الجمهورية التونسية

رئاسة الجمهورية

مجلس الأمن القومي

# الإستراتيجية الوطنيـــة للأمـــــن السّيبرني

# 2025-2020

# الفـــــهرس

# توطئـــــــــــــــــــة

يشهد العالم تطورا سريعا ومكثفا لاستعمال تكنولوجيات المعلومات والاتصالات في جميع المجالات ومن قبل جميع الفئات، سيما القطاع العام والخاص والمواطن في أغلب مجالات حياته اليومية.

ولئن وفّرت هذه التكنولوجيات بيئة رقمية مترابطة فيما بينها بالمرونة والنّمو السّريع وتحقيق رفاهة لدى المواطن، إلاّ أنّ هذه الميزات لا تخلو من مخاطر تتربص بالفضاء السّيبرني، علاوة على التّهديدات من الداخل والخارج التي تستهدف الحقوق والحريات والأمن القومي.

وقد أفرز هذا التطور التكنولوجي مفاهيم جديدة ومتغيرة، على غرار الحوسبة السحابية وانترنت الأشياء والجيل الخامس للاتصالات وشبكات التواصل الاجتماعي والذكاء الاصطناعي والعملات الافتراضية والبيانات المتسلسلة وغيرها، مع إستعمال وإستغلال مكثّف وموسّع للإنترنت ليشمل مختلف المجالات الحيويّة للفرد والمجتمع والدّولة، مما أدّى إلى إرتفاع منسوب المخاطر والتّهديدات والهجمات السّيبرنية بمختلف أنواعها ومصادرها خاصّة في ظلّ الإنفتاح على المستوى الإقليمي والدّولي.

وعليه، وتبعا لمداولات مجلس الأمن القومي المنعقد في 05 جويلية 2018، تم بعث فريق عمل تابع للجنة أمن المعلومات والاتصالات المنبثقة عن هذا المجلس وتحث إشراف المستشار أوّل للأمن القومي، لإعداد الإستراتيجية الوطنية للأمن السّيبرني التي تهدف إلى حماية الفضاء السّيبرني الوطني وتطويره من خلال بناء القدرات الوطنيّة وضمان الثّقة الرّقمية في تفاعل مع جملة الإستراتيجيات القطاعية والخاصة وتنفيذ الخطط في المجال بالتنسيق مع جميع الأطراف المتداخلة، وذلك في إطار إحترام الحقوق والحرّيات وفق مقتضيات وأحكام الدّستور والإتفاقيات والمعاهدات الدّولية.

تُعنى هذه الإستراتيجية بخمس مجالات وهي التّوجّهات والإستراتيجيّات القطاعية، والإطار القانوني والتّنظيمي، والتّعليم والتّدريب والمهارات، والثقافة والمجتمع السّيبرني، والمعايير والتّقنيات.

# الرؤيـــــــــــــــــة

أن تكون الدّولة التونسية قادرة على التّوقّي من التّهديدات السّيبرنية والصّمود في وجهها بالإعتماد على القدرات الوطنية، وقيادة الفضاء السّيبرني الوطني وإدارته، ودعم الثّقة الرّقمية، وتعزيز التّعاون الدّولي، وتحقيق الرّيادة في المجال الرّقمي.

# نطاق الإستراتيجيـــــــــــة

تغطّي هذه الإستراتيجية الفضاء السّيبرني الوطني المتكوّن خاصّة من جميع الخدمات والبيانات والشّبكات والمنصّات والمنظومات المعلوماتيّة والبُنَى التّحتيّة الرّقميّة الحيويّة المرتبطة بمصالح الدّولة، كما تخصّ هذه الإستراتيجية جميع المتداخلين من مواطنين ومؤسّسات وجمعيّات وشركات بالقطاع العام والخاصّ والمجتمع المدني والوسط الأكاديمي والبحثي.

