



الجمهورية التونسية
رئاسة الجمهورية

الاستراتيجية الوطنية للأمن السيبراني

2030 - 2026
مجلس الأمن القومي



توطئة

تمّ إعداد الاستراتيجية الوطنية للأمن السيبرني 2026-2030 من قبل لجنة فنيّة أحدثت صلب لجنة أمن الاتّصالات والمعلومات المنبثقة عن مجلس الأمن القومي وذلك بعد مراجعة وتحيين الاستراتيجية الوطنيّة للأمن السيبرني 2020-2025.

وقد تمّ الاعتماد في ذلك على منهج تشاركي وتفاعلي، ساهمت فيه مختلف الأطراف المتداخلة في مجال الأمن السيبرني من وزارات وهيكل عموميّة وممثّلين عن القطاع الخاصّ وخبراء في المجال، إضافة إلى الاستئناس بالتّجارب المقارنة على المستوى الدّولي والممارسات الفضلى في المجال. وفي هذا الصّدد، وحرصاً على تعزيز جاهزيّة الدّولة لمواجهة التّحديات المستقبلية، تمّ إطلاق استشارة وطنيّة موسّعة شملت مختلف الأطراف المعنية، أفضت إلى إعداد الاستراتيجية الوطنيّة للأمن السيبرني 2026-2030.

وتهدف هذه الاستراتيجية إلى إرساء فضاء سيبرني آمن وموثوق من خلال الاستجابة لمتطلّبات المرحلة المتعلّقة أساساً بالتحوّلات التكنولوجيّة المتسارعة وتطوّر مكوّنات الفضاء السيبرني الوطني بالإضافة إلى تنامي التّحديات السيبرنية المتنوّعة والمستجدّة التي تستهدف مختلف شرائح المجتمع بما يهدّد الهوية الوطنيّة ويعيق النموّ الاقتصادي.

الفهرس

تقديم عامّ

4

تعريف المصطلحات

8

الرؤية

10

مجالات الاستراتيجيةّ

11

أهداف الاستراتيجية

15

أولويات تنفيذ مجالات الاستراتيجية

22

المتابعة والتّقييم

23

تقديم عام

في ظلّ التحوّلات الرقمية المتسارعة التي يشهدها العالم، أصبح الفضاء السيبرني جزءاً لا يتجزأ من مشاغل الأفراد والمؤسسات والدول، إذ تتيح فرصاً هامة للتنمية والتطوير لكنها تطرح في الوقت ذاته تحديات عديدة. كما أن الاعتماد المتزايد على التكنولوجيات الحديثة، واندماجها في مختلف مظاهر الحياة اليومية، على الصعيدين العام والخاص، أدّى إلى تنامي التهديدات السيبرنية بشكل غير مسبوق، مما يفرض على الدول وضع استراتيجيات شاملة، استباقية وفعالة لمجابهة هذه التحديات.

وفي هذا السياق، كلّف مجلس الأمن القومي خلال سنة 2018 فريق عمل تابع للجنة أمن الاتصالات والمعلومات، تحت إشراف السيد المستشار الأول للأمن القومي، لوضع الاستراتيجية الوطنية للأمن السيبرني 2020-2025.

وقد مثلت هذه الاستراتيجية نقلة حقيقية في تعاطي الدولة مع المسائل السيبرنية، حيث تم وضع أطر تشريعية وتنظيمية متقدمة وتفعيل آليات الاستجابة للطوارئ وتعزيز التعاون الدولي بالإضافة إلى جملة من المشاريع التي تهدف إلى الرفع من مستوى سلامة الفضاء السيبرني الوطني على غرار البرنامج الوطني للتدقيق في السلامة المعلوماتية لفائدة الهياكل الوطنية.

هذا، ويمثل تعزيز الحماية السيبرنية للأفراد والمجتمع ضرورة حيوية لترسيخ ثقة المواطنين في الفضاء السيبرني ولضمان سلامة الإقتصاد الرقمي الوطني والحد من الانعكاسات الإقتصادية والإجتماعية للجرائم الإلكترونية في ظل بيئة رقمية تتطور بوتيرة متسارعة.

غير أن التقييم الحالي لتنفيذ هذه الاستراتيجية كشف عن عدّة إشكاليات ونقائص وجب تداركها، من أبرزها محدودية البنية التحتية الرقمية والنقص في وسائل السلامة المعتمدة وتفاوت درجة وعي مختلف مكوّنات المجتمع بأهمية السلامة السيبرانية وكيفية التعامل مع التهديدات التي تستهدفها إلى جانب الصعوبات المتعلقة بعدم ملائمة منظومة الشّراءات العمومية لخصوصيّات المشاريع السيبرانية بالإضافة إلى غياب رؤية مهنية واضحة للمحافظة على الكفاءات الوطنية المتخصصة في المجال.

