الجمهورية العربية السورية

وزارة الاتصالات والتقانة
MINISTRY OF COMMUNICATIONS & TECHNOLOGY

استراتيجية الأمن السيبراني للجمهورية العربية السورية

ملخص تنفيذي

المقدمة:

تكتسب تكنولوجيا المعلومات والاتصالات أهمية كبيرة في تحقيق التنمية الاقتصادية والاجتماعية، وتزداد الأهمية أكثر في ظل الاعتماد المتزايد على شبكة الإنترنت لتبادل المعلومات والخدمات في الأعمال التجارية والحكومية، وتحول الاقتصاد التقليدي إلى الاقتصاد الرقمي من خلال رقمنة عدد من المجالات والقطاعات المختلفة، إلا أن ذلك أدى أيضاً إلى وجود بيئة ملائمة للجرائم المعلوماتية، لذلك تزايد الاهتمام بالأمن السيبراني وأصبح أمن المعلومات الرقمية جزءاً من الأمن الوطني وأمن الأفراد والشركات،

اعتمدت الحكومة في الجمهورية العربية السورية الاستراتيجية الوطنية للتحول الرقمي للخدمات الحكومية الإلكترونية عام 2021، وتسعى الحكومة من خلال هذه الاستراتيجية إلى تطوير قدراتها في مجال الأمن السيبراني، بهدف تعزيز مستوى حماية الأصول المعلوماتية من المخاطر السيبرانية الداخلية والخارجية، التي يمكن أن تؤثر بشكل كبير على مقدرات الدولة.

تسعى حكومة الجمهورية العربية السورية إلى تعزيز الاهتمام في مجالات الأمن السيبراني، من خلال تطوير السياسات، وتوفير الأدوات اللازمة لحماية الأصول المعلوماتية، وتعزيز القدرات الوطنية في مواجهة المخاطر السيبرانية المحتملة، حيث تشكل هذه الوثيقة التوجهات الوطنية الأساسية وإطار عمل مرجعي للعاملين والمهتمين في مجال الأمن السيبراني من القطاعين العام والخاص، بما يضمن حماية الأصول المعلوماتية وفقاً لأهميتها، ويضمن توزيع الأدوار وتحديد الصلاحيات بين جميع الأطراف سواء داخل المؤسسات أو على المستوى الوطني.

رؤية استراتيجية:

(فضاء سيبراني آمن وموثوق في جميع المجالات، بما يسهم في حماية المصالح الوطنية ويعزز الثقة في التحول الرقمي)

أهداف الاستراتيجية:

تسعى هذه الاستراتيجية إلى تحقيق الأهداف الآتية:

1. تأسيس بنية أمن سيبراني قوية ومستدامة توفر الحماية المتكاملة للأصول المعلوماتية والتقنية.
2. إدارة فعالة ومتكاملة لمواجهة التهديدات والتصدي للمخاطر على مستوى الجمهورية العربية السورية.
3. تطوير الجوانب التشريعية والتنظيمية، ووضع القواعد القانونية الملائمة، والإجراءات المتبعة للتصدي للجرائم الخاصة بالأمن السيبراني.
4. تطوير وصقل الإمكانات الوطنية، البشرية والتقنية للأمن السيبراني، وبناء الثقافة وإذكاء الوعي المجتمعي للوصول لأفضل الممارسات في مجال الأمن السيبراني.
5. تشجيع الأبحاث والتحقيقات والبحث العلمي في مجال الأمن السيبراني.
6. تحقيق الحوكمة الفعالة للتنسيق بين جميع الجهات وضمان حُسن التنفيذ.
7. تعزيز التنسيق والتعاون في قضايا الأمن السيبراني على المستويين الإقليمي والدولي.

برامج الاستراتيجية:

البرنامج الأول أمن البنى التحتية:

يهدف هذا البرنامج إلى دعم الشبكة والنظم المعلوماتية الوطنية بالحلول الأمنية العتادية والبرمجية والتصميمية لزيادة مناعتها في مواجهة الهجمات الإلكترونية وفق ما يلي:
إنشاء وتطوير المركز الوطني للاستجابة للطوارئ المعلوماتية، وتأهيل فريق مختص بتكنولوجيا المعلومات وأمنها للاستجابة للطوارئ المعلوماتية، وتشكيل فرق للاستجابة للطوارئ المعلوماتية في المؤسسات التي لديها منظومات معلوماتية، واستكمال بناء منظومة التوقيع الرقمي، بالإضافة لتعزيز البنية التحتية المعلوماتية للمؤسسات التي لديها منظومات معلوماتية.

البرنامج الثاني تطوير الإطار القانوني والتنظيمي:

يهدف البرنامج إلى مراجعة الجوانب القانونية والتنظيمية المتعلقة بالأمن السيبراني من قوانين وسياسات وضوابط وفق ما يلي:
إصدار تشريع للأمن السيبراني بعد مراجعة شاملة لكافة القوانين ذات الصلة بالأمن السيبراني، وقانون حماية البيانات الشخصية، إضافةً لتطوير وتحديث السياسات في مجال الأمن السيبراني.

