مرسوم عدد 17 لسنة 2023 مؤرخ في 11 مارس 2023 يتعلق بالسلامة السيبرنية.

إن رئيس الجمهورية،

بعد مداولة مجلس الوزراء،

يصدر المرسوم الآتي نصه.

الباب الأول

أحكام عامة

الفصل الأول ـ يهدف هذا المرسوم إلى تنظيم مجال السلامة السيبرنية وضبط المهام الموكولة للوكالة الوطنية للسلامة السيبرنية والآليات المخولة لها لضمان سلامة الفضاء السيبرني الوطني في إطار مشمولاتها.

الفصل 2 ـ تستثنى من تطبيق أحكام هذا المرسوم الأنظمة المعلوماتية والأجهزة الإلكترونية التي يتم عن طريقها معالجة معطيات تتعلق بالأمن العام أو الدفاع الوطني والتي فيها مساس بالأمن القومي والمصلحة العليا للبلاد.

وتضبط قائمة الهياكل التي تستغل الأنظمة المعلوماتية والأجهزة الإلكترونية المعنية بالاستثناء الوارد بالفقرة الأولى من هذا الفصل بمقتضى أمر.

الفصل 3 ـ يقصد على معنى هذا المرسوم بـ:

ـ **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 تجرى باستعمال هذه العناصر.

ـ **شبكة إعلامية:** أنظمة تقوم بربط جهازين أو أكثر معا وذلك من أجل تبادل المعلومات باستخدام تقنيات نظم الاتصالات وأيضا من أجل مشاركة الموارد والبيانات المتاحة بينها.

ـ **شبكة الاتصالات:** مجموعة من الأجهزة المتّصلة ببعضها البعض من خلال وسائط اتصال سلكيّة أو لاسلكيّة تمكنها من تأمين الاتصالات باعتماد بروتوكولات متوافق عليها.

ـ البنى التحتية الرقمية الحيوية: الأنظمة المعلوماتية التي تأوي الأصول والخدمات الحساسة على المستوى الوطني والتي يمكن أن يؤثر توقفها أو المس من سلامتها على الأمن القومي.

ـ السلامة السيبرنية: مختلف التدابير والآليات التقنية وغير التقنية التي يقع تركيزها بغرض حماية الفضاء السيبرني وتعزيز القدرة على الاستباقية والتوقي من المخاطر السيبرنية والتفطن السريع للحوادث والهجمات السيبرنية والقدرة على الاستجابة في حالات الطوارئ بهدف الحد من التداعيات وضمان استمرارية النشاط عند حدوث الأزمات السيبرنية.

ـ الأزمة السيبرنية: هي حالة اضطراب بسبب حادث سيبرني أضر بشكل متواصل بمكون أو أكثر من مكونات الفضاء السيبرني وأدى إلى تعطيل استمرارية الخدمات.

ـ نظام معلوماتي: مجموعة موارد مادية ولا مادية وبرمجيّات وأدوات وأجهزة منعزلة أو متصّلة ببعضها البعض تمكن من التصرف في المعلومات ومن تأمين عمليات تجميع وتخزين ومعالجة وإرسال ونشر البيانات.

ـ الثغرة: نقطة ضعف أو خلل على مستوى مكون من مكونات الفضاء السيبرني تجعله عرضة للحوادث أو الهجمات السيبرنية.

ـ هجمة سيبرنية: هي جملة الإجراءات التقنية المتعمدة وغير المرخص لها التي تستغل الثغرات وتسبب ضررا بهدف اختراق، أو تعطيل، أو إضعاف، أو التشويش على عمل الأجهزة ونظم الشبكات والمعلومات أو بهدف الاستحواذ على البيانات أو تغيرها أو إتلافها.

ـ حادث سيبرني: هو فعل أو مشكل عرضي أو مفتعل يسبب ضررا ماديا أو لا ماديا لمكون أو أكثر من مكونات الفضاء السيبرني.

ـ التهديد السيبرني: هو مجموعة العوامل الخارجية أو الداخلية، العرضية أو المفتعلة التي من شأنها المساس أو الإضرار بمكون أو أكثر من مكونات الفضاء السيبرني.