كما بيّن التقييم أن تطوّر أدوات الهجوم باستخدام الذكاء الاصطناعي قد ساهم في ظهور مخاطر جديدة وتزايد عددها، في وقت تتوسّع فيه رقعة الرّقمنة بشكل يفوق القدرة على مواكبتها بالإعتماد على الكفاءات الوطنية والآليات الفنية المتوفرة.

هذا وسجّل أيضا تنامي إستعمال شبكات التواصل الاجتماعي من قبل مختلف الفئات العمرية بما في ذلك الأطفال.

وتعتبر هذه الشبكات إحدى مكوّنات الفضاء السيبراني التي تكتسي خصوصية مقارنة ببقية المكونات على غرار الخدمات على الخط بإعتبار أنها تدار من قبل أطراف خارجية ويتم إيواؤها خارج حدود الوطن مما يشكّل تحديًا وي طرح صعوبات عملية في التعامل مع الإشكاليات المتعلقة بها على غرار الهجمات والإختراقات للصفحات الرسمية وحسابات المشرفين عليها. كما لوحظ إستعمال شبكات التواصل الاجتماعي لبث أخبار زائفة ومحاولة التضليل والتأثير على الرأي العام وهتك الأعراض بالإضافة إلى ظواهر تمسّ من الهوية التونسية وتستهدف الأطفال والفئات الهشة على الخط.

وفي المقابل، كشفت هذه المرحلة عن فرص هامة يمكن توظيفها لتطوير الأمن السيبراني الوطني، على غرار توفير الفرص الاقتصادية ومواطن شغل إضافية إلى جانب جلب المستثمرين والمختصين في المجال بالإضافة إلى دعم الشركات الناشئة في المجال الرقمي وتطوير البحث العلمي.

ووعيا بأنّ التحدّيات الجديدة المتجدّدة على مستوى الأمن السيبرني تتطلّب استعدادا إستباقيا ومنهجيا لمواجهتها وإدراكا لأهميّة ترسيخ بيئة رقمية آمنة وموثوقة وانطلاقا من الحرص على حماية المصالح الوطنيّة السياديّة وحقوق المواطنين، تضع الجمهوريّة التونسيّة هذه الاستراتيجية الوطنيّة للأمن السيبرني للفترة 2026-2030.

و تهدف هذه الاستراتيجية إلى إرساء رؤية وطنية شاملة تقوم على مقاربة متوازنة بين الجوانب التقنيّة والتوعويّة، وتحديد أهداف استراتيجية دقيقة، مع الحرص على توفير الإمكانيّات البشريّة والتكنولوجيّة الكفيلة بترجمة هذه الرؤية إلى واقع ملموس، في إطار مخطّط وطني موحد ومتكامل يستجيب لمقتضيات المرحلة ويعزّز سيادة تونس الرقميّة.

وقد أعدّت هذه الاستراتيجية استنادا إلى تقييم شامل للوضع الحاليّ واستلهاما من التجارب والممارسات الفضلى على الصّعيد العالميّ.

وإنّ نجاح تنفيذها يتطلّب التزاما قويا وتنسيقا فعّالا بين كافة الأطراف المتداخلة، لضمان أمن تونس السيبرني ومناعتها الرقميّة، وتحقيق التحوّل الرّقمي في إطار من السيادة والعدالة والثّقة.

و تعدّ هذه الاستراتيجية إطارا مرجعيّا وطنيا يمكن من :

- توحيد الجهود العموميّة والخاصّة في مجال الأمن السيبرني.
- تحسين القدرات الوطنيّة في الرّصد والتصدي والاستجابة للتهديدات السيبرنيّة.
- تعزيز ثقة المواطن والمستثمر في الاقتصاد الرّقمي.
- الاستثمار في الأمن السيبرني (الاستثمار في شركات ناشئة تطوّر تقنيات جديدة مثل الذكاء الاصطناعي والأمن السّحابي وأمن أنترنات الأشياء، إلخ).
- دعم التّعاون الدّولي والشّراكات.

ويغطّي نطاق هذه الاستراتيجية جميع مكوّنات الفضاء السيبرني من خدمات وبيانات وشبكات ومنصّات رقميّة وأنظمة معلوماتيّة بالإضافة إلى البنى التحتيّة الرقميّة الحسّاسة. ويمتدّ هذا النّطاق ليشمل جميع الفاعلين من أفراد ومؤسّسات وشركات في القطاعين العامّ والخاصّ فضلاً عن المجتمع المدني والوسط الأكاديمي والبحثي وجميع العمليّات التي تجري باستعمال هذه المكوّنات.

ويراعي نطاق الاستراتيجية التطوّرات التكنولوجيّة الحديثة على غرار الذكاء الاصطناعي وإنترنت الأشياء والحوسبة السّحابية وسلاسل الكتل لما لها من تأثير مباشر على أمن المعلومات وحماية البيانات واستمراريّة الخدمات الحيويّة في الفضاء الرّقمي.

