ملخصًا للمفاهيم الأساسية المحدّدة في الإطار الوطني وتلقي نظرة عامة على سير العمل المبسّط لإدارة الحوادث. وتُعد الإصدارات التفصيلية مصمّمة خصيصًا لتلبية احتياجات محدّدة متاحة عند الطلب، على أن تخضع هذه الطلبات للتقييم لضمان توافقها مع الأهداف الشاملة للإطار الوطني.

3.1 الغرض من هذه الوثيقة

يوضح هذا الإصدار من الإطار الوطني لإدارة الحوادث السيبرانية النهج المتّبع للاستجابة ولإدارة الحوادث ذات التأثير الوطني في دولة قطر، ويهدف إلى إعلام الجمهور العام وتوعيته حول الخطة الوطنية للتعامل مع الحوادث السيبرانية.

4.1 المبادئ والافتراضات

يعتمد التنفيذ والتطبيق الفعّال للإطار الوطني لإدارة الحوادث السيبرانية على الافتراضات والمبادئ الرئيسية التالية:

- **الامتثال والالتزام:** يتعين على كافة الجهات المشاركة الامتثال لإرشادات الإطار الوطني وتأدية الأنشطة الموكلة إليها ضمن الأُطر الزمنية المطلوبة.
- **الإبلاغ والاستجابة في الوقت المناسب:** يجب على كافة الجهات إبلاغ الوكالة الوطنية للأمن السيبراني على الفور بالحوادث السيبرانية ذات الصلة لتمكينها من اتخاذ إجراءات فعّالة للاستجابة في الوقت المناسب.
- **الموارد الكافية:** يعتمد نجاح الإطار الوطني على تخصيص الموارد الكافية، بما فيها الموارد البشرية، والتكنولوجيا، والتمويل، لدعم عملياته.
- **التواصل والتنسيق:** يتطلب تطبيق هذا الإطار وجود تواصل وتنسيق مستمر بين كافة الجهات المشاركة لضمان الاستجابة الموحّدة والفعّالة للحوادث السيبرانية.
- **المشاركة الفعّالة للجهات المعنية:** من المتوقع مشاركة كافة الجهات المعنية، بما فيها المؤسسات العامة والخاصة، بفعّالية في دعم جهود الوكالة الوطنية للأمن السيبراني في إدارة الحوادث والمساهمة في نجاحها.
- **التحسين المستمر:** سيخضع الإطار الوطني لمراجعات وتحديثات دورية بناءً على التهديدات الناشئة والتطورات التكنولوجية والدروس المستفادة لضمان استمرارية فعاليته وملاءمته.
- **التكامل مع السياسات الحالية:** سيتماشى الإطار الوطني لإدارة الحوادث مع السياسات والخطط والإجراءات الوطنية الحالية الأُخرى لضمان اتّساقه وفعاليته.

5.1 التعريفات

1.5.1 حادثة أمن المعلومات

وفقاً لتعريف الإصدار 1.2 من معيار تأمين المعلومات الوطنية لدولة قطر، "إنّ حادث أمن المعلومات هو حادث يؤثر على تعديل (على سرية أو توافر أو سلامة أي نظام أو شبكة معلومات من خلال إجراء يخالف سياسة الأمن المنصوص عليها. ولأغراض هذا النطاق، يتم تعريف الحادث بأنه انتهاك أو تهديد وشيك بانتهاك سياسات أمن الحاسب الآلي أو سياسات الاستخدام المقبولة أو الممارسات النموذجية "[1].

2.5.1 الحادثة السيبرانية ذات التأثير الوطني

تُعرّف الحادثة السيبرانية ذات التأثير الوطني في دولة قطر على أنها حادثة سيبرانية لها تأثير سلبي على الأصول المعلوماتية لدولة قطر (بما فيها أنظمة التحكّم الصناعية والتكنولوجيا التشغيلية الأخرى) و/أو بنيتها التحتية التمكينية.

3.5.1 الأزمة

وفقًا لمعيار ISO 22361:2022، تُعرف الأزمة بأنها حالة غير مستقرة وغير طبيعية تهدد المنظمة أو المجتمع وتتطلب استجابة استراتيجية وتكيفية وفي الوقت المناسب للحفاظ على بقاء المنظمة وسلامتها (ISO)[2].

6.1 تصنيف الحوادث السيبرانية

عند رصد حادثة سيبرانية محتملة، تُجري الوكالة الوطنية للأمن السيبراني تحليلاً لها، ومن ثم تقوم بتصنيفها كحادثة سيبرانية ذات تأثير وطني (أحمر، برتقالي، أصفر) أو حادثة سيبرانية لا تؤثر على المستوى الوطني (أبيض) بناءً على تأثيرها، وخطورتها، وانتشارها، والحاجة الملحّة لاتخاذ الإجراء الصحيح بشأنها. كما ويحدّد تصنيف الحادثة تقسيم المسؤوليات بين الجهات المشاركة (الوكالة الوطنية للأمن السيبراني. وفريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع، والجهة المتضررة)، والخطوات العملية التي سيتم اتخاذها في كافة مراحل إدارتها، ومستوى طبيعة مشاركة الشركاء.

[1] Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)
[2] ISO. (2022). ISO 22361:2022 - Security and resilience — Crisis management — Guidelines. International Organization for Standardization.

تقوم الوكالة الوطنية للأمن السيبراني بتعيين إحدى الفئات التالية لأي حادثة سيبرانية يتم الإبلاغ عنها:

حادثة سيبرانية يتم تنسيقها على مستوى الدولة

حادثة سيبرانية تمثل تهديدات كبيرة أو تكشف ثغرات أمنية خطيرة تؤثر على الحكومة أو القطاعين سواءً العام أو الخاص، مع احتمال وقوع عواقب خطيرة اقتصادية أو اجتماعية أو متعلقة بالأمن الوطني أو بالسمعة، تتطلّب استجابة منسّقة على مستوى الدولة.

حادثة سيبرانية يتم تنسيقها على مستوى القطاع

حادثة سيبرانية كبيرة تنطوي على تهديدات كبيرة أو ثغرات أمنية خطيرة قد تكون مصحوبةً بعواقب وخيمة على قطاع معيّن أو جهة كبرى، حيث يمكن احتواء الضرر باستجابة منسّقة على مستوى القطاع.