# أهداف الإستراتيجيـــــــــــة

تهدف هذه الإستراتيجيّة إلى:

1. **قيادة الفضاء السّيبرني الوطني وإدارته،** من خلال تحديد الأطراف المكلّفة بتعزيز العمل المشترك بين كل المتداخلين في المجال ودعم التّنسيق بينها.
2. **التوقّي من التّهديدات السّيبرنية والصّمود،** من خلال تعزيز القدرات الوطنيّة ودعم التّوعية وحماية البُنَى التّحتيّة المعلوماتيّة الحيويّة.
3. **دعم الثّقة الرّقمية،** من خلال وضع الآليات والإجراءات الضرورية للغرض.
4. **تحقيق الرّيادة في المجال الرّقمي،** من خلال تطوير بيئة رقميّة آمنة وتحقيق الأسبقيّة إقليميا ودوليا.
5. **التّعاون الدّولي،** من خلال إرساء مقاربة متوازنة بين التعاون الدولي وضمان المصالح العليا للدّولة.

# مجالات الإستراتيجيـــــــــــــــــــــة

تم إعداد الإستراتيجية الوطنية للأمن السّيبرني بطريقة تشاركية بين جميع الأطراف بالاعتماد على نتائج تحاليل المخاطر التي تهدّد الفضاء السّيبرني الوطني واستعمالاته، وبالرّجوع إلى مرجعيّات عالميّة في المجال.

تُحدّد هذه الإستراتيجيّة جملة من التّوجهات تتعلّق بكافّة مجالات الإقتصاد والمجتمع، وتضمن حين تنفيذها مرونة وصلابة الخدمات والبُنَى التّحتيّة المعلوماتية الحيويّة الوطنيّة بهدف تدعيم الثّقة الرّقمية.

كما تعمل أيضا على تطوير المنظومة القانونيّة للمجال الرّقمي مع إيجاد آليّات تعاون على الصّعيد القطاعي والمحلّي والعالمي لإدارة المخاطر التي تهدد الفضاء السّيبرني، وتوفير الكفاءات والمهارات الوطنيّة.

وترتكز هذه الإستراتيجيّة على المجالات التّالية:

**1. التّوجهات والإستراتيجيّات القطاعيّة:**

إلتزام الأطراف الفاعلة بتدعيم مناعة الفضاء السّيبرني الوطني وحماية البُنَي التحتية المعلوماتيّة الحسّاسة ضدّ المخاطر والتّهديدات التي يمكن أن تمسّ من الأمن القومي، وذلك عبر تطوير إجراءات وآليّات التّعامل والتّفاعل مع الحوادث السّيبرنية وإدارة الأزمات المتعلّقة بالمجال.

**2. الإطار القانوني والتنظيمي:**

تطوير ومُوَاءَمَة النّصوص القانونيّة مع التّطور في المجال الرّقمي، خاصّة تلك المتعلّقة بمجال:

- حرّية التّعبير على الإنترنت،
- حماية الخصوصيّة والمعطيات الشّخصية،
- حماية الأطفال على الإنترنت،
- حماية المستهلك "الرقمي"،
- حماية الملكية الفكرية والصناعية وبراءات الإختراع على الإنترنت،
- حماية المعاملات الماليّة على الإنترنت،
- مكافحة الجرائم السّيبرنية.

3. **التّعليم والتّدريب والمهارات:**

وذلك من خلال:

- توعية الأفراد بالمخاطر السّيبرنية وكيّفيّة مواجهتها،
- إرساء تكوين أكاديمي في المجال الرّقمي يعتمد على مكوّنين متخصّصين بالشراكة مع القطاع الصناعي،
- تطوير كفاءات متخصّصة في مجال سلامة الفضاء السّيبرني.

4. **الثّقافة والمجتمع السّيبرني:**

إرساء ثقافة الأمن السيبرني من خلال توعية الفرد بضرورة الحذر في تعامله مع الخدمات الإلكترونية على الإنترنت ومواقع التّواصل الإجتماعي، والعمل على حماية معطياته المهنيّة والشخصيّة.