تعريف المصطلحات

المصطلح	التعريف
الفضاء السيبرني	فضاء رقمي يربط منظومات المعالجة الالكترونية للمعطيات بشبكات المعلومات والاتصال ويشمل عناصر مادية ولا مادية من حواسيب وخوادم وأنظمة تشغيل وبرمجيات وشبكات اتصال ومحتوى رقمي والمستخدمين سواء كانوا مشغلين أو مستعملين وجميع العمليات التي تجري باستعمال هذه العناصر.
المرونة السيبرنية	القدرة على التوقّي من الهجمات السيبرنية والكشف عنها والاستجابة لها والتّعافي من أثارها إلى جانب القدرة على التكيّف وضمان استمرارية العمل وتحقيق التحسين المستمرّ.
الأزمات السيبرنية	حالة اضطراب بسبب حادث سيبرني أضرب بشكل متواصل بمكوّن أو أكثر من مكوّنات الفضاء السيبرني وأدى إلى تعطيل استمرارية الخدمات.
الدفاع السيبرني	مجموعة الوسائل والإجراءات التنظيمية والفنية والردعية التي تمكّن من الحماية ضدّ / الحدّ من تأثير والمعالجة السريعة للهجمات السيبرنية التي تستهدف البنى التحتية الرقمية الحيوية.
الأمن السيبرني	توفير الإمكانيات الضرورية لحماية الفضاء السيبرني ضدّ التهديدات التي يمكن أن تمسّ من سرية وسلامة وتوفّر المعطيات والخدمات.
السلامة السيبرنية	مختلف التدابير والآليات التقنية وغير التقنية التي يقع تركيزها بغرض حماية الفضاء السيبرني وتعزيز القدرة على الاستباقية والتوقّي من المخاطر السيبرنية والتفطن السريع للحوادث والهجمات السيبرنية والقدرة على الاستجابة في حالات الطوارئ بهدف الحدّ من التداعيات وضمان استمرارية النشاط عند حدوث الأزمات السيبرنية.

المصطلح	التعريف
التشفير ما بعد الكمي	نوع من التشفير يهدف إلى تطوير خوارزميات وبروتوكولات تشفير منيعة ضد الهجمات التي تعتمد على أجهزة الحوسبة الكمية مع الحفاظ على التوافق مع الأنظمة والبروتوكولات الحالية.
البنى التحتية الرقمية الحساسة	الأنظمة المعلوماتية التي تأوي الأصول والخدمات الحساسة على المستوى الوطني والتي يمكن أن يؤثر توقفها أو المس من سلامتها على الأمن القومي.
التمارين السيبرانية	أنشطة محاكاة منظّمة لحوادث أو هجمات سيبرانية تهدف إلى تقييم ورفع جاهزية الأفراد والمؤسسات في التعامل مع التهديدات السيبرانية.
التهديدات السيبرانية	مجموعة العوامل الخارجية أو الداخلية، العرضية أو المفصلة التي من شأنها المساس أو الإضرار بمكوّن أو أكثر من مكوّنات الفضاء السيبراني.
مركز الاستجابة للطوارئ السيبرانية	وحدة متخصصة تعمل على رصد وتحليل والاستجابة للحوادث والتهديدات السيبرانية التي تستهدف البنية التحتية الرقمية لمنظمة أو دولة، بهدف الحد من الأضرار، استعادة الأنظمة، وتنسيق الجهود بين الجهات المختلفة.

المراجع :

- [1] المرسوم عدد 17 لسنة 2023 الصادر في 11 مارس 2023 والمتعلق بالسلامة السيبرانية.
- [2] الإستراتيجية الوطنية للأمن السيبراني 2020–2025.
- [3] ISO.
- [4] NIST.

الرؤية

صيغت الرؤية لتلبي الاحتياجات والأولويات الوطنية في مجال الأمن السيبراني سعياً إلى حماية البنى التحتية الرقمية الحساسة والبيانات الوطنية من خلال بناء قدرات دفاعية قوية وتنمية كفاءات وطنية متخصصة بما يضمن دعم ثقة المجتمع في بيئة رقمية متطورة ومحمية من التهديدات السيبرانية.

فضاء سيبراني تونسي آمن وموثوق
به يعزز السيادة الوطنية ويدعم
التحول الرقمي والنمو الاقتصادي
وحماية الأسرة والمجتمع.



مجالات الاستراتيجية

تهدف المجالات إلى تحقيق الرؤية للاستراتيجية الوطنية للأمن السيبرني للفترة 2026-2030 وقد تمّ تحديدها استئناسا بالمعايير الدولية في مجال الأمن السيبرني والتي تشمل الجوانب التنظيمية والتقنية والموارد البشرية بالإضافة إلى التعاون الدولي.