حادثة سيبرانية يتم تنسيقها على مستوى الجهة

حادثة سيبرانية ذات تأثير وطني يتم تنسيقها على مستوى الجهة ولا تؤثر سوى على جهة واحدة، من المرجّح احتواؤها على مستوى تلك الجهة مع الحدّ من انتشارها وعدم ترك أي آثار بالغة أوسع لها، ولكن ينبغي مراقبتها لضمان عدم حدوث أي تصعيد محتمل.

حادثة ليس لها تأثير وطني

حادثة سيبرانية ليس لها تأثير وطني ولا تؤثر على الخدمات الوطنية الحيوية، يمكن احتواؤها من قبل الجهة المتضررة ولا يكون لها تأثير على المستوى الوطني، ولكن يمكن تسجيلها لأغراض إحصائية تتم من قبل الوكالة الوطنية للأمن السيبراني في المستقبل.

الشكل 1: تصنيفات الحوادث ذات التأثير الوطني

يتم تصنيف الحوادث السيبرانية من قبل الوكالة الوطنية للأمن السيبراني خلال مرحلة الإبلاغ والتصنيف المُفصلة في مراحل إدارة الحادثة السيبرانية .

في فترة الأحداث الكبرى، يمكن للوكالة الوطنية للأمن السيبراني تعديل معايير فئات الحوادث بشكل استباقي في إطار الجهود التي تبذلها لرفع جاهزيتها. وتعرّف فترة الأحداث الكبرى بأنّها فترة زمنية تقع خلالها حادثة سيبرانية ذات تأثير اقتصادي أو أمني أو ثقافي داخل دولة قطر تستلزم رفع درجة التأهب والاستعداد على مستوى وطني.

1.6.1 تصعيد الأزمة السيبرانية

في حال تصعيد الحادثة السيبرانية ذات التأثير الوطني إلى أزمة، فإنه من الضروري اعتماد نهج استراتيجي وتدريجي للاستجابة. وللتعامل مع ذلك، يتيح الإطار الوطني لإدارة الأزمات السيبرانية القدرة على إدارة الأزمات السيبرانية الوطنية مقارنةً بالإطار الوطني لإدارة الحوادث، حيث يتطلّب اتخاذ تدابير استثنائية وبذل جهود منسّقة وتحديد الموارد لضمان الاستجابة الفعّالة، وتسهيل التعافي، والتشجيع على تكييف مفاهيم السرعة والقدرة على مواجهة التحديات على المستويات الوطنية والقطاعية والمؤسسية.

02

حوكمة الإطار الوطني لإدارة الحوادث السيبرانية

2. حوكمة الإطار الوطني لإدارة الحوادث السيبرانية

1.2 الصلاحيات

بموجب القرار الأميري رقم (1) لسنة 2021، تتولّى الوكالة الوطنية للأمن السيبراني مسؤولية حماية الفضاء السيبراني لدولة قطر. ولتمكين الوكالة الوطنية من القيام بمهامها، فقد تم إنشاء الإطار الوطني لإدارة الحوادث السيبرانية بغرض توفير معلومات تفصيلية حول كيفية إدارة الحوادث السيبرانية من قبل الوكالة الوطنية والجهات المشاركة. كما تتحمّل الوكالة الوطنية للأمن السيبراني مسؤولية إدارة الحوادث والاستجابة لها عند وقوع الحوادث ذات التأثير الوطني والتي تؤثّر على المؤسسات الوطنية الحيوية والخدمات الحيوية بمساندة الشركاء الرئيسيين.

ووفقاً للمادة رقم (3) من القرار المذكور أعلاه، يحقّ للوكالة الوطنية للأمن السيبراني في إطار الصلاحيات الممنوحة لها "**إعداد وتنفيذ الخطة الوطنية للاستجابة والتعافي من الحوادث والهجمات السيبرانية بالتنسيق مع الجهات المشاركة**"[3].

بالإضافة إلى ذلك فإن الإطار الوطني لإدارة الحوادث السيبرانية يتماشى مع أهداف الاستراتيجية الوطنية للأمن السيبراني الثانية والتي تعد جزءًا أساسياً من رؤية قطر الوطنية 2030.

2.2 الخدمات

تضطلع الوكالة الوطنية للأمن السيبراني بدور محوري في حماية الفضاء السيبراني لدولة قطر عبر إدارة الحوادث ذات التأثير الوطني، حيث تعمل على تنفيذ تدابير استباقية للتخفيف من حدّة المخاطر وتعزيز قدرات الدولة للاستجابة للحوادث.

تتولّى الوكالة الوطنية للأمن السيبراني مسؤولية التحقيق في الحوادث السيبرانية، وتحليلها، وإعداد التقارير الفنية الناتجة عن عملية التحليل، كما تدعم جهود تقديم ومتابعة إرشادات المعالجة لضمان التعافي الفعّال واحتواء التهديدات. كما وتصدر الوكالة الوطنية للأمن السيبراني إرشادات تتعلق بالاستجابة للحوادث، بما يتيح تقديم المشورة الفنية لتحسين تدابير الأمن السيبراني. وبالإضافة إلى ذلك، تقوم الوكالة الوطنية للأمن السيبراني بتنفيذ برامج تدريبية دورية لرفع كفاءة الجهات المعنية في الاستجابة للحوادث السيبرانية، مما سيضمن للوكالة تقديم خدمات استجابة فعّالة في الوقت المناسب خلال الحوادث ذات التأثير الوطني، مع توفير الدعم للتعافي والمعالجة في كافة القطاعات الحيوية والجهات الحكومية.

3.2 التحقيق الجنائي في الحوادث السيبرانية

بموجب قانون مكافحة الجرائم الإلكترونية في دولة قطر رقم (14) سنة 2014، تم تعريف الجريمة الإلكترونية في القانون بأنّها "**أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون**"[4].

وتتم إجراءات جمع الاستدلالات من قبل إدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية و/أو جهاز أمن الدولة بالتنسيق مع النيابة العامة بشكل مستقل عن إجراءات الاستجابة للحوادث التي تحددها الوكالة الوطنية للأمن السيبراني.

