ESTÁNDAR N°1

OBLIGACIÓN DE AUTENTICACIÓN MULTIFACTOR Y OTRAS MEDIDAS DE PREVENCIÓN DE INCIDENTES DE CIBERSEGURIDAD PARA LOS SERVICIOS ESENCIALES Y OPERADORES DE IMPORTANCIA VITAL SEÑALADOS EN EL ARTÍCULO 4° DE LA LEY N°21.663.

FECHA: **19 DE NOVIEMBRE DE 2026**

VISTO:

Lo dispuesto en la ley N°21.663, Marco de Ciberseguridad;

CONSIDERANDO:

1. Que, la ley N°21.663, Marco de Ciberseguridad (en adelante, "la ley"), tiene como objeto establecer la institucionalidad, los principios y la normativa general que permitan estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares, así como establecer los requisitos mínimos para la prevención, contención, resolución y respuesta a incidentes de ciberseguridad.

2. Que, en conformidad a lo dispuesto en el artículo 11 letra b) de la ley N°21.663, le corresponde a la Agencia Nacional de Ciberseguridad (en adelante "ANCI" o "la Agencia") dictar los protocolos y estándares que señala el artículo 7° del mismo cuerpo normativo.

3. Que, el artículo 7° de la ley N°21.663 establece que las instituciones obligadas por dicho cuerpo legal deberán aplicar, de manera permanente, medidas destinadas a prevenir, reportar y resolver incidentes de ciberseguridad, las que podrán ser de naturaleza tecnológica, organizacional, física o informativa, según corresponda. Asimismo, el referido artículo señala que el cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia.

BORRADOR

4. Que el objeto de dichos protocolos y estándares es la prevención y gestión de los riesgos asociados a la ciberseguridad, así como la contención y mitigación del impacto que los incidentes puedan tener sobre la continuidad operacional del servicio prestado o la confidencialidad y la integridad de la información o de las redes o sistemas informáticos, de conformidad con lo prescrito en la ley.

5. Que, adicionalmente, la norma contenida en el inciso tercero del artículo 7° de la ley N°21.663 dispone que, para efectos de emitir las medidas de seguridad, la Agencia deberá someter dichos protocolos y estándares a consulta pública, en la misma forma y plazo que los señalados para la calificación de operadores de importancia vital.

6. Que, con fecha 30 de mayo de 2026, se publicó en el Diario Oficial la resolución exenta N°140 de la Agencia Nacional de Ciberseguridad, de 27 de mayo de 2026, que aprueba y da inicio a la consulta pública de la normativa que establece estándares básicos obligatorios de ciberseguridad.

7. Que, el proceso de consulta pública se extendió por treinta días con la finalidad de recoger, ordenar y examinar las observaciones formuladas por personas naturales y jurídicas respecto de la normativa que establece estándares básicos obligatorios de ciberseguridad, publicada por la ANCI. El resumen ejecutivo de dicha consulta fue publicado el 20 de agosto de 2026 y se encuentra disponible en el sitio web institucional de la Agencia.

8. Que, al menos un 55% de los incidentes de efecto significativo reportados a la Agencia desde marzo de 2025 a la fecha corresponde a un acceso no autorizado mediante uso de credenciales válidas obtenidas a través de técnicas como phishing, *infostealers* o fuerza bruta, entre otros; lo que evidencia la necesidad de fortalecer los mecanismos de autenticación para prevenir accesos no autorizados.

BORRADOR

9. Que, en este sentido, la autenticación multifactor constituye una medida ampliamente reconocida por su eficacia y costo relativo para prevenir el uso no autorizado de cuentas y los incidentes derivados de él.

10. Que, si bien el uso de un segundo factor de autenticación de distinta naturaleza al primario mejora considerablemente la seguridad en comparación con el uso exclusivo de contraseñas, no todos los métodos de autenticación multifactor ofrecen el mismo nivel de protección. En particular, algunos presentan mayores vulnerabilidades por depender de infraestructuras o canales de comunicación que pueden ser comprometidos, como los mensajes de texto (SMS), o de canales que no garantizan por sí mismos la confidencialidad de las comunicaciones, como el correo electrónico.

11. Que, algunas soluciones de software como servicio o equipos con funcionalidades de acceso remoto comercializadas tienen como práctica el cobro separado de funcionalidades básicas de ciberseguridad, tales como registros de acceso, integración con proveedores de identidad centralizados o autenticación multifactor, por lo que resulta necesario que la Agencia establezca medidas alternativas de carácter transitorio para aquellas instituciones que acrediten no estar en condiciones de implementarla dentro de los plazos establecidos.

12. Que, durante el proceso de consulta pública se formularon observaciones relativas al ámbito de aplicación y a las condiciones de implementación de las medidas de MFA, las que fueron consideradas en la elaboración del presente estándar. En particular, se precisó que sus disposiciones resultan aplicables a las cuentas de usuario final, excluyendo aquellas destinadas exclusivamente a comunicaciones automatizadas entre sistemas, aplicaciones o dispositivos (máquina a máquina), que no requieren la intervención de una persona para su autenticación

13. Que, habida consideración de lo anterior resulta necesario establecer medidas de aplicación general para la prevención de incidentes de ciberseguridad y de fácil adopción por las entidades reguladas.

BORRADOR

14. Que, en mérito de lo anterior, se dicta el siguiente estándar obligatorio de ciberseguridad:

Artículo primero. Definiciones. Para los efectos del presente estándar, se entenderá por:

a) **Mecanismo de autenticación multifactor** (en adelante, "MFA"): método de autenticación que exige la utilización de dos o más factores de categorías distintas para verificar la identidad de un usuario, correspondientes a: algo que el usuario sabe (por ejemplo, una contraseña o PIN), algo que el usuario posee (por ejemplo, un token físico, una tarjeta inteligente o un dispositivo que recibe o genera códigos) y algo que el usuario es (por ejemplo, una característica biométrica).

   La combinación de dos instancias pertenecientes a una misma categoría, como una contraseña y una pregunta de seguridad, no constituye autenticación multifactor.

   Los procedimientos de autenticación podrán comprender, entre otros, contraseñas de un solo uso basadas en tiempo (TOTP), llaves de seguridad y credenciales criptográficas, incluidas las passkeys, siempre que su implementación permita verificar la identidad del usuario mediante factores de categorías distintas.

   Los mecanismos de recuperación, restablecimiento o desactivación del MFA deberán incorporar medidas de seguridad que impidan eludir la protección multifactor mediante la sola utilización del factor primario.

b) **Cuenta con privilegios administrativos:** cuenta de usuario que permite instalar o desinstalar software, modificar configuraciones de sistemas o aplicaciones, gestionar cuentas o credenciales de otros usuarios, o acceder sin restricciones a la información contenida en un sistema.

c) **Sistema expuesto a Internet:** todo sistema informático, aplicación o servicio accesible directamente desde redes públicas, incluso si existe bloqueo de acceso por ubicación geográfica estimada de las IP de origen (*geofencing*).

BORRADOR

d) **Sistemas SCADA (Supervisory Control and Data Acquisition):** arquitectura de sistemas de control que considera interfaces gráficas y equipos y redes informáticas, cuyo objetivo es facilitar el monitoreo y administración de procesos y máquinas.

e) **Sistemas SRA (Secure Remote Access):** aplicaciones que actúan de intermediarios entre Internet y los sistemas de control industrial o de tecnologías operacionales.

f) **Sujetos obligados:** todas las instituciones públicas y privadas señaladas en el artículo 4° de la ley N°21.663.

g) **Tecnologías de Información** (en adelante, "TI"): equipamiento, Sistema o subsistema interconectado que es usado para la recolección automática, el almacenamiento, la manipulación, el movimiento, el control, el despliegue, el intercambio, la transmisión o la recepción de datos o información.

h) **Tecnologías Operacionales** (en adelante, "TO"): sistemas o dispositivos programables que interactúan con el entorno físico, o que administran dispositivos que interactúan con el entorno físico, detectando o generando cambios directos en él mediante el monitoreo y/o control de dispositivos, procesos y eventos.

i) **Usuario final:** persona natural que accede o utiliza un sistema, aplicación o servicio. Quedan fuera de las obligaciones de MFA las cuentas destinadas exclusivamente a comunicaciones automatizadas entre sistemas, aplicaciones o dispositivos, que no requieran la intervención de una persona para autenticarse.

Artículo segundo. Obligación de implementar MFA en sistemas de TI. Todos los sujetos obligados deberán implementar y/o habilitar y exigir MFA para el acceso mediante cuentas de usuario final a los sistemas, aplicaciones o servicios institucionales. Esta obligación comprende, entre otros, los accesos remotos, los servicios en la nube y las consolas de administración accesibles desde Internet.

Cuando el sistema, aplicación o servicio disponga de un MFA, los sujetos obligados que tengan el control de su configuración deberán habilitarla y exigir su utilización respecto de todos sus usuarios

BORRADOR

finales, dentro de los plazos establecidos en el artículo duodécimo. Esta obligación no supone, por sí sola, desarrollar funcionalidades tecnológicas inexistentes.

Las nuevas plataformas, aplicaciones y servicios que se desarrollen o incorporen deberán contemplar un MFA desde su diseño.

Artículo tercero. Priorización de la implementación. Los sujetos obligados deberán priorizar la implementación de un MFA en las cuentas con privilegios administrativos y los accesos remotos desde redes externas a sistemas, aplicaciones y servicios institucionales.

La implementación se extenderá progresivamente a las demás cuentas de usuario final, incluidas las utilizadas exclusivamente en redes internas, de conformidad con los plazos máximos establecidos en el artículo duodécimo.

Artículo cuarto. Modalidades de implementación. El MFA podrá implementarse directamente en el sistema, aplicación o servicio institucional, o mediante mecanismos de control de acceso, tales como redes privadas virtuales (VPN), pasarelas de acceso o proveedores de identidad.

Para estos efectos, podrán utilizarse aplicaciones de autenticación instaladas en dispositivos móviles, llaves de seguridad físicas u otros mecanismos que permitan verificar la identidad del usuario mediante factores de autenticación independientes.

Los sujetos obligados deberán verificar que no existan vías alternativas de acceso a través de Internet que permitan eludir los MFA exigidos por el presente estándar.

Artículo quinto. Persistencia de sesiones y autenticación reforzada. La obligación de MFA no implicará exigir un nuevo factor en cada operación dentro de una sesión válidamente autenticada. Podrán emplearse inicio de sesión único (SSO), sesiones persistentes y

BORRADOR

mecanismos equivalentes, siempre que protejan las credenciales y sesiones contra usos no autorizados.

Las instituciones deberán establecer mecanismos de expiración de sesiones proporcionales al riesgo, revocación de sesiones y reautenticación ante indicios de compromiso, cambios relevantes en las condiciones de acceso o comportamientos anómalos que puedan indicar un uso no autorizado de las cuentas o sesiones. Para estos efectos, las instituciones deberán implementar, según corresponda, mecanismos de detección y respuesta frente a patrones de actividad inusuales o incompatibles con el comportamiento habitual del usuario, tales como accesos a volúmenes extraordinarios de información, descargas masivas de datos, consultas inusuales a información sensible u otras operaciones que se aparten de los patrones normales de utilización. Cuando dichas circunstancias permitan presumir razonablemente un compromiso de seguridad, las instituciones deberán adoptar medidas oportunas de contención, incluyendo, según la gravedad del riesgo, la exigencia de una nueva autenticación, la suspensión de operaciones, la revocación de sesiones o el bloqueo temporal del acceso.

Para cuentas con privilegios administrativos deberá exigirse un MFA efectivo al iniciar una sesión administrativa o al elevar privilegios, sin que una sesión ordinaria activa permita eludir esta exigencia. No será necesario un nuevo desafío por cada operación administrativa dentro de una sesión privilegiada válidamente autenticada, sin perjuicio de controles reforzados para operaciones especialmente sensibles.

Artículo sexto. Uso de dispositivos personales. Los sujetos obligados podrán permitir el uso de dispositivos personales de sus trabajadores o funcionarios para la implementación del MFA, de conformidad con la normativa aplicable.

Asimismo, podrán autorizar el acceso de sus trabajadores o funcionarios a sistemas, aplicaciones o servicios institucionales desde dispositivos personales, pero únicamente condicionado al uso de MFA.

BORRADOR

En aquellos casos en que el uso de dispositivos personales para el acceso remoto a la información o sistemas institucionales se encontrare autorizado con anterioridad a la entrada en vigencia del presente instrumento, se deberá condicionar la continuidad de ese permiso al uso de MFA. Si el titular del dispositivo se negare a implementarlo, la institución deberá impedir todo acceso remoto a información, sistemas o aplicaciones institucionales desde dispositivos personales.

Artículo séptimo. Obligación de proteger el acceso a sistemas de TO expuestos a Internet. Las instituciones que utilicen sistemas de TO no deberán exponer directamente a Internet las redes de TO, los sistemas SCADA que las administren, ni las interfaces de administración de sistemas de control industrial u otros componentes de tecnologías operacionales. Cuando sea indispensable administrarlos desde una red externa, el acceso deberá realizarse mediante un punto de entrada controlado que exija MFA a las personas autorizadas; por ejemplo, a través de sistemas SRA. La institución deberá verificar que no exista una conexión directa que permita eludir ese punto de entrada.

Artículo octavo. Administración de los accesos desde Internet. Las instituciones deberán mantener identificadas las cuentas habilitadas para los accesos comprendidos en el presente instrumento y deshabilitar oportunamente aquellas que ya no correspondan a personas autorizadas.

Deberán, además, configurar medidas para limitar los intentos automatizados de inicio de sesión, de acuerdo con las capacidades del servicio utilizado, y conservar los registros de autenticación disponibles por un período mínimo de 12 meses.

Si existen antecedentes de que una credencial pudo haber sido comprometida, deberán adoptar las medidas necesarias para impedir su uso no autorizado, restablecerla y cerrar las sesiones que puedan seguir activas. Si el compromiso afecta a un equipo, deberán verificar que este ya no se encuentre comprometido y que se hayan corregido las

BORRADOR

vulnerabilidades o condiciones de seguridad que permitieron dicho compromiso, antes de usarlo para generar nuevas credenciales.

Artículo noveno. Impedimentos transitorios para implementar un MFA. Excepcionalmente, los sujetos obligados podrán solicitar un plazo adicional para implementar MFA en cuentas de usuario final sin privilegios administrativos cuyo acceso esté restringido a redes internas, cuando acrediten impedimentos técnicos u operacionales objetivos que no hayan podido razonablemente superar dentro del plazo aplicable.

Los impedimentos presupuestarios solo podrán invocarse si se acreditan las gestiones de contratación