وفي هذا الإطار، تمّ حصر خمس مجالات أساسية للاستراتيجية والتي تشكل الركائز المحورية لضمان فضاء سيبرني وطني آمن وموثوق به، كما يبينها الرسم البياني التالي :



مجالات الإستراتيجية

رسم بياني 1

1. الحوكمة والتوجهات الاستراتيجية القطاعية

يُعنى هذا المجال بتعزيز منظومة الحوكمة الفعّالة للأمن السيبرني من خلال تطوير الأطر التنظيمية والتشريعية التي تنظّم بيئة العمل السيبرني على المستويين الوطني والقطاعي، بما يضمن وضوح الأدوار وتحديد المسؤوليات بين الجهات ذات العلاقة.

يتم التركيز في هذا المجال على إنشاء آليات تنسيقية فعّالة لضمان التعاون والتكامل بين القطاعات المختلفة، وتفعيل الرقابة بالإضافة إلى الامتثال للإجراءات وتطبيق التوصيات والاستجابة للمعايير ذات الصلة. ويشمل هذا المجال أيضاً مواءمة الاستراتيجيات القطاعية للأمن السيبرني مع التوجهات الوطنية الشاملة بما يعزّز الانسجام ويمنع التداخل في الجهود ويسهم في بناء بيئة سيبرنية آمنة ومرنة وموثوقة تعزّز السيادة الوطنية وتدعم التحول الرقمي والنمو الاقتصادي وحماية الأسرة والمجتمع.

2. المرونة والتصدي للتهديدات السيبرنية

يعنى هذا المجال بتعزيز قدرة الدولة التونسية على التنبؤ بالمخاطر والتهديدات السيبرنية المحتملة والاستعداد المسبق لها، والاستجابة السريعة والفعّالة عند وقوعها، بما يضمن استمرارية الخدمات الحيوية وتقليل الآثار السلبية. ومن مستوجبات تحقيق ذلك تطوير بنية تحتية رقمية آمنة، تتسم بالمرونة والقدرة على التعافي من الهجمات، إلى جانب إرساء مراكز متطورة للاستجابة للطوارئ السيبرنية وتعزيزها بالإطارات المختصة وتزويدها بالتقنيات الحديثة. وهو يشمل وضع خطط وطنية لاختبار الجاهزية السيبرنية من خلال القيام بتمارين سيبرنية دورية وتعزيز قدرات الكشف المبكر والاستجابة المنسقة بين القطاعات العامة والخاصة ولا سيما في المجالات الحيوية. ويهدف هذا التوجّه إلى بناء منظومة وطنية متكاملة للصمود الرقمي تساهم في حماية مصالح الدولة الداخلية والخارجية وتعزيز الثقة الرقمية.

3. تطوير وبناء القدرات في مجال الأمن السيبرني

يهدف هذا المجال إلى تأهيل الكفاءات البشرية وتعزيز القدرات الفنيّة من خلال التّكوين الأكاديمي وبرامج التّأهيل المهني لتأمين الموارد البشريّة اللازمة لحماية الفضاء السيبرني ورفع مستوى الوعي بالمخاطر السيبرنيّة.

ويمكن ذلك في دعم وإدراج مفاهيم الأمن السيبرني ضمن البرامج التعليميّة في مختلف المستويات بدءًا من التّعليم الأساسي وصولًا إلى التّعليم العالي وإنشاء مسارات أكاديميّة متطوّرة بالتّعاون مع الجامعات والمؤسّسات البحثيّة الوطنيّة والدّوليّة. كما يتضمّن تصميم برامج تكوينيّة مهنيّة موجّهة لموظّفي القطاعات الحيويّة والهيكل الحكوميّة بالإضافة إلى دعم الشّهادات الاحترافيّة والتّكوين التطبيقي المستمرّ لضمان مواكبة أحدث التّقنيات والممارسات الفضلى العالميّة في المجال.

كما يولي هذا المجال أهميّة لتعزيز البحث والتّطوير في الأمن السيبرني، وتحفيز الابتكار المحليّ وبناء مجتمع مهني نشيط فيه من الخبراء والمختصّين ما يُسهم في خلق منظومة وطنيّة مستمرة وقادرة على التطوّر الذاتي ومجابهة التّحديات المستقبلية بأكثر فاعليّة.

4. التوعية ونشر ثقافة الأمن السيبرني في المجتمع

يُركّز هذا المجال على ترسيخ الوعي المجتمعي بالأمن السيبرني وتوجيه سلوكيّات المستخدمين نحو ممارسات رقميّة آمنة عبر حملات تحسيسيّة ومبادرات تعليميّة على كافّة المستويات تستهدف كافّة شرائح المجتمع ومختلف الفئات العمريّة مع مراعاة خصوصيّة الفئات الهشّة.