ـ المخاطر السيبرنيّة: هي احتمال تجاوز التهديد السيبرني العرضي أو المفتعل لآليات السلامة السيبرنية عبر استغلال الثغرات الموجودة بمكون أو أكثر من مكونات الفضاء السيبرني مع إمكانية إحداث ضرر.

ـ علامة "مؤمن": هي نتيجة عملية إشهاد يتم بمقتضاها تصنيف البرمجية أو الجهاز الإلكتروني بعد التثبت من مطابقته لمجموعة من معايير السلامة الفنية.

ـ السحابة: مركز بيانات يتم الوصول إليه عن طريق شبكات الاتصال.

ـ الحوسبة السحابية: نموذج نقل الموارد ونقل معالجة وتخزين البيانات إلى السحابة وآليات تمكين المستخدم منها عبر شبكة الاتصالات.

ـ مسدي خدمات الحوسبة السحابية الحكومي: مزود خدمات حوسبة سحابية مختص في إيواء المنظومات والمنصات الإلكترونية والبنى التحتية الرقمية الحكومية، يكون مرتبطا وجوبا بالشبكة الوطنية الإدارية المندمجة وبمنصة الترابط البيني الوطنية.

ـ الشبكة الوطنية الإدارية المندمجة: شبكة إعلامية خاصة تؤمن خدمات مندمجة ومتكونة من مجموعة مواقع إدارية تمكن من تبادل المعطيات بين الموزعات والحواسيب المرتبطة بها عبر بروتوكولات موحدة وترقيم خاص بها.

ـ مسدي خدمات الحوسبة السحابية الوطني: مزود خدمات حوسبة سحابية مختص في ايواء المنظومات والمنصات الإلكترونية والبنى التحتية الرقمية الوطنية.

الباب الثاني

في الوكالة الوطنية للسلامة السيبرنية

الفصل 4 ـ تحدث مؤسسة عمومية لا تكتسي صبغة إدارية تتمتع بالشخصية المعنوية وبالاستقلال المالي يطلق عليها اسم "الوكالة الوطنية للسلامة السيبرنية" وتخضع في علاقاتها مع الغير إلى التشريع التجاري ويكون مقرها بتونس العاصمة ويشار إليها فيما يلي بـ "الوكالة".

تخضع الوكالة لإشراف الوزارة المكلفة بتكنولوجيات الاتصال.

يضبط التنظيم الإداري والمالي وطرق سير الوكالة بمقتضى أمر.

الفصل 5 ـ تكلف الوكالة بالتنسيق مع مختلف الهياكل المتدخلة في المجال بالقيام بمراقبة سلامة النظم المعلوماتية والاتصال للهياكل العمومية والخاصة بالفضاء السيبرني الوطني، وتضطلع أساسا بالمهام التالية:

ـ وضع وتحيين سياسات وآليات حوكمة وسلامة الفضاء السيبرني الوطني وتعميمها على القطاعات والهياكل المعنية.

ـ متابعة تطبيق المخططات التنفيذية لسلامة الفضاء السيبرني الوطني المتعلقة بـــ:

- الإجراءات الاستباقية لتفادي التهديدات المفتعلة والعرضية على الفضاء السيبرني الوطني.
- التدابير الوقائية للحماية من المخاطر السيبرنية.
- آليات التفطن والإبلاغ الحيني عن الحوادث والهجمات السيبرنية.
- الاستجابة الاستعجالية في حالات الطوارئ للتصدي للهجمات السيبرنية والحد من تداعياتها.

• التعافي السريع من آثار الحوادث والهجمات السيبرنية لضمان استمرارية النشاط.

• الاستقصاء والتحري الرقمي لتشخيص الحوادث وتحديد المسؤوليات ذات الصلة بالسلامة السيبرنية.

- إعداد ومتابعة تطبيق برامج تطوير الكفاءات في مجال السلامة السيبرنية من خلال:

• المشاركة في إعداد البرامج الأكاديمية والمهنية المختصة في مجال السلامة السيبرنية.

• المصادقة على برامج التكوين في مجال السلامة السيبرنية ونشرها بموقع الواب الرسمي للوكالة.

• تنظيم دورات تكوينية مختصة في مجال السلامة السيبرنية.