وفي حال البدء بتحقيق جنائي، تقوم الوكالة الوطنية للأمن السيبراني باتباع الإجراءات المنصوص عليها في الإطار الوطني لإدارة الحوادث السيبرانية والتنسيق مع سلطات إنفاذ القانون والسلطات المختصة وتقديم الدعم الفني في التحقيق الجنائي.

تقوم إدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية والوكالة الوطنية للأمن السيبراني بالتنسيق في عملية جمع البيانات الرقمية بما يتماشى مع أفضل الممارسات الدولية ومبادئ جمع الأدلة.

[3] القرار الأميري رقم 1 لسنة 2021 بإنشاء الوكالة الوطنية للأمن السيبراني، المادة 3، منشور في بوابة الميزان القانونية، متاح على: www.almeezan.qa.

[4] قانون رقم (14) لسنة 2014 بشأن مكافحة الجرائم الاقتصادية والإلكترونية. موقع الميزان (https://almeezan.qa) في فبراير 2025

03

الجهات المشاركة في الإطار الوطني لإدارة الحوادث السيبرانية

3. الجهات المشاركة في الإطار الوطني لإدارة الحوادث السيبرانية

يقتضي الإطار الوطني لإدارة الحوادث والذي أصدرته الوكالة الوطنية للأمن السيبراني التعاون بين الجهات المشاركة، وهو أمر ضروري لإدارة الحوادث السيبرانية ذات التأثير الوطني، والتحقيق فيها، ومعالجتها بشكل فعّال. وبالإضافة إلى ذلك، فإنه خلال مرحلة بدء الاستجابة للحادثة، يتم تشكيل عدّة مجموعات وفرق لتنسيق الاستجابة للحادثة السيبرانية ذات التأثير الوطني. يوضح هذا القسم الجهات المشاركة بالإطار الوطني لإدارة الحوادث السيبرانية، حيث يعرض الشكل 2 الجهات المشاركة المشمولة ضمن مراحل الاستجابة للحادثة السيبرانية، بينما يوضح الشكل 3 مجموعات إدارة الاستجابة للحوادث السيبرانية، والتي يتم تشكيلها للتعامل مع الحادثة خلال فترة الاستجابة.

1.3 الجهات المشاركة

تشمل الجهات المشاركة جميع الشركاء وفرق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع والجهات الأخرى التي تتعاون مع الوكالة الوطنية للأمن السيبراني على إدارة الحوادث والاستجابة لها.

الوكالة الوطنية للأمن السيبراني

الوكالة الوطنية للأمن السيبراني هي الجهة المسؤولة عن ضمان استمرارية تحديث الإطار الوطني لإدارة الحوادث السيبرانية والإشراف على تطبيقه، والجهة المعنية الأساسية المسؤولة عن الاستجابة للحوادث السيبرانية، ومعالجتها، وإدارتها.

الشركاء

يشمل الجهات الحكومية المُختارة والتي تدعم الوكالة الوطنية للأمن السيبراني في مراحل إدارة الحوادث السيبرانية. ويُعتبر الشركاء مسؤولون عن مجالات اختصاصهم في سياق الحوادث السيبرانية.

فريق إدارة الأزمات

يتم إشراك فريق إدارة الأزمات في حال تم الإعلان عن حدوث أزمة بسبب حادثة سيبرانية، ويتم تسليم فريق إدارة الأزمات المسؤوليات الاستراتيجية الوطنية من الفريق المفوض، بينما يحتفظ الفريق المفوض بالمسؤوليات التشغيلية الهامة.

فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع

هي مؤسسة لها سلطات رقابية ضمن قطاع معيّن ولديها القدرات الكافية في مجال الأمن السيبراني لأداء أنشطة الاستجابة للحوادث السيبرانية. وقد يتم تعيين هذا الدور للمؤسسة وفقاً لما تحدده الوكالة الوطنية للأمن السيبراني. ويجب على هذه الفرق أن تستوفي معايير معيّنة وأن تكون قادرة على دعم الاستجابة للحوادث على مستوى القطاع. كما وتقوم الوكالة الوطنية للأمن السيبراني بتنسيق الاستجابة للحوادث السيبرانية ذات التأثير الوطني مع فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع المعني بالجهات المتضررة.

الجهات المُتضررة

هي المؤسسات الوطنية الحيوية أو الجهات الحكومية أو أي من الجهات الأُخرى ضمن الفضاء السيبراني لدولة قطر والتي تأثّرت بالحادثة السيبرانية. وتُصبح الجهة "جهة مُتضررة" في اللحظة التي يتم فيها اكتشاف الحادثة وإبلاغ الوكالة الوطنية للأمن السيبراني عنها.

الشكل 2: الجهات المشاركة

2.3 مجموعات إدارة الاستجابة للحوادث السيبرانية

يتم تشكيل مجموعات إدارة الاستجابة للحوادث السيبرانية من قبل الوكالة الوطنية للأمن السيبراني استجابةً لحادثة معيّنة ذات تأثير وطني لغرض التعاون وتقديم الدعم، حيث تدعم هذه الفرق الاستجابة للحوادث السيبرانية وإدارتها طوال فترة الحادثة السيبرانية.

الفريق المُفوض

الفريق المُفوض هو مجموعة من كبار المسؤولين التنفيذيين من الجهات الحيوية. ويتولى الفريق مسؤولية مراقبة عملية إدارة الحادثة واتخاذ القرارات الاستراتيجية المتعلّقة به. ويتمثل الغرض من الفريق المفوض في جمع ممثلي الجهات المعنية الاستراتيجيين في مجموعة واحدة، بما يسمح لهم باتخاذ قرارات سريعة وفعّالة. ويتم تشكيل هذا الفريق خصيصاً طوال فترة الحادثة السيبرانية.

فريق الدعم من الجهة المُتضررة

تُقدم الجهة المُتضررة الدعم لفريق الاستجابة للحادثة التابع للوكالة الوطنية للأمن السيبراني أو فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع في أنشطة الاستجابة للحادثة السيبرانية. ويقوم فريق الدعم من الجهة المُتضررة بتسهيل إتاحة الوصول المادي والرقمي المطلوب، وتوفير المعلومات الضرورية حول الجهة، وتقديم الدعم اللوجستي والإداري.