يتضمّن هذا المجال تنظيم أنشطة تحسيسيّة وتمارين تطبيقية بالإضافة إلى تطوير أدوات تفاعليّة ومحتوى رقمي يسهم في تبسيط المفاهيم التقنيّة للمستخدمين غير المختصّين في المجال وتعزيز ممارسات السّلامة الرّقمية في الحياة اليوميّة.

كما يُعزّز هذا المجال من خلال شراكات فعّالة مع مكوّنات المجتمع المدني، باعتبارها عنصراً فاعلاً في التّوعية المجتمعيّة وفي الوصول إلى الفئات الهشّة إضافة إلى تشريك القطاع الخاصّ في دعم المبادرات ذات الصّلة وتوفير منصّات آمنة وسهلة الاستخدام وسيلعب الإعلام دوراً محورياً في إيصال الرّسائل التوعويّة وتعزيز السلوكيّات الآمنة وتحفيز النقاش المجتمعي حول القضايا السيبرنية.

تهدف هذه الجهود إلى بناء مجتمع رقمي واعٍ قادر على التفاعل الآمن مع التكنولوجيا ويساهم في حماية الفضاء السيبرني الوطني من التّهديدات المتزايدة والمحافظة على الهوية المجتمعيّة.

5. التّعاون الدّولي والشّراكات

يعنى هذا المجال بتعزيز الدبلوماسية التّونسيّة السيبرنيّة، من خلال تطوير قنوات فعّالة للتّسيق والتّعاون مع المنظّمات والهيئات المختصّة، وتبادل المعلومات الفنيّة ذات الصّلة بالتّهديدات والهجمات السيبرنية، بما يساعد في تحسين القدرة على التنبؤ والاستجابة بشكل أسرع وأكثر تنسيقاً. كما يشمل هذا التّعاون المشاركة النشطة في المبادرات والمنتديات الدّولية المعنيّة بالأمن السيبرني، والامتثال للمعايير والاتفاقيات الدّولية في الخصوص.

ويمتدّ هذا المجال ليشمل بناء شراكات استراتيجيّة مع القطاع الخاصّ، لا سيّما مزودي خدمات التكنولوجيا والبنى التحتيّة الرقميّة، بما يعزّز من فعاليّة الحماية والتّعافي من الهجمات السيبرنيّة. كما يُعدّ التّعاون مع المؤسّسات الأكاديميّة ومراكز البحث والتّطوير عنصراً محورياً لتعزيز الابتكار وبناء القدرات الوطنيّة في هذا المجال.

ويُشجع هذا التوجّه أيضاً على إرساء أطر واضحة للتّعاون الثنائي ومتعدّد الأطراف المؤسّس على قواعد التكافؤ وإحترام خصوصيّات كل دولة وإنشاء آليات لتبادل أفضل الممارسات والدروس المستفادة، والمشاركة في تمارين واختبارات سيبرنيّة مشتركة. وتهدف هذه الجهود إلى دعم السيادة الرقميّة، ورفع مستوى الجاهزيّة الوطنيّة، وتعزيز موقع تونس كشريك فاعل ومؤثر في الأمن السيبرني على الصّعيدين الإقليمي والدّولي.

أهداف الاستراتيجية

تعكس الأهداف الواردة في هذه الاستراتيجية ما تمّ تحقيقه من تقدّم في تنفيذ الاستراتيجية الوطنية للأمن السيبراني 2020-2025 وتلبي في الوقت ذاته متطلّبات المرحلة الحالية وتحدياتها كما تؤكد حرص الدولة على تعزيز حماية الفضاء السيبراني التونسي بما يوفر بنية رقمية موثوقة وأمنة و يتيح للمؤسسات الحكومية والقطاع الخاص والمواطنين الانخراط لدعم التحوّل الرقمي والنمو الاقتصادي وحماية الأسرة والمجتمع. وتمّ ضبط هذه الأهداف بناء على المجالات المحددة والتي من شأنها أن تحقّق الرؤية المزمع العمل على بلوغها.



رسم بياني 2 أهداف الإستراتيجية



1. تطوير الإطار القانوني والتنظيمي

يمثل هذا الهدف أحد الركائز الأساسية في الاستراتيجية الوطنية للأمن السيبراني نظراً لما يتيح من فرص لإحداث إطار قانوني متطور رادع ومرن ووضع إجراءات تنظيمية تواكب التحوّلات وتوفّر الحماية اللازمة لمختلف الفاعلين في الفضاء السيبراني الوطني.

