الجمهورية الجزائرية الديمقراطية الشعبية

وكالة أمن الأنظمة المعلوماتية
Information Systems Security Agency

الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية

2029 - 2025

توطئة السيد رئيس الجمهورية

أطلقت بلادنا سياسة طموحة من أجل تعميم استعمال الرقمنة على مستوى إدارتنا، بهدف تسهيل الحياة اليومية للمواطنين ومرافقة انتعاش اقتصادها على أسس صلبة ومستدامة.

مدركون بأن هذه السياسة ستكون دون أدنى شك هدفا رئيسيا لأعداء بلادنا، بات حتميا وضع آليات ملائمة لحمايتها من هذا الاستهداف الخبيث.

وبالارتكاز على هذه الرؤية الاستراتيجية، وضعت بلادنا، بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي سنة 2020، منظومة وطنية لأمن الأنظمة المعلوماتية التي أتاحت إحداث وكالة أمن الأنظمة المعلوماتية. لا يرتكز النموذج المفاهيمي المعتمد على روح التعاون بين قطاعات مختلف الهيئات المشاركة فقط، حيث يجب أن يكون البحث عن المعلومة المفيدة والموثوقة والفعالة مرفقا باستغلالها العملياتي الآني، وإنما يرتكز كذلك على أهمية توجيه كل طاقتنا لوضع مقاربات مبتكرة تتماشى مع الأهداف المرجوة.

لذلك، فإن الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية ليست غاية في حد ذاتها، ولا قيمة لها إن لم يتم تقييمها، قدر الإمكان، لإبقائها في توافق مع التطورات التكنولوجية والأهداف المرجوة.

بإيجاز، إن استباق المواقف، وتحديد النقائص ونقاط الضعف، وفهم الأسباب، ثم التفكير في الإجراءات الممكنة، بغية الرفع من الفعالية، سواء بالنسبة للجانب التنظيمي أو حتى بالنسبة للمنظومة العملياتية، هي بالذات المقاربة المعتمدة من طرف بلادنا للتصدي لمختلف التهديدات السيبرانية المحيطة.

عبد المجيد تبون

الفهرس

1. مقدمة

يتصدر التحول الرقمي للبلاد انشغالات السلطات العليا للبلاد، التي ما تنفك تُذكّر بأهمية وفائدة إدراج تكنولوجيا المعلومات في القطاعات الإدارية والاقتصادية والصناعية وكذا ضمن المجتمع الجزائري برمته.

في هذا الصدد، يولي السيد رئيس الجمهورية اهتماما خاصا بتسريع نسق التحول الرقمي لمؤسسات الدولة وكذا القطاع الاقتصادي، الذي يشكل هدفا استراتيجيا للسياسات العمومية المعمول بها حاليا في جميع المجالات.

بالفعل، يشكل التحول الرقمي أداة أساسية لا غنى عنها للتنمية الاجتماعية والاقتصادية في بلادنا، حيث يوفر تسييرا شفافا وفعالا للممتلكات العامة، وأداء ناجعا للهيئات العمومية، بالإضافة إلى تثمين وحماية التراث المعلوماتي للدولة والتراث الوطني بشكل عام.

ويعتمد تحقيق هدف التحول الرقمي المنشود بالتكفل الفعال بالأنظمة المعلوماتية والبنى التحتية الحساسة، من خلال توفير الظروف ووضع التدابير اللازمة على الأصعدة التشريعية والتنظيمية، والهيكلية، والوظيفية، والتقنية، من أجل بلوغه بما يتوافق مع المتطلبات الشاملة لتأمين الفضاء السيبراني الوطني.

إدراكا لهذا الرهان، قررت السلطات العليا تزويد الدولة بجهاز مناسب فيما يخص أمن الأنظمة المعلوماتية، من خلال وضع منظومة وطنية لأمن الأنظمة المعلوماتية، تتكون من مجلس وطني وكذا وكالة لأمن الأنظمة المعلوماتية، بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 والمتضمن وضع هذه المنظومة.

في الواقع، إن الهدف الرئيسي من هذه المنظومة يكمن في إعداد ووضع الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، من أجل تهيئة بيئة ملائمة لجميع الفاعليين الوطنيين المعنيين بالأمن السيبراني من خلال توفير كل الظروف اللازمة للمساهمة الناجعة في حماية السيادة الرقمية الوطنية والحفاظ عليها.

ترتكز المقاربة المعتمدة في إعداد الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية على إشراك مؤسسات الدولة والهيئات العمومية والخاصة المعنية، وكذا تحليل المشهد الرقمي الوطني وتحديد الصعوبات والوقوف على العراقيل التي يمكن مواجهتها، مع الأخذ بعين الاعتبار تطور التكنولوجيات الرقمية وتصنيف التهديد السيبراني.