- إعداد ونشر المرجعيات والنماذج والأدلة المتعلقة بالسلامة السيبرنية والتي يجب على الهياكل العمومية والخاصة اعتمادها.

- إعداد مؤشرات قيس المستوى الوطني للسلامة السيبرنية وإصدار لوائح القيادة بشكل دوري.

- القيام بحملات اتصالية وتحسيسية دورية في مجال السلامة السيبرنية خاصة خلال الأزمات السيبرنية.

- تأمين اليقظة التكنولوجية ومواكبة التطورات في مجال السلامة السيبرنية.

- التعاون الدولي والتنسيق مع الجهات الخارجية الرسمية المختصة وفقا للاتفاقيات المبرمة في الغرض على الصعيد الثنائي والإقليمي والدولي.

- وبصفة عامة كل نشاط آخر يقع تكليفها به من قبل سلطة الإشراف وله علاقة بميدان تدخلها.

الباب الثالث

في التدقيق الإجباري لسلامة النظم المعلوماتية

الفصل 6 - تخضع لنظام تدقيق إجباري ودوري النظم المعلوماتية والشبكات الراجعة بالنظر إلى الهياكل العمومية وهياكل القطاع الخاص التالية:

- مشغلي الشبكات العمومية للاتصالات ومزودي خدمات الاتصالات والأنترنات.

- الهياكل ذات الشبكات الإعلامية المرتبطة فيما بينها عبر شبكات الاتصال.

- مسدي خدمات الإيواء والحوسبة السحابية.

- الهياكل التي تتولى المعالجة الآلية للمعطيات الشخصية للمتعاملين معها في إطار توفير خدماتها عبر شبكات الاتصالات.

- البنى التحتية الرقمية الحيوية.

تضبط المعايير الفنية للتدقيق وإجراءات متابعة تطبيق التوصيات الواردة في تقرير التدقيق بقرار من الوزير المكلف بتكنولوجيات الاتصال.

الفصل 7 - تنجز عملية التدقيق الإجباري في سلامة النظم المعلوماتية من طرف الخبراء الممارسين لنشاطهم طبقا للتشريع الجاري به العمل بصفة دورية مرة على الأقل كل اثني عشر (12) شهرا.

تتولى الوكالة نشر وتحيين قائمة الخبراء والهياكل المخول لهم ممارسة نشاط التدقيق في مجال السلامة السيبرنية.

الفصل 8 - على الهياكل الخاضعة لتدقيق سلامة النظم المعلوماتية تسليم نسخة إلكترونية محمية من تقرير التدقيق للوكالة في أجل لا يتعدى عشرة (10) أيام من نهاية عمليات التدقيق.

يتعين على الهياكل المشار إليها بالفقرة الأولى من هذا الفصل تطبيق جميع توصيات السلامة المدرجة بالتقرير.

الفصل 9 - يحجر على أعوان الوكالة وعلى الخبراء المكلفين بأعمال التدقيق، إفشاء أي معلومات أمكن لهم الاطلاع عليها بمناسبة قيامهم بالمهام الموكولة إليهم.

تسلط العقوبات المقررة بالفصل 254 من المجلة الجنائية على كل من يفشي هذه المعلومات أو يشارك في إفشائها أو يحث على ذلك.

الباب الرابع

في سلامة البرمجيات والأجهزة الالكترونية

الفصل 10 - تسند الوكالة بناء على طلب من المطوّر أو المستورد علامة "مؤمن" لكل برمجية أو جهاز إلكتروني.

يكون طلب العلامة بصفة اختيارية وبناء على تقرير تدقيق سلامة مفصل مقدّم من قبل خبراء التدقيق الممارسين لنشاطهم طبقا للتشريع الجاري به العمل.

الفصل 11 - تجدد علامة "مؤمن" المسندة للبرمجية أو للجهاز الإلكتروني كل ثلاث (3) سنوات ويمكن سحبها قبل انتهاء مدة الصلاحية في حالة تعديل المميزّات التقنية أو حدوث تغيير تكنولوجي يدرج ثغرات بالبرمجية أو بالجهاز الإلكتروني.

تضبط إجراءات وشروط إسناد علامة "مؤمن" وسحبها بمقتضى قرار من الوزير المكلف بـتكنولوجيات الاتصال.