وفي ظلّ التوسّع المستمرّ لهذا الفضاء واعتماد مختلف القطاعات على التكنولوجيات الحديثة أصبح من الضروري أن تواكب المنظومة القانونية الوطنية والإجراءات التنظيمية هذا التحوّل الهامّ بما يضمن ملاءمتها مع التطوّرات التكنولوجية والتّحديات السيبرانية المتجدّدة والأشكال المستحدثة من الجرائم وتشمل الجوانب التالية :

- حماية البنى التحتية الرقمية الحساسة من أي اختراق أو استهداف يهدّد استمرارية الخدمات الحيوية.
- مكافحة الجرائم السيبرانية بمختلف أنواعها.
- ضمان حماية المعطيات الشخصية والمحافظة على الخصوصية للمواطنين في الفضاء الرقمي.
- تعزيز جاهزية الدولة في مواكبة التطوّرات التكنولوجية السريعة والتّفاعل مع التّحديات السيبرانية المستجدة بكفاءة وفاعلية.
- تأمين المعاملات المالية عبر الإنترنت وضمان نزاهتها وسلامتها.
- حماية حقوق الملكية الفكرية والصناعية بما في ذلك براءات الاختراع في البيئة الرقمية.

- التصدي للمخاطر التي تهدد الأطفال ومختلف شرائح المجتمع في الفضاء السيبرني.
- إنشاء آليات وهياكل مختصة من شأنها أن تساهم في إضفاء نجاعة في الأداء وتعزيز التنسيق بين مختلف الأطراف المتداخلة في مجال مكافحة الجرائم السيبرنية.
- توضيح المهام وتحديد المسؤوليات.

ويستوجب تطوير الإطار القانوني والتنظيمي تقييم التشريعات الوطنية الحالية وتحسينها بالإضافة إلى وضع إطار تنظيمي متكامل لحماية البنى التحتية الرقمية الحساسة وتوفير إطار قانوني لتصنيف المعطيات وتمكين الهياكل الوطنية من مرجعية تمكن من التعامل مع المعطيات بطريقة آمنة وموثوقة.

2. حوكمة الأمن السيبرني الوطني

تمثل حوكمة الأمن السيبرني الوطني ركيزة أساسية تقوم عليها الاستراتيجية الوطنية للأمن السيبرني، بما يُرسخ مقومات الحوكمة الرشيدة ويضمن استدامة الجهود الوطنية في حماية الفضاء السيبرني الوطني وتعزيز السيادة الرقمية.

وتهدف هذه الحوكمة إلى تمكين الدولة من تطوير قدراتها في مجالات الوقاية من المخاطر والتصدي للهجمات السيبرنية والتعافي السريع من أثارها بما يضمن حماية المعطيات والمعلومات السيادية والبنى التحتية الرقمية الحساسة.

كما يتم تحقيق الهدف عبر توفير مراجع وطنية مختصة بالأمن السيبرني وإيجاد الآليات لتمويل المشاريع المتعلقة بالأمن السيبرني وإرساء سياسة سلامة حكومية موحدة بالإضافة إلى توفير الجوانب التنظيمية المستوجبة للمتابعة والتنسيق والاستجابة السريعة في حالات الطوارئ السيبرنية ويستند إليها كمرجعية في إدارة الأزمات على المستويين المركزي والقطاعي.



3. حماية البنى التحتية الرقمية الحساسة

تُعدّ حماية البنى التحتية الرقمية الحساسة من أبرز أولويات الأمن السيبراني الوطني نظراً لما تمثّله من أهمية استراتيجية لضمان استمرارية عمل المؤسسات وسير المرافق الحيوية وحماية مصالح الدولة. وتشمل تأمين الأنظمة والشبكات بالإضافة إلى الخدمات الرقمية الحيوية والتطبيقات الوطنية الحساسة التي يُمكن أن يؤدي استهدافها إلى تهديد الأمن القومي أو المساس بالسلامة العامة.

كما يستوجب تحقيق هذا الهدف اتخاذ العديد من الإجراءات التي تشمل آليات لإدارة المخاطر للبنى التحتية الرقمية الحساسة بالإضافة إلى تأهيلها حسب المعايير الدولية للسلامة السيبرانية.

4. تعزيز القدرات الفنية لحماية الفضاء السيبراني الوطني

يعتبر تعزيز القدرات الفنية أحد الأهداف الضرورية لضمان أمن الفضاء السيبراني الوطني لما له من دور محوري في تمكين الدولة من التصدي بفاعلية للتهديدات السيبرانية المتزايدة والمعقدة. ويتحقّق بتطوير وتحديث الأدوات والآليات والتقنيات المعتمدة لرصد الحوادث السيبرانية والتعامل معها بالإضافة إلى تبني أحدث الحلول التكنولوجية في مجال السلامة السيبرانية وتوفير الآليات اللازمة للوقوف على مستوى سلامة الفضاء السيبراني الوطني والمساعدة على استشراف الحلول الناجعة للرفع من مستوى سلامته.