تجدر الإشارة أيضا إلى أن الاستراتيجية الوطنية تستند على للنصوص التشريعية والتنظيمية السارية المفعول التي تسير مختلف جوانب الأمن السيبراني والمجالات ذات الصلة، حيث يجب التأكيد على ضرورة تحديثها وتعزيزها بشكل مستمر.

علاوة على ذلك، وبالنظر لتعقيد وحساسية المهام الموكلة للمنظومة الوطنية لأمن الأنظمة المعلوماتية، والتي تعد النقطة المحورية في هذا الشأن، المتعلقة بالأمن والسيادة الوطنيين، فإن أولى الإلزاميات لهذه الاستراتيجية هي التركيز على ضرورة تزويد البلاد بإمكانيات عملياتية تضمن جاهزية المعلومات وسلامتها وسريتها، فضلا عن أمن ومرونة الأنظمة والبنى التحتية الحساسة، وهذا وفقا للأبعاد الثلاثية لتأمين كل من الموارد البشرية، والإجراءات، والتكنولوجيات.

إنه من المنطقي أن الاستراتيجية الوطنية تبرز ضرورة تكوين واستخدام وتثمين وكذا الحفاظ على مورد بشري ذي مؤهلات عالية في المجالات المتقدمة للأمن السيبراني، حيث يمثل هذا المورد، المطلوب بشدة في جميع أنحاء العالم، ميزة أساسية وعامل نجاح رئيسي للدولة.

تندرج هذه الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية، بصفة شاملة، في إطار الرؤية الوطنية المتعلقة برقمنة مؤسسات الدولة والقطاع الاجتماعي والاقتصادي، مع الأخذ بعين الاعتبار التطور المستمر للتكنولوجيات الحديثة للرقمنة، بالإضافة إلى تنامي التهديد السيبراني الذي يمكن أن يشكل خطرا على أمن الأنظمة المعلوماتية الوطنية.

2. الرؤية

تتمثل الرؤية التي تحددها الاستراتيجية الوطنية لأمن أنظمة المعلومات فيما يلي:

«ضمان المرونة السيبرانية الوطنية من خلال تعزيز قدرات الوقاية والكشف والاستجابة للحوادث السيبرانية لدعم التحول الرقمي لبلدنا والحفاظ على السيادة الرقمية الوطنية»

3. أهداف الاستراتيجية

يتمثل الهدف الرئيسي من هذه الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية في مرافقة مؤسسات الدولة والهيئات العمومية والخاصة، من خلال تنفيذ نهج تدريجي وشامل ومحكم فيما يتعلق بأمن ومرونة الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة، خلال السنوات الأربعة (4) القادمة.

فيتعلق الأمر بالتالي ببلوغ أقصى حد من الأداء من حيث الأمن والمرونة السيبرانية للأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة، في كافة القطاعات.

وفي هذا الصدد، يجب تحديد مستويات الحساسية لمختلف القطاعات والأنظمة مع التركيز، بشكل خاص، على تلك التي يمكن أن يكون لتعطيل عملها آثار سلبية كبيرة، سواء على عمل و/أو أمن وسمعة مؤسسات الدولة والهيئات العمومية والخاصة و/أو على رفاهية وأمن السكان بشكل عام، منها المؤسسات الحكومية، والهيئات العمومية الإدارية أو المالية، والأمن العمومي، والطاقة، والصحة، والموارد المائية، والاتصالات، والنقل، وكذا سلاسل إنتاج وتوزيع المنتجات الغذائية الأساسية.

تحدد هذه الاستراتيجية، التي تشكل الإطار المرجعي لعمل مؤسسات الدولة وجميع الأطراف المعنية، الإجراءات التي يجب اتخاذها والتوجهات الواجب اتباعها لتحقيق الأهداف المرجوة حسب أهميتها وأولويتها، وهذا بطريقة تدريجية، شاملة ومحكمة.

تهدف هذه الاستراتيجية إلى تزويد بلدنا، علاوة على الموارد البشرية المؤهلة، والهيكلية، والتنظيمية، والوظيفية ذات الصلة، بقدرات الوقاية والكشف والاستجابة للحوادث السيبرانية، سواء كانت غير مقصودة أو خبيثة، من خلال توفير الوسائل الفعالة.

تحدد هذه الاستراتيجية بشكل ملموس، وفي نهاية المطاف، أهدافا تسمح لبلدنا باكتساب وضمان سيادة في الفضاء السيبراني وباكتساب دراية في هذا المجال المعقد والحساس والذي يتعلق بالأمن الوطني.