فريق العمل الفني

فريق العمل الفني هو مجموعة فنيين متخصّصين مؤهّلين وذوي خبرة يتولون مسؤولية المراقبة الفنية للحادثة ويتم تشكيل هذا الفريق خصيصاً طوال فترة الحادثة السيبرانية.

فريق الاستجابة للحادثة

يتولّى فريق الاستجابة للحادثة العديد من المهام خلال مراحل إدارة الحادثة، وتؤدي الوكالة الوطنية للأمن السيبراني دائمًا دور الفريق الأولي للاستجابة للحادثة بعد مرحلة البدء (الموضحة في مراحل إدارة الحادثة السيبرانية الشكل 4). وبعد جمع البيانات الرقمية، يجوز تفويض دور فريق الاستجابة للحادثة إلى فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع (في الحادثة المصنفة باللون البرتقالي) أو الجهة المُتضررة (في الحادثة المصنفة باللون الأصفر).

الشكل 3: مجموعات إدارة الاستجابة للحوادث السيبرانية

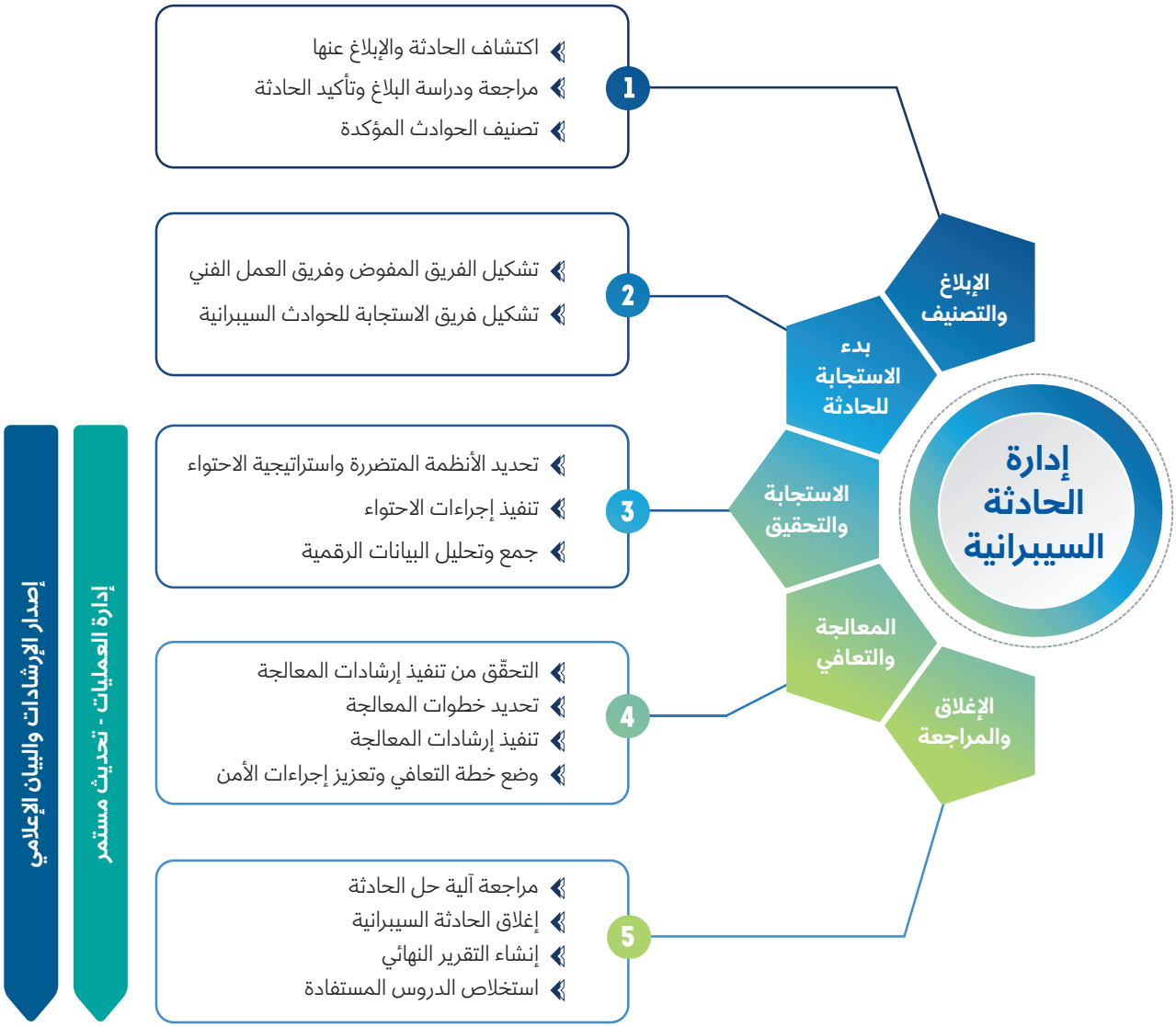
04

مراحل إدارة الحادثة السيبرانية

4. مراحل إدارة الحادثة السيبرانية

تعتبر مراحل إدارة الحادثة نهجاً منظّماً للتعامل مع الحوادث السيبرانية، وتتم على خمسة مراحل. وتمثل هذه المراحل العملية الشاملة للإدارة الفعّالة للحوادث السيبرانية ذات التأثير الوطني، بما يضمن الاستجابة السريعة والمنسّقة.

المراحل الخمس لإدارة الحادثة السيبرانية موضحة في الشكل 4:



الشكل 4: مراحل إدارة الحادثة السيبرانية

تبدأ إدارة الحادثة بمرحلة الإبلاغ والتصنيف وتنتهي بمرحلة الإغلاق والمراجعة.

وبالإضافة إلى المراحل المذكورة أعلاه، يشمل الإطار الوطني لإدارة الحوادث السيبرانية أنشطة إدارة العمليات التي تجري بالتوازي مع المراحل الثلاث الأخيرة.