5. تنمية الكفاءات الوطنية في مجال الأمن السيبراني

تمثل تنمية الكفاءات الوطنية في مجال الأمن السيبراني استثمارًا استراتيجيًا يهدف إلى تأهيل وتكوين الإطارات الوطنية على إكتساب المهارات والمعارف اللازمة للرفع من مستوى سلامة النظم المعلوماتية والتعامل بفاعلية مع التهديدات السيبرانية وتحقيق السيادة الرقمية. ويتحقق ذلك من خلال برامج تعليمية متخصصة وتوفير شهادات مهنية معتمدة إلى جانب مبادرات عملية تسهم في بناء خبرات متقدمة في مختلف مجالات الأمن السيبراني. وللحفاظ على الكفاءات المؤهلة في المجال، تستوجب هذه المرحلة التخطيط لتوفير وتحفيز الكفاءات باعتماد الآليات اللازمة.

6. دعم البحث العلمي والتطوير في مجال الأمن السيبراني

يمثل البحث العلمي والتطوير في مجال الأمن السيبراني محورا أساسيًا في بناء منظومة وطنية متقدمة للأمن السيبراني قادرة على مواجهة التهديدات المتجددة والتكيف مع التطورات التكنولوجية المتسارعة. وتكمن أهمية دعم هذا المجال في تعزيز الابتكار المحلي وبناء القدرات الوطنية وتحقيق الاستقلالية التقنية. وتهدف الاستراتيجية الوطنية إلى تحفيز البحث العلمي التطبيقي وتشجيع التعاون بين المؤسسات الأكاديمية ومراكز البحث والقطاعين العام والخاص من أجل تطوير حلول مبتكرة تعزز من أمن الفضاء السيبراني وتدعم تحقيق السيادة الرقمية.



7. حماية الأسرة والمجتمع والمحافظة على هويته

تولي الاستراتيجية الوطنية للأمن السيبرني أهمية خاصة لحماية الأسرة والمجتمع من التهديدات السيبرنية التي قد تؤثر على القيم الثقافية والاجتماعية والهوية الوطنية. ويأتي ذلك من خلال تعزيز الوعي السيبرني وتمكين مكونات المجتمع من الاستخدام الآمن للتكنولوجيا ومكافحة المحتوى الضار المنتشر عبر المنصات الرقمية. كما تسعى الاستراتيجية إلى دعم مبادرات التعليم والتثقيف الإلكتروني التي ترسخ القيم الأخلاقية وتحافظ على الخصوصية الثقافية بما يسهم في بناء مجتمع رقمي آمن ومتوازن يحترم الهوية الوطنية ويعزز الانتماء ويحمي النسيج الاجتماعي من الاختراقات الفكرية والسلوكية.

8. إرساء ثقافة الأمن السيبرني بالهياكل الوطنية

يُعدّ إرساء ثقافة الأمن السيبرني داخل الهياكل الوطنية ركيزة أساسية لتعزيز المنظومة الوقائية والدفاعية الرقمية للدولة حيث يعتمد الأمن السيبرني بشكل كبير على وعي الأفراد والمؤسسات بمخاطر الفضاء الرقمي وسبل الوقاية منه. فالعنصر البشري يظل من أبرز نقاط الضعف في مواجهة التهديدات السيبرنية مما يستوجب تعزيز الوعي وترسيخ الممارسات الآمنة لدى الموظفين على اختلاف مستوياتهم. وتعمل الاستراتيجية الوطنية على دمج مبادئ الأمن السيبرني صلب مختلف الهياكل الوطنية من خلال تطوير برامج توعوية وتدريبية مستمرة وإرساء سياسات داخلية واضحة وتفعيل آليات الإبلاغ عن الحوادث السيبرنية بما يسهم في بناء سلوك رقمي مسؤول داخل الهياكل والمؤسسات الوطنية.



9. تعزيز التعاون الدولي والإقليمي

يشكّل تعزيز التعاون الدولي والإقليمي أحد الركائز الأساسية لدعم قدرات الدولة في مجال الأمن السيبراني في ظلّ التهديدات السيبرانية العابرة للحدود. وتسعى الاستراتيجية الوطنية إلى تدعيم الدبلوماسية السيبرانية التونسية عبر توطيد علاقات الشراكة وتبادل الخبرات مع المنظّمات الدولية والإقليمية بهدف الاستفادة من أفضل الممارسات والمشاركة في المبادرات الجماعية وتعزيز التنسيق في مجالات الاستجابة للحوادث والتكوين وتطوير السياسات. كما تهدف إلى الانخراط الفعّال في المنتديات السيبرانية الدولية والمساهمة في صياغة معايير وتوجّهات تُراعي مصالح وألويّات الأمن السيبراني الوطني بالإضافة إلى إبرام اتفاقيّات تعاون على المستوى الإقليمي والدولي في مجال الأمن السيبراني.