تتولى الوكالة مسك ونشر سجل وطني للبرمجيات والأجهزة الإلكترونية المتحصلة على علامة "مؤمن" ويتم تحيينه بصفة دورية.

الباب الخامس

في تصنيف مزودي خدمات الحوسبة السحابية والإيواء

الفصل 12 ـ تتولى الوكالة إسناد وتجديد وسحب علامة "مسدي خدمات الحوسبة السحابية الحكومي" وعلامة "مسدي خدمات الحوسبة السحابية الوطني" لمزودي خدمات الإيواء بعد أخذ رأي وزارتي الدفاع الوطني والداخلية.

تضبط إجراءات وشروط إسناد وتجديد وسحب علامة "مسدي خدمات الحوسبة السحابية الحكومي" وعلامة "مسدي خدمات الحوسبة السحابية الوطني" وفق قرار من الوزير المكلف بتكنولوجيات الاتصال.

تتولى الوكالة نشر وتحيين قائمة مزوّدي خدمات الحوسبة السحابية المتحصلين على العلامة.

الفصل 13 ـ تجدد علامة "مسدي خدمات الحوسبة السحابية الحكومي" وعلامة "مسدي خدمات الحوسبة السحابية الوطني" سنويا.

يمكن سحب العلامة المسندة قبل انتهاء مدة الصلاحية في صورة الإخلال بشرط من الشروط الفنية المنصوص عليها بالقرار المشار إليه بالفصل 12 من هذا المرسوم.

الفصل 14 ـ يتعين على الهياكل المشار إليها بالفصل 6 من هذا المرسوم إيواء المنظومات والخدمات الإلكترونية الحكومية لدى مسدي خدمات الحوسبة المتحصلين على العلامة وفق الشروط الفنية المنصوص عليها بالقرار المشار إليه بالفصل 12 من هذا المرسوم.

الباب السادس

في التصنيف حسب مستوى السلامة

الفصل 15 ـ تخضع الهياكل المشار إليها بالفصل 6 من هذا المرسوم لنظام تصنيف إجباري ودوري.

تتولى الوكالة تصنيف الهياكل المعنية وفق مستوى الثقة الرقمية إلى ثلاث (3) مستويات كما يلي:

ـ مستوى أول: هيكل مصنف درجة أولى.

ـ مستوى ثان: هيكل مصنف درجة ثانية.

ـ مستوى ثالث: هيكل غير مصنف.

يتم تحديد مستويات التصنيف بالاعتماد على المعايير التالية:

ـ التزام الهيكل بالتدقيق الإجباري لسلامة النظم المعلوماتية ومدى تطبيقه للتوصيات المنبثقة عنه.

ـ استعمال الهيكل لتجهيزات وحلول مصادق عليها طبقا للتشريع الجاري به العمل.

ـ إيواء الهيكل لمنظوماته لدى مسدي خدمات إيواء مصنف طبقا لمقتضيات الفصل 8 من هذا المرسوم.

تضبط إجراءات وآليات تصنيف الهياكل المشار إليها بالفصل 6 من هذا المرسوم ونشرها بمقتضى قرار من الوزير المكلف بتكنولوجيات الاتصال.

الفصل 16 ـ يقوم الوزير المكلف بتكنولوجيات الاتصال وباقتراح من الوكالة بتوجيه تنبيه للهياكل المصنفة بالمستوى الثالث للالتزام بالمعايير المعتمدة في التصنيف في أجل لا يتجاوز سنة.

الفصل 17 ـ عند تعرض احدى الهياكل المذكورة بالفصل 6 من هذا المرسوم إلى حادث أو هجمة سيبرنية تسببت في عرقلة استغلال نظام معلوماتي أو شبكة اتصالات أو شكلت خطرا على سلامة الفضاء السيبرني الوطني تتولى الوكالة التنبيه على الهيكل المعني لرفع الإخلالات في أجل لا يتجاوز ثلاثين (30) يوما.

يمكن للوزير المكلف بتكنولوجيات الاتصال في الصورة المشار إليها بالفقرة الأولى من هذا الفصل اتخاذ قرار بعزل النظم المعلوماتية والشبكات بصفة وقتية بغاية حماية الفضاء السيبرني وذلك بمقتضى مقرر بناء على تقرير معلل من الوكالة.