أنشطة إدارة العمليات

تبدأ أنشطة إدارة العمليات بعد إتمام مرحلة بدء الاستجابة للحادثة. وتجري هذه المرحلة بالتوازي مع بقية المراحل، وتشمل جميع أنشطة الإدارة والتنسيق حتى إغلاق الحادثة. وفي نطاق إدارة العمليات، يتّخذ الفريق المفوض قرارات استراتيجية بشأن أنشطة الاستجابة، بدعم من فريق العمل الفني.

وبناءً على تصنيف الحادثة، تعطي الوكالة الوطنية للأمن السيبراني تعليماتها بشأن كيفية الاستجابة وتخصيص الأنشطة وفق إجراءات محددة، ويجوز لها أيضًا تفويض هذه المسؤولية جزئيًا إلى فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع أو الجهة المتضررة. وفي نطاق إدارة العمليات، يجوز للوكالة الوطنية للأمن السيبراني إصدار الإرشادات والبيانات الإعلامية بالتنسيق مع الجهة المختصة. وفيما يلي ملخص ومقارنة بين شكل الإصدارين:

إرشادات الوكالة الوطنية للأمن السيبراني

- **الإرشادات الفنية**: محتواها متعلق بالتهديدات أو الثغرات الأمنية.
- **الجمهور المستهدف**: المصرح لهم فقط وفق بروتوكول الإشارة الضوئية المستخدم.

البيان الإعلامي

- بيان عام حول الحادثة.
- الجمهور المستهدف : الجمهور العام.
- معتمد وصادر عن الفريق المفوض والوكالة الوطنية للأمن السيبراني والسلطات المعنية الأخرى.
- قد يكون على شكل بيان إعلامي أو مقابلة تلفزيونية أو تصريح صحفي أو منشور على وسائل التواصل الاجتماعي أو غير ذلك.

1.4 مرحلة الإبلاغ والتصنيف

يُعد الإبلاغ الفوري عن الحوادث شديدة الخطورة أمراً بالغ الأهمية لضمان الاستجابة السريعة والفعّالة. لذا، تحث الوكالة الوطنية للأمن السيبراني الجهات المعنية على التواصل معها عبر بيانات التواصل المُتاحة على الموقع الإلكتروني للوكالة[5]، إذ تضمن التبليغات بالحوادث في الوقت المناسب الاستجابة السريعة من قبل الوكالة الوطنية للأمن السيبراني للحدّ من انتشار الحادثة والتخفيف من تأثيرها السلبي و قد تمنع المزيد من التصعيد.

ووفقًا لمعيار تأمين المعلومات الوطنية لدولة قطر[6]، يتعيّن على جميع المؤسسات داخل دولة قطر إبلاغ الوكالة الوطنية للأمن السيبراني بالحوادث السيبرانية الحرجة في غضون ساعتين من تحديدها.

ولهذا، تتيح الوكالة الوطنية للأمن السيبراني قنوات إبلاغ متعدّدة يمكن من خلالها الإبلاغ عن الحوادث، حيث تقوم الوكالة الوطنية للأمن السيبراني عند استلام البلاغ بتقييمه لتأكيد الحادثة. وتصنّف الوكالة الوطنية للأمن السيبراني الحوادث المؤكدة بناءً على درجة خطورتها، ومدى انتشارها، ومدى ضرورة سرعة التعامل معها، ومدى تأثيرها على المستوى الوطني.

تجدر الإشارة إلى أن تصنيف الحوادث الذي تجريه الوكالة الوطنية للأمن السيبراني يقيّم تأثير الحادثة السيبرانية على المستوى الوطني، بمعزل عن التصنيف الذي تُجريه الجهة المُتضررة داخليًا.

2.4 مرحلة بدء الاستجابة للحادثة

بعد التصنيف، يتم بدء عملية الاستجابة للحادثة السيبرانية عن طريق إبلاغ الجهات المشاركة، وتحديد فريق الاستجابة للحادثة السيبرانية، وجمع المعلومات الأولية عن الحادثة السيبرانية. وخلال هذه المرحلة، تبدأ الوكالة الوطنية للأمن السيبراني باستدعاء كل من الكوادر الداخلية والجهات المعنية الخارجية لإدارة الحادثة السيبرانية والاستجابة لها. وعلى وجه التحديد، يتم تشكيل الفرق التالية فيما يتعلّق بكل حادثة ذات تأثير وطني:

- فريق الاستجابة للحادثة السيبرانية التابع للوكالة الوطنية للأمن السيبراني
- فريق الدعم من الجهة المتضررة
- الفريق المفوض
- فريق العمل الفني

[5] https://www.ncsa.gov.qa
[6] Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)

3.4 مرحلة الاستجابة والتحقيق

تبدأ مرحلة الاستجابة والتحقيق بعد إتمام مرحلة بدء الاستجابة للحادثة السيبرانية. وفي هذه المرحلة، يتّخذ فريق الاستجابة للحادثة إجراءات فورية لاحتواء الحادثة السيبرانية والحدّ منها. كما ويُجري فريق الاستجابة للحادثة السيبرانية تحقيقًا شاملاً مؤلفًا من عدّة خطوات، مع التركيز على الوقاية من الضرر ومنع الانتشار.

يتم تحليل الحادثة السيبرانية إمّا من قبل الوكالة الوطنية للأمن السيبراني، أو فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع المعني، أو الجهة المتضررة نفسها بحسب تصنيف الحادثة ووفقًا لعوامل أخرى، وتقوم الوكالة الوطنية للأمن السيبراني بتحديد الجهة المسؤولة وإبلاغها بذلك.

1.3.4 الاستجابة الأولية

في نطاق الاستجابة الأولية، يتّخذ فريق الاستجابة للحادثة السيبرانية التابع للوكالة الوطنية للأمن السيبراني إجراءات فورية لتأمين (تقييد الوصول المادي والرقمي) للأنظمة المتضررة، واحتواء الحادثة السيبرانية لمنع تفاقم الضرر وانتشاره. ويُعتبر الهدف الأساسي من عملية الاحتواء هو عدم تصعيد الحادثة بشكل أكبر وضبطها لإجراء تحقيق شامل وإيجاد حلّ نهائي لها.