10. دعم الشراكة بين القطاع العام والخاص

تعتبر الشراكة الفاعلة بين القطاع العام والخاص عاملاً جوهرياً في بناء منظومة وطنية فعّالة لحماية الفضاء السيبراني ودعم النمو الاقتصادي. وتهدف الاستراتيجية إلى إرساء آليات وتطوير أطر تعاون مستدامة تتيح تبادل المعلومات والخبرات بين الجهات الحكومية والشركات الخاصة ومنها العاملة في القطاعات الحيوية وهو من شأنه تعزيز الاستثمار والابتكار المحلي في الأمن السيبراني وتكامل الخبرات والموارد. كما تسعى إلى تشجيع الاستثمار في البنية التحتية السيبرانية وتعزيز الابتكار من خلال دعم المبادرات المشتركة في مجالات التكوين والبحث والتطوير والاستجابة للحوادث السيبرانية. تسهم هذه الشراكة في بناء قدرة وطنية متكاملة قادرة على مواجهة التحديات المتزايدة وحماية المصالح الوطنية في الفضاء الرقمي.

أولويات تنفيذ مجالات الاستراتيجية

يرتكز تنفيذ الاستراتيجية الوطنية للأمن السيبراني على أولويات موزعة زمنياً على ثلاث مراحل للفترة 2026-2030 وذلك لضمان تحقيق الأهداف بشكل متكامل وفعال :

- المدى القصير (من سنة إلى سنتين) : تركّز الجهود على تعزيز الإطار التشريعي والتنظيمي وتطوير الهيكلية المؤسسية لحوكمة الأمن السيبراني وإطلاق حملات توعوية وطنية إلى جانب تطوير خطط الاستجابة للحوادث السيبرانية وتكوين لجان وفرق متخصصة والعمل على تنمية الكفاءات الوطنية في مجال.
- المدى المتوسط (من سنتين إلى ثلاث سنوات) : يتمّ التركيز على تطوير البنية التحتية الرقمية الآمنة والموثوق بها ودعم البحث العلمي والابتكار وتكثيف التعاون بين القطاعين العام والخاص مع إدراج الأمن السيبراني في أنظمة التعليم والتكوين المهني.
- المدى الطويل (من ثلاث إلى خمس سنوات) : تسعى الاستراتيجية إلى تحقيق الاستقلالية الرقمية وتعزيز مكانة الدولة على المستوى الإقليمي والدولي في مجال الأمن السيبراني من خلال شراكات متقدمة ومراكز خبرة وطنية وقيادة مبادرات دولية في الفضاء السيبراني.

ويُراعى في تنفيذ هذه الأولويات التقييم الدوري واعتماد مؤشرات أداء واضحة تضمن المرونة في التعديل حسب التطورات التكنولوجية والتهديدات السيبرانية المستجدة.

المتابعة والتقييم

تمثل المتابعة والتقييم عنصراً جوهرياً لضمان فعالية تنفيذ الاستراتيجية الوطنية للأمن السيبراني وتحقيق غاياتها المرحلية والإستراتيجية على المستويات الزمنية القريبة والمتوسطة والبعيدة. وتقوم هذه العملية على آليات دقيقة ومنهجية تسمح برصد مدى التقدم المحرز وتحديد نقاط القوة والضعف واقتراح التعديلات اللازمة في الوقت المناسب لضمان تحقيق النتائج المرجوة.

ولضمان حسن متابعة وتقييم مدى تنفيذ الإستراتيجية الوطنية للأمن السيبراني تمّ تحديد جملة من المؤشرات الكمية والنوعية قابلة للقياس تغطي الجوانب التقنية (مثل رصد الحوادث والتهديدات السيبرانية) والتشريعية والتنظيمية، إضافة إلى مؤشرات خاصة بالتوعية والتكوين والتعاون بين مختلف الأطراف. وقد صيغت بالاستناد إلى الأهداف الاستراتيجية العامة وسيتمّ متابعتها من قبل لجنة فرعية تحت إشراف لجنة أمن الإتصالات والمعلومات. وقد تمّ ربط المؤشرات بنتائج إستراتيجية يتمّ التوصل إليها من خلال احتساب المؤشرات بهدف تحقيق الرؤية. وتتمثل هذه النتائج في :

- تقليص المخاطر
- ترسيخ الثقة الرقمية.
- تعزيز السيادة الرقمية.
- دعم النمو الاقتصادي.
- رفع مدى وعي مكونات المجتمع بالأمن السيبراني.

وتعقد هذه اللجنة اجتماعات تقييم دورية لمراجعة الأداء واقتراح الإجراءات التصحيحية بما يتماشى مع المستجدات.

ولضمان ملاءمة الاستراتيجية مع التطورات المحلية والدولية، ستخضع محاورها لتقييم شامل ومحدث بصفة منتظمة، مدعوم باستبيانات دورية تقيس مستوى رضا المؤسسات والجهات المعنية عن جودة التنفيذ وكفاءته. وستُستثمر نتائج هذه التقييمات في تحسين آليات العمل وتعزيز استدامة الفاعلية على المدى الطويل.