الباب السابع

في الاستجابة للطوارئ السيبرنية

الفصل 18 ـ تتولى الوكالة في إطار الاستجابة للطوارئ السيبرنية القيام بالمهام التالية:

ـ وضع وتطبيق الخطة الوطنية للاستجابة للطوارئ السيبرنية بالتنسيق مع مراكز الاستجابة للطوارئ السيبرنية القطاعية العمومية والخاصة.

ـ تركيز الآليات التقنية اللازمة للتفطن السريع للحوادث والهجمات السيبرنية التي تهدد الفضاء السيبرني الوطني.

ـ تركيز واستغلال قنوات الإبلاغ عن الحوادث والهجمات السيبرنية.

ـ الحد من تداعيات الحوادث والهجمات السيبرنية وضمان استمرارية النشاط والتعافي السريع من آثارها.

ـ إنذار المؤسسات والإدارات والأفراد وتحصين الأنظمة المعلوماتية ومعالجة الحوادث وتنظيم وتنسيق جهود معالجة نقاط الضعف ودراستها وتحليلها وإيجاد الحلول الملائمة لها.

ـ تعيين نقطة اتصال وطنية للاستجابة للطوارئ السيبرنية تتولى التنسيق مع مراكز الاستجابة للطوارئ السيبرنية العمومية أو القطاعية أو الخاصة المشار إليها بالفصل 19 من هذا المرسوم.

الفصل 19 ـ يتعين على الهياكل المذكورة بالفصل 6 من هذا المرسوم إحداث مراكز استجابة للطوارئ خاصة بها أو الانخراط في مراكز الاستجابة للطوارئ السيبرنية العمومية أو القطاعية أو الخاصة.

يتعين على مراكز الاستجابة للطوارئ السيبرنية التنسيق وجوبا مع نقطة الاتصال المشار إليها بالمطة الأخيرة من الفصل 18 من هذا المرسوم.

الفصل 20 ـ تتولى الهياكل المذكورة بالفصل 6 من هذا المرسوم فورا إبلاغ نقطة الاتصال الوطنية للاستجابة للطوارئ السيبرنية أو مركز الاستجابة للطوارئ السيبرنية بالحوادث والهجمات السيبرنية ويتعين عليها الامتثال للتدابير الاستعجالية المقررة من قبلها.

الباب الثامن

في الأحكام الخاصة بالبنى التحتية الرقمية الحيوية

الفصل 21 ـ يتم ضبط قائمة الهياكل التي تدير بنى تحتية رقمية حيوية بمقتضى أمر.

الفصل 22 ـ يتعين على الهياكل التي تدير بنى تحتية رقمية حيوية اتخاذ إجراءات السلامة التالية:

ـ استعمال برمجيات وأجهزة الكترونية متحصلة على علامة "مؤمّن".

ـ اعتماد مركز إيواء رئيسي خاص بها ومركز إيواء احتياطي لدى مسدي خدمات حوسبة سحابية متحصل على علامة.

ـ التقيد بالتدابير والإجراءات الضرورية لضمان استمرارية النشاط ولحماية قواعد البيانات الحساسة التي يمكن أن يؤثر المس من سلامتها على الأمن القومي عند الأزمات السيبرنية وذلك وفق دليل إجراءات تتم المصادقة عليه بمقتضى أمر باقتراح من الوزير المكلف بتكنولوجيات الاتصال.

الباب التاسع

في المخالفات والعقوبات

القسم الأول

في معاينة المخالفات

الفصل 23 ـ تتم معاينة مخالفة أحكام هذا المرسوم بناء على تقرير من الوكالة موجه للوزير المكلف بتكنولوجيات الاتصال بمقتضى محاضر يحررها اثنان من الأعوان الآتي ذكرهم:

ـ مأمورو الضابطة العدلية المشار إليهم بالعددين 3 و4 من الفصل 10 من مجلة الإجراءات الجزائية.

ـ الأعوان المحلفون للوزارة المكلفة بتكنولوجيات الاتصال.

ـ الأعوان المحلفون لوزارة الداخلية.

تحال المحاضر إلى الوزير المكلف بتكنولوجيات الاتصال الذي يحيلها إلى وكيل الجمهورية المختص ترابيا للتتبع.

القسم الثاني

في العقوبات الإدارية

الفصل 24 ـ يمكن للوزير المكلف بتكنولوجيات الاتصال بناء على تقرير معلل من الوكالة الحط من تصنيف الهياكل المذكورة بالفصل 6 من هذا المرسوم والمصنفة بالمستويين الأول والثاني وذلك في الحالات التالية:

ـ عدم القيام بالتدقيق الإجباري والدوري لسلامة النظم المعلوماتية.

ـ عدم تسليم نسخة إلكترونية محمية من تقرير التدقيق للوكالة في الأجل المذكور بالفصل 8 من هذا المرسوم.

ـ عدم تطبيق التوصيات المنبثقة عن تقرير التدقيق أو تطبيقها بصفة جزئية في أجل لا يتجاوز السنة.

ـ عدم الامتثال للتدابير الاستعجالية المقررة من قبل نقطة الاتصال الوطنية للاستجابة للطوارئ السيبرنية أو مركز الاستجابة للطوارئ السيبرنية على إثر وقوع حادث أو هجمة سيبرنية.

ـ عدم رفع الإخلالات في الأجل المذكور بالفصل 17 من هذا المرسوم.

ـ عدم إحداث مركز استجابة للطوارئ السيبرنية أو عدم الانخراط في مراكز الاستجابة للطوارئ السيبرنية.

ـ عدم التقيد بالدليل المرجعي المشار إليه بالفصل 14 من هذا المرسوم.

القسم الثالث

في العقوبات المالية

الفصل 25 ـ يعاقب بخطية من خمسين ألف دينار إلى مائة ألف دينار الهياكل المذكورة بالفصل 6 من هذا المرسوم والمصنفة بالمستوى الثالث وذلك في الحالات التالية:

ـ عدم القيام بالتدقيق الإجباري والدوري لسلامة النظم المعلوماتية.

ـ عدم تطبيق التوصيات المنبثقة عن تقرير التدقيق أو تطبيقها بصفة جزئية في أجل لا يتعدى السنة.

ـ عدم الامتثال للتدابير الاستعجالية المقررة من قبل نقطة الاتصال الوطنية للاستجابة للطوارئ السيبرنية أو مركز الاستجابة للطوارئ السيبرنية على إثر وقوع حادث أو هجمة سيبرنية.

ـ عدم رفع الإخلالات في الأجل المذكور بالفصل 17 من هذا المرسوم.

ـ عدم إحداث مركز استجابة للطوارئ السيبرنية أو الانخراط في مراكز الاستجابة للطوارئ السيبرنية.

الباب العاشر

أحكام ختامية

الفصل 26 ـ يتم ضبط قواعد إبرام وتنفيذ ومراقبة الصفقات والاستشارات المرتبطة بخصوصية مهام الوكالة بأمر.

الفصل 27 ـ تحل الوكالة المحدثة بالفصل 4 من هذا المرسوم محل الوكالة الوطنية للسلامة المعلوماتية المحدثة بالفصل 2 من القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية. وتحال إليها جميع ممتلكاتها وحقوقها والتزاماتها.

وفي صورة حل الوكالة ترجع ممتلكاتها إلى الدولة التي تتولى تنفيذ التزاماتها وتعهداتها طبقا للتشريع الجاري به العمل.

الفصل 28 ـ تلغى بداية من تاريخ دخول هذا المرسوم حيز النفاذ جميع الأحكام المخالفة له وخاصة منها أحكام القانون عدد 5 لسنة 2004 المؤرخ في 3 فيفري 2004 المتعلق بالسلامة المعلوماتية.

الفصل 29 ـ تعوض عبارة "الوكالة الوطنية للسلامة المعلوماتية" أينما وردت في النصوص التشريعية والترتيبية بعبارة "الوكالة الوطنية للسلامة السيبرنية".

الفصل 30 ـ تدخل أحكام هذا المرسوم حيّز النفاذ بعد ستة أشهر من تاريخ نشره بالرائد الرسمي للجمهورية التونسية.

الفصل 31 ـ ينشر هذا المرسوم بالرائد الرسمي للجمهورية التونسية.

تونس في 11 مارس 2023.

رئيس الجمهورية
قيس سعيّد