5. **المعايير والتّقنيات والبحث العلمي:**

حسن الإستعداد والوقاية من المخاطر والتّهديدات المحتملة بالإعتماد على المعايير الدّولية في المجال، وتحفيز مختلف المتداخلين لتطوير القدرات والحلول الضّرورية للغرض.

# أولويّات تنفيذ المجـــــــــالات

لتنفيذ مجالات هذه الإستراتيجية، سيتمّ إتّباع التمشّي التّالي:

1. **الجانب التنظيمي:**

- التّطوير المستمر للإطار القانوني في مجال السّلامة الرّقميّة،
- المصادقة على الإتّفاقيات والمعاهدات الدّولية في الغرض،
- حوكمة السّلامة الرّقمية وإدارة الأزمات والتّنسيق بين جميع الهياكل المتداخلة،
- الحرص على تطبيق سياسات وقواعد وإجراءات السّلامة الرّقمية.

2. **الجانب البشري:**

- الرّفع من مستوى وعي المستخدمين والمسؤولين بالمخاطر المرتبطة بإستعمالات التّكنولوجيات الحديثة والإنترت،
- توفير الكفاءات المتخصّصة والمحافظة عليها،
- توعية المسؤولين بأهمّية دورهم في حسن إدارة المجال الرّقمي.
- تطوير الطّاقات الوطنيّة في مجال البحث العلمي وتحفيز مختلف المتداخلين لتطوير قدرات وحلول وطنيّة في المجال.

**3. الجانب العمليّاتي:**

- الحرص على إرساء قواعد الحوكمة الرّشيدة للمعطيات،
- إدراج السّلامة الرّقمية ضمن الأولويّات الوطنيّة،
- دعم التّكوين وآليّات التّمويل الخاصّة بتركيز وإستغلال المنظومات الوطنيّة الرّقميّة،
- تعزيز قدرات الدّفاع السّيبرني،
- تركيز آليّات التّنسيق العمليّاتي الرّقمي على المستوى الوطني وتحديد الإختصاص ومجال التّدخل لمجابهة وإدارة الحوادث السّيبرنية.

**4. العوامل المرتبطة بالمحيط:**

- وضع الآليّات اللازمة لقيادة الفضاء السّيبرني الوطني وإدارته،
- أخذ التّدابير اللاّزمة لدعم الثّقة في الفضاء السّيبرني والخدمات الرّقمية،
- تحقيق بنية تحتيّة وخدمات رقميّة تستجيب لمتطلّبات السّلامة حسب المواصفات العالميّة في المجال،
- ضمان الإستقرار الوطني في المجال الإجتماعي والإقتصادي والسّياسي،
- دعم الثّقة في الفضاء السّيبرني.

# المتابعة والتّقييم

في إطار التأكيد على ضمان السّيادة الوطنية والثقة الرّقمية في الفضاء السّيبرني الوطني، تحرص الدّولة التونسيّة على إتّخاذ التّدابير والإجراءات الضّرورية لتنفيذ هذه الإستراتيجية، وإنجاز خطط عمل مفصّلة تتضمّن الإجراءات الواجب إتخاذها مع العمل على تعزيز التّعاون الدّولي في هذا المجال.

وتمتدّ هذه الإستراتيجية على مدى ستّ سنوات ويتمّ تحيينها حسب المتغيّرات.

يتم الاشراف ومتابعة تنفيذ هذه الإستراتيجية واقتراح تحيينها على مجلس الأمن القومي من طرف لجنة أمن الاتصالات والمعلومات المنبثقة عن ذات المجلس.

# قاموس المصطلحات

| | المصطلح | التعريف |
|---|---|---|
| .1 | المعطيات<br>Données/Data | أي تمثيل للمعلومات أو المفاهيم في شكل يمكن قراءتها بأي وسيلة كانت. |
| .2 | الخدمات الرقمية<br>Services numériques/Digital services | كل خدمة يتم إسداؤها إلى شخص طبيعي أو معنوي باستعمال مكوّن أو أكثر من مكوّنات الفضاء السّيبرني. |
| .3 | التوفر<br>Disponibilité/Availability | خاصية استمرارية وديمومة الخدمة و/أو المعطيات |
| .4 | التهديد<br>Menace/Threat | هو إحتمال حدوث حادث يمس من توفر الخدمة المسداة أو من سلامة وسرية وتوفر المعطيات على الفضاء السيبرني |
| .5 | الثغرة<br>Vulnérabilité/Vulnerability | نقطة ضعف أو خلل على مستوى مكون من مكونات الفضاء السيبرني يمكن استغلالها من قبل أشخاص لتهديد أمن الفضاء السيبرني والمس منه. |
| .6 | الخطر<br>Risque/Risk | تأثير استغلال التهديد للثغرات الموجودة باعتبار إجراءات السلامة المتوفرة. |
| .7 | البنى التحتية الرقمية الحيوية<br>Opérateur d'Importance Vitale (OIV)<br>Critical Digital Infrastructure (CDI) | هي الأنظمة المعلوماتية التي تأوي الأصول والخدمات الحساسة على المستوى الوطني، والتي يمكن أن يؤثّر توقفها أو المسّ من سلامتها على سلامة الأمن القومي. |
| .8 | حماية البنى التحتية الرقمية الحيوية<br>Protection des OIV/CDI Protection | توفير الوسائل والإجراءات التنظيمية والفنية لضمان ديمومة الخدمات وسرية وسلامة وتوفر المعطيات الحساسة. |
| .9 | الفضاء السيبرني<br>Espace cybernétique/Cyber space | الفضاء السيبرني هو فضاء رقمي يربط منظومات المعالجة الالكترونية للمعطيات بشبكات المعلومات والاتصال، ويشمل الحواسيب والشبكات والمنصات والمحتوى والعمليات التي تجرى باستعمال هذه الشبكات. |
| 10 | الأمن السيبرني(أمن الفضاء السيبرني)<br>Sécurité cybernétique/Cyber security | الأمن السيبرني هو توفير الإمكانيات الضرورية لحماية الفضاء السيبرني ضد التهديدات التي يمكن أن تمس من سرية وسلامة وتوفر المعطيات والخدمات. |
| 11 | الدفاع السيبرني<br>Cyber défense/Cyber defense | مجموعة الوسائل والإجراءات التنظيمية والفنية والردعية التي تمكن من الحماية ضد/ الحد من تأثير، والمعالجة السريعة للهجمات السيبرنية التي تستهدف البنى التحتية الرّقميّة الحيويّة. |
| 12 | الجريمة السّيبرنية<br>Crime cybernétique/Cyber crime | هي "الجريمة المتعلّقة بتكنولوجيات المعلومات والإتّصال" |
| 13 | حادث سيبرني<br>Incident cybernétique/Cyber incident | حادث غير متوقع يسبب ضررا لمكون أو أكثر من مكونات الفضاء السيبرني |
| 14 | حدث<br>Evènement/Event | اكتشاف نشاط "غير عادي" في الشّبكة أو منظومة المعالجة (ليست كل الأحداث ضارة). |


المصادر

- Norme ISO 27000
- ITU2006 دليل الامن السيبرني للبلدان النامية –
- ملفات تخص البلدان : فرنسا، بريطانيا، كندا، الولايات المتحدة الأمريكية، تشيكيا، ليتوان
- Convention sur la cybercriminalité, Budapest (STE N°185)
- القانون عدد 22 لسنة 2016 حول حق النفاذ للمعلومة
- مخرجات الدراسة لوضع مرجعية وطنية لتصنيف المعطيات العمومية
- مجلة الاتصالات /مشروع المجلة الرقمية