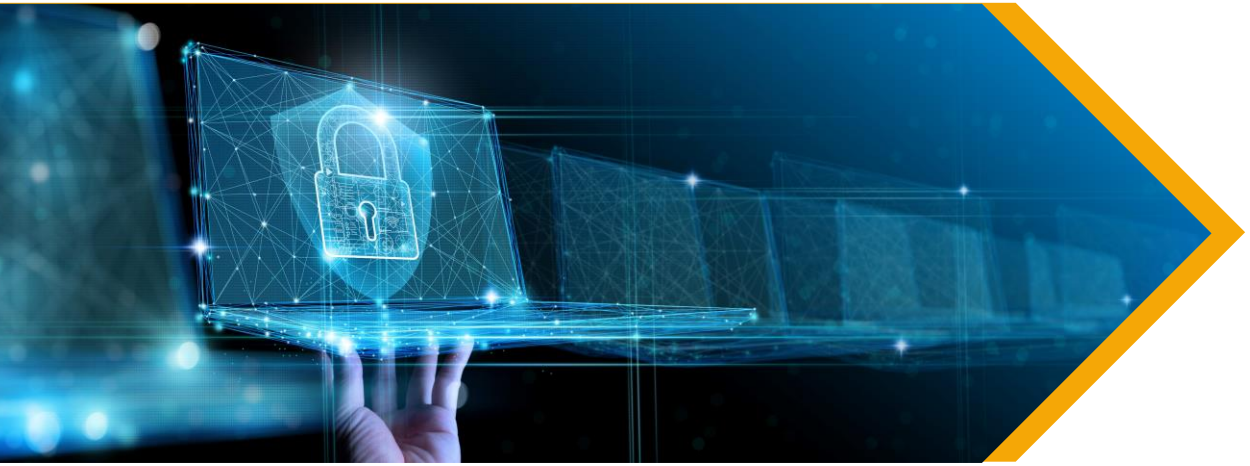
البرنامج الثالث نشر ثقافة الوعي السيبراني:

يهدف هذا البرنامج إلى تعزيز الوعي العام للمستخدمين بالقضايا الأساسية المتعلقة بالأمن السيبراني، وتم تحديد خمسة مسارات رئيسية لعمل البرنامج تتمثل بتعزيز الوعي بقضايا الأمن السيبراني، والثقة لدى المستخدمين تجاه الخدمات المقدمة على الشبكة، ورفع مستوى فهم المستخدمين لأهمية حماية بياناتهم على الشبكة، ووضع آلية لإدارة ومعالجة الشكاوى المتعلقة بالاستخدامات المسيئة على شبكة الإنترنت، والاعتماد على وسائل الإعلام والمنصات الإعلامية الرقمية في تغطية القضايا المتعلقة بالأمن السيبراني.

البرنامج الرابع بناء القدرات والمعرفة:

يهدف هذا البرنامج إلى تنمية القدرات في مجال الأمن السيبراني لدى الحكومة والقطاع الخاص والمواطنين بشكل عام، وذلك وفق ثلاث مسارات رئيسية هي:

1. التعليم في مجالات الأمن السيبراني
2. التدريب الاحترافي في مجالات الأمن السيبراني.
3. البحث والابتكار في مجالات الأمن السيبراني.



البرنامج الخامس الشراكات والتعاون الإقليمي والدولي :

يهدف البرنامج إلى تطوير الشراكات والتعاون على المستويين الإقليمي والدولي في مجال الأمن السيبراني، بما يسمح بتبادل الخبرات والإنذار المبكر حول الأخطار المحتملة والحوادث الأمنية الشائعة، ووضع آليات للتصدي لهذه الحوادث وخطة لمعالجتها من خلال مراكز الاستجابة للطوارئ المعلوماتية، وصولاً لإيجاد اتفاقات دولية وعربية في مجال مكافحة الجرائم الإلكترونية، وتعزيز دور القطاع الخاص المحلي في مجال الأمن السيبراني، بما يساهم في دعم الجهود الوطنية الرامية إلى رفع مستوى أمن المعلومات في القطاعين العام والخاص.

البرنامج السادس تطوير هياكل وظيفية متخصصة:

تخصيص وحدات هيكلية تُعنى بالأمن السيبراني في كل جهة عامة ضرورة ملحة، مع تأمين المستلزمات الفنية والكوادر البشرية المؤهلة والمدربة والتي تسهم في تنفيذ الاستراتيجية المقرة من الحكومة.

حوكمة الاستراتيجية

تشكيل اللجنة التنفيذية للأمن السيبراني، برئاسة وزير الاتصالات والتقانة وعضوية الوزارات والجهات المعنية المعنية بتنفيذ وتتبع تنفيذ استراتيجية الأمن السيبراني وفق البرامج الستة مع المبادرات والمشاريع الواردة ضمن الاستراتيجية
ترفع اللجنة تقاريرها إلى اللجنة العليا للتحول الرقمي برئاسة السيد رئيس مجلس الوزراء بهدف إقرار الخطط والأولويات المقترحة من اللجنة التنفيذية للأمن السيبراني وتأمين التمويل اللازم لتنفيذ المشاريع والمبادرات المتعلقة بالاستراتيجية ومتابعة التقدم في تنفيذ الاستراتيجية بناء على تقارير اللجنة التنفيذية للأمن السيبراني.
تتابع اللجنة الوطنية للأمن السيراني الوحدة الوظيفية المختصة بأمن المعلومات ضمن الوزارات والجهات المعنية بتنفيذ المشاريع والمبادرات وفق الخطط التي تضعها اللجنة التنفيذية للأمن السيبراني، والتوجيهات التي أقرتها اللجنة الوطنية للتحول الرقمي، وتحدد مهامها من قبل اللجنة التنفيذية.