2.3.4 جمع البيانات الرقمية والتحقيق فيها

تتضمن مرحلة التحقيق جمع البيانات الرقمية وتحليلها، حيث يتم جمع البيانات الرقمية فقط من قبل الوكالة الوطنية للأمن السيبراني وإدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية لضمان استيفائها للمتطلبات القانونية، ومن ثم يتم تحليل البيانات الرقمية التي تم جمعها لتحديد السبب الجذري للحادثة السيبرانية، وتقييم مدى الضرر، لمعالجته والحدّ منه.

كما ويقوم فريق الاستجابة للحادثة السيبرانية بتقييم تأثير الحادثة على الأنظمة والبيانات والعمليات، حيث يساعد ذلك في تحديد أولويات جهود التعافي والتوجيه للتواصل مع الجهات المعنية.

3.3.4 التواصل والتحديث المستمر

خلال مرحلة الاستجابة للحادثة السيبرانية، يعتبر التواصل الفعال والمستمر أمرًا ضروريًا، حيث يقدّم فريق الاستجابة للحادثة السيبرانية تحديثات منتظمة للجهات المشاركة، بما في ذلك كبار المسؤولين التنفيذيين والإدارات المتضررة من الجهة والشركاء الخارجيين، ممّا يضمن الشفافية وتنسيق الجهود. كما ويتم إنشاء تقارير تفصيلية لتوثيق الحادثة السيبرانية والإجراءات المتخذة والدروس المستفادة، مما يُسهم في التحسين المستمر لوضع الأمن السيبراني للمؤسسة.

4.4 مرحلة المعالجة والتعافي

يتم تفعيل مرحلة المعالجة والتعافي حالما ينهي فريق الاستجابة للحادثة السيبرانية الإجراءات الأولية للاستجابة والتحقيق. ويُعد الغرض من مرحلة المعالجة والتعافي هو معالجة عواقب الحادثة السيبرانية واستعادة الجاهزية التشغيلية. وفي هذه المرحلة، تقوم الوكالة الوطنية للأمن السيبراني أو فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع بتقديم إرشادات المعالجة والتحقق من تنفيذها.

يتم تقديم خطة المعالجة والتعافي إما من قبل الوكالة الوطنية للأمن السيبراني، أو فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع المعني، أو من قبل الجهة المتضررة بحسب تصنيف الحادثة السيبرانية ووفقًا لعوامل أخرى.

5.4 مرحلة الإغلاق والمراجعة

حالما ينتهي فريق الاستجابة للحادثة السيبرانية من أنشطة الاستجابة والتحقّق من تنفيذ إرشادات المعالجة والتعافي، يتم في المرحلة النهائية إغلاق الحادثة رسميًا وإجراء مراجعة شاملة لما بعد الحادثة. وتتضمّن هذه المرحلة تقييم مدى فعّالية الاستجابة للحادثة السيبرانية، وتحديد مجالات التحسين، وتوثيق الدروس المستفادة. وتعدّ الاستنتاجات المستخلصة من هذه المراجعة أمرًا ضرورياً لتحسين إجراءات الاستجابة للحوادث السيبرانية، وتعزيز الوضع الأمني العام للمؤسسة، وتعزيز سبل التعاون بين كافة الجهات المعنية المشاركة. ويضمن هذا النهج المنظّم التحسين المستمر والجاهزية الدائمة لأي حوادث مُستقبلية.

05

الملحق

5. الملحق

1.5 جداول المصطلحـــات

1.1.5 - المصطلحات العامة

المصطلح	شرح المصطلح
حادثة سيبرانية	تُعرّف الحادثة السيبرانية ذات التأثير الوطني في دولة قطر بأنّها حادثة لها تأثير سلبي على الأصول المعلوماتية لدولة قطر (بما فيها أنظمة التحكّم الصناعية والتكنولوجيا التشغيلية الأخرى) و/أو بنيتها التحتية التمكينية [7].
فريق الاستجابة لطوارئ الحاسب الآلي	فريق الاستجابة لطوارئ الحاسب الآلي هو مجموعة من خبراء الأمن السيبراني المسؤولون عن الاستجابة لحوادث أمن الحاسوب والحدّ منها، وتقديم التوجيه والإرشاد حول أفضل الممارسات، وتسهيل التنسيق بين المؤسسات لتعزيز الأمن السيبراني عمومًا.
الأدلة	المعلومات التي تستخدمها إدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية (أو سلطات إنفاذ القانون الأخرى) للتحقيق الجنائي أو عندما تنسب البيانات التي تم جمعها وتحليلها إلى السبب الجذري أو الجدول الزمني المتعلّق بالحادثة. وعند البدء بالتحقيق الجنائي، ينبغي معاملة جميع البيانات الرقمية كأدلّة محتملة في هذا التحقيق الجنائي.
البيانات الرقمية	يستخدم مصطلح البيانات الرقمية عند الإشارة إلى مجموعة الحقائق أو المعلومات المتعلّقة بالحادثة، والتي قد تحتوي على أدلة واقعية. وتسري كافة مبادئ الأدلة على البيانات الرقمية.
حادثة ذات تأثير وطني	الحوادث السيبرانية التي تؤثر على البنية التحتية الوطنية الحيوية والخدمات الحيوية داخل دولة قطر.
الإطار الوطني لإدارة الحوادث	هو الإطار العام والقدرات اللازمة للاستعداد بكفاءة وفعّالية للحوادث ذات التأثير الوطني، والحدّ منها إذا أمكن، والاستجابة لها، واستعادة الأنظمة المتأثرة بسببها.
فترة الأحداث الكبرى	فترة زمنية يقع خلالها حادثة ذات تأثير اقتصادي أو أمني أو ثقافي داخل دولة قطر تستلزم رفع درجة التأهب والاستعداد على مستوى وطني.
الجهة المشاركة	المؤسسات القطرية المعنية بتنفيذ عمليات إدارة الحوادث الوطنية.
النظام	أي نقطة طرفية أو خادم أو بنية تحتية سحابية أو أداة برمجية أو بوابة إلكترونية أو جهة أُخرى يُمكن جمع البيانات الرقمية منها.

[7] Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa/ar/regulatory-tools)

2.1.5- الجهات المشاركة

الجهة المشاركة	وصف الجهة المشاركة
الجهة المتضررة	هيئة حكومية أو مؤسسة خاصة تأثرت بالحادثة السيبرانية ذات التأثير الوطني.
الفريق المفوض	الفريق المسؤول عن المراقبة واتخاذ القرارات الاستراتيجية ضمن عمليات إدارة الحوادث الوطنية.
المؤسسات الوطنية الحيوية	المؤسسات التي تقدّم خدمات حيوية في دولة قطر.
فريق الاستجابة للحوادث	يتولّى فريق الاستجابة للحادثة الجوانب التشغيلية لعملية إدارة الحادثة. ويجوز للوكالة الوطنية للأمن السيبراني أو فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع أو الجهة المُتضررة القيام بدور فريق الاستجابة للحادثة.
إدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية	الإدارة الوطنية المختصة في إنفاذ القانون بدولة قطر والمعنية بمعالجة الجرائم التي تنطوي على استخدام شبكات الاتصالات الحديثة مثل شبكة الإنترنت.
الوكالة الوطنية للأمن السيبراني	الوكالة الوطنية للأمن السيبراني في دولة قطر، وتعمل تحت رئاسة مجلس الوزراء.
النيابة العامة	هيئة قضائية مستقلة تتولى الدعوى العمومية باسم المجتمع وتشرف على شؤون الضبط القضائي وتسهر على تطبيق القوانين، وتختص دون غيرها بتحريك الدعوى الجنائية ومباشرتها ولا تحرك من غيرها إلا في الأحوال المبينة في القانون[8].
فريق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع	هو مؤسسة ضمن قطاع معيّن يجوز تعيينها لأداء هذا الدور حسبما تقرّره الوكالة الوطنية للأمن السيبراني ولديها قدرات كافية في مجال الأمن السيبراني لأداء أنشطة الاستجابة للحوادث. وتوافق الوكالة الوطنية للأمن السيبراني على فرق الاستجابة لطوارئ الحاسب الآلي على مستوى القطاع بناءً على معايير معيّنة ووفقاً لقدرتها على دعم الاستجابة للحوادث على مستوى القطاع.
جهاز أمن الدولة	هو جهاز حكومي في دولة قطر يتولّى ضمن الإطار الوطني لإدارة الحوادث مسؤولية الأمن الوطني والتحقيقات الجنائية بالتعاون مع إدارة مكافحة الجرائم الاقتصادية والإلكترونية بوزارة الداخلية.
فريق العمل الفني	تناط بفريق العمل الفني مسؤولية المراقبة الفنية وصنع القرار. ويقدّم فريق العمل الفني المشورة لفريق الاستجابة للحادثة ويصعّد أية مخاوف مثارة إلى الفريق المفوض.

[8] https://www.pp.gov.qa/English/Pages/default.aspx

2.5 بيانات الاتصال

يمكن استخدام بيانات الاتصال والإرشادات التالية للتواصل مع الوكالة الوطنية للأمن السيبراني في حال وقوع حادثة سيبرانية:

اسم الفريق	مكتب قيادة عمليات تنسيق الاتصالات
العنوان	ص.ب 24100، شارع وادي السيل، الدوحة، دولة قطر
المنطقة الزمنية	التوقيت القياسي العربي، توقيت غرينتش + 3 ساعات
رقم الهاتف	16555 متاح 7/24
البريد الإلكتروني	NCSOC@ncsa.gov.qa
رقم الهاتف الدولي	+974 51016555 متاح 7/24
البريد الإلكتروني المخصّص للتواصل الدولي	Cert@ncsa.gov.qa
المفاتيح العامة والتشفير	يمكن استخدام المفتاح العام للوكالة الوطنية للأمن السيبراني عند رغبتكم في/حاجتكم إلى تشفير الرسائل المرسلة إلى الوكالة الوطنية للأمن السيبراني. وإذا لزم الأمر، ستقوم الوكالة الوطنية للأمن السيبراني بتوقيع الرسائل باستخدام المفتاح عينه. للحصول على المفتاح العام، يرجى الاتصال بالوكالة الوطنية للأمن السيبراني باستخدام المعلومات أعلاه. وعند الضرورة، يرجى توقيع رسائلكم باستخدام مفتاحكم الخاص – ومن الأفضل أن يتم التحقّق من صحّة هذا المفتاح باستخدام خوادم المفاتيح العامة.
الموقع الإلكتروني	https://www.ncsa.gov.qa

3.5 المواد ذات الصلة

معيار تأمين المعلومات الوطنية[9]

معيار قطري يهدف إلى تنظيم وحوكمة تأمين البيانات وأمنها في مؤسسات دولة قطر وتحديد المبدأ الأساسي لفهم حوكمة البيانات وتغطية الضوابط المهمة لإدارة أمن المعلومات في المؤسسات.

الإطار الوطني للامتثال لأمن المعلومات[10]

إطار رقابي تم إنشاؤه للتحقّق من أمن المعلومات وضمانه بدعم وتوجيه من معيار تأمين المعلومات الوطنية.

4.5 جاهزية التحليل الرقمي

استعداد المؤسسة لجمع الأدلة الرقمية، والحفاظ عليها، وتحليلها، وتقديمها عند الحاجة. ويشمل التحليل الرقمي تنفيذ العمليات والإجراءات التي تمكّن المؤسسة من الاستفادة من الأدلّة الرقمية مع العمل على اختصار الوقت وخفض التكاليف المرتبطة بالتحليل الرقمي إلى أدنى حد ممكن. يُعد التحليل الرقمي أمرًا بالغ الأهمية لتمكين الاستجابة السريعة والفعالة للحوادث السيبرانية، مما يضمن التعامل السليم مع الأدلّة لدعم المتطلبات القانونية والرقابية.

فوائد جاهزية التحليل الرقمي

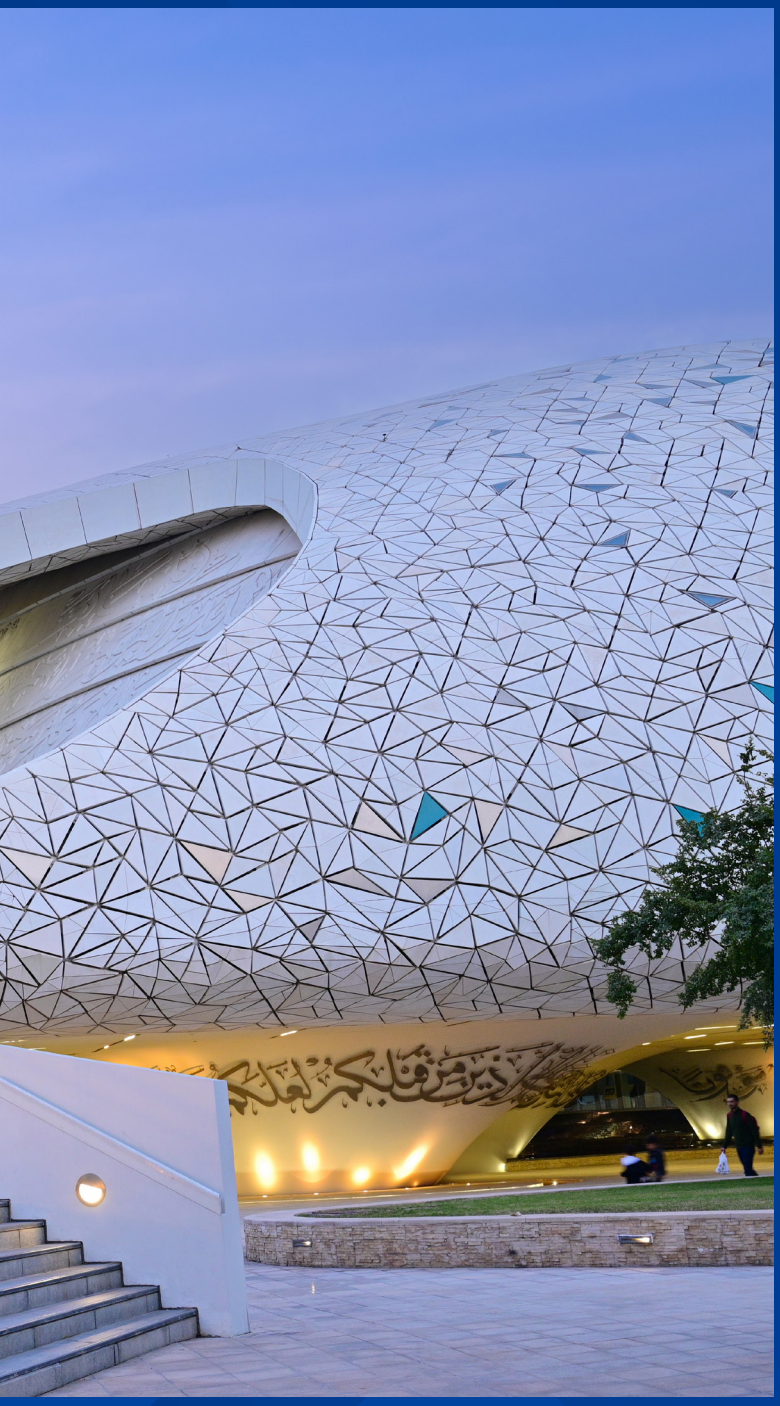
- **تحسين الاستجابة للحوادث:** تسهيل الجمع والتحليل السريع والفعّال للأدلّة، وبالتالي الحدّ من تأثير الحوادث واختصار وقت التعافي منها.
- **تحسين استمرارية الأعمال:** تقليل التعارض مع عمليات المؤسسة، وبالتالي ضمان استمرارية عمل البنية التحتية وإتاحة الخدمات الوطنية الحيوية.
- **تعزيز الوضع الأمني والتعاون:** تعزيز الأمن بشكل عام، ودعم التعاون الوطني، وتمكين التحسين المستمر من خلال المرئيات الاستراتيجية والدروس المستفادة.
- **كفاءة استغلال الموارد:** خفض التكاليف المباشرة وغير المباشرة لتحليل الأدلة الرقمية إلى أدنى حد ممكن من خلال وضع إجراءات وعمليات محدّدة مسبقًا.

[9] Cyber Security Policies and Standards | National Cyber Governance and Assurance Affairs (ncsa.gov.qa)
[10] National Information Security Compliance Framework | National Cyber Governance and Assurance Affairs (ncsa.gov.qa)

06

الخاتمة

6. الخاتمة



إن الإطار الوطني لإدارة الحوادث السيبرانية يدعم تلبية الاحتياجات والتحدّيات المُستجدة لدولة قطر، وذلك من خلال وضع نهجٍ شاملٍ ومنسّق لإدارة الحوادث السيبرانية ذات التأثير الوطني.

ويعد هذا الإطار مبادرة هامة لتعزيز قدرة الدولة ومؤسساتها للتعامل مع الحوادث السيبرانية ذات التأثير الوطني والاستجابة لها بكفاءة و فعالية.

ولقد كرست الوكالة الوطنية جهودها لإعداد وتطوير الإطار الوطني، وفقاً لأفضل الممارسات العالمية الخاصة بحوكمة الأمن السيبراني، فكانت النتيجة إطاراً وطنياً يضمن تضافر جهات الدولة وتعاونها في إدارة الحوادث السيبرانية ذات التأثير الوطني باختلاف أنواع التقنية. ويحمي بالتالي مكتسبات الدولة من أصول وموارد ويضمن استمرارية أعمالها.

كما ويعد الإطار الوطني لإدارة الحوادث السيبرانية مرجعاً استراتيجياً للقيادة الفعالة لإدارة الحوادث التي تهدّد الأمن الوطني ويضمن الاستجابة الفعالة لتحقيق استمرارية الخدمات الحيوية، ويضمن استعادة التشغيل الموثوق للخدمات خلال عملية إدارة الحادثة، والاستجابة لها، والتعافي منها.

ويتميز الإطار بكونه إطاراً ديناميكياً وقابلاً للتكيف، وفقاً للمتغيرات والمخاطر الناشئة بما يضمن جاهزية دولة قطر للاستجابة بشكل استباقي للوتيرة المتسارعة للتطور التكنولوجي العالمي.