تبرز هذه الأهداف الاستراتيجية بشكل خاص مدى تعزيز القدرات التقنية والعملياتية للجزائر من خلال توفير بيئة ملائمة في مجال الأمن السيبراني، قادرة على مواجهة أي تهديد أو تحدٍ في سياق جد حساس يتميز بظهور تكنولوجيات حديثة وتحول رقمي، وهو ما يعد حتمية لا يمكن غض النظر عنها في أي رؤية استشرافية لبلدنا وكذا لتطويره.

تتمثل الأهداف الاستراتيجية لهذه الاستراتيجية فيما يلي:

01 بناء المرونة السيبرانية للأنظمة المعلوماتية الوطنية.

02 العمل على وضع نظام بيئي وطني ملائم في مجال الأمن السيبيراني.

03 إنشاء إطار وطني من أجل تطوير موارد بشرية مؤهلة في الأمن السيبيراني.

04 تعزيز التعاون الدولي في الأمن السبيراني.

4. المبادئ التوجيهية

المبادئ التوجيهية المذكورة أدناه كعناصر مرجعية في الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية:

01 تعزيز السيادة الرقمية الوطنية.

02 مرافقة التحول الرقمي المباشر من طرف الدولة.

03 الحفاظ على المكاسب المحققة.

04 تشجيع العمل التنسيقي الشامل.

05 تثمين تشارك الموارد.

06 تحديد أهداف قابلة للتحقيق في اجالها المحددة وقابلة للقياس.

5. محاور الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية

في إطار تحقيق الأهداف الاستراتيجية المدرجة ضمن هذه الاستراتيجية الوطنية، تتوزع الجهود الواجب بذلها على المحاور الأربعة (4) التالية:

- المحور 1: القدرات التقنية-العملياتية.
- المحور 2: الإطار القانوني والتنظيمي والمعياري.
- المحور 3: التكوين والبحث والتطوير والتحسيس.
- المحور 4: التعاون الوطني والدولي.

1.5. المحور 1 : القدرات التقنية-العملياتية

يرمي تطوير القدرات التقنية-العملياتية في مجال حماية ومرونة الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة إلى تزويد بلدنا بوسائل الوقاية والكشف والاستجابة للحوادث السيبرانية، من خلال السعي إلى تحقيق الأهداف التالية:

1. تدعيم حماية الأنظمة المعلوماتية الوطنية والبنى التحتية الحساسة،
2. تعزيز القدرات التقنية-العملياتية الوطنية للوقاية من الحوادث والكشف عنها والاستجابة لها.

2.5.المحور 2 : الإطار القانوني والتنظيمي والمعياري

نظرا للطبيعة الشاملة لهذا المحور، فإن الأهداف المدرجة فيه تهدف إلى تزويد بلدنا بإطار قانوني، وتنظيمي، ومعياري ملائم، يُمكّنه من تحقيق الرؤية الاستراتيجية السالف وصفها، وبذلك ضمان المرونة السيبرانية الوطنية. الأهداف المدرجة لهذا المحور هي كالتالي:

1. تعزيز الإطار القانوني والتنظيمي،
2. إرساء إطار معياري.

3.5. المحور 3 : التكوين والبحث والتطوير والتحسيس

ترمي الأهداف المدرجة في هذا المحور إلى تزويد العنصر البشري، بصفته الحلقة الأهم في السلسلة الأمنية، بالكفاءات والمعارف الضرورية التي تسمح له بممارسة مهامه في الفضاء السيبراني بطريقة آمنة وفعالة:

1. التوفر على موارد بشرية مؤهلة في مجال الأمن السيبراني،
2. ترقية البحث والتطوير والابتكار في مجال الأمن السيبراني،
3. ترسيخ ثقافة في الأمن السيبراني.

4.5. المحور 4 : التعاون الوطني والدولي

يهدف التعاون على الصعيد الوطني، إلى تحسين وتشارك وسائل العمل وكذا ترقية تبادل المعلومات في جميع الجوانب المتعلقة بالأمن السيبراني، بين القطاعين العام والخاص ووكالة أمن الأنظمة المعلوماتية.

علاوة على ذلك، وعلى الصعيد الدولي، يشكل التعاون في مجال الأمن السيبراني وسيلة لا غنى عنها لبلدنا، من أجل إضفاء التناسق على الأعمال ومجابهة التهديدات السيبرانية بصفة جماعية، من خلال إقامة روابط عملياتية فعالة.

الأهداف الواردة في هذا المحور هي كالتالي:

1. تعزيز وتثمين التعاون والشراكة في مجال الأمن السيبراني بين كل الأطراف المعنية على المستوى الوطني،
2. تأطير التعاون الدولي على المستويين الاستراتيجي والتقني-عملياتي في مجال الأمن السيبراني؛
3. المساهمة بفعالية في عملية إعداد الإطار القانوني والمعياري على المستوى الدولي في مجال الأمن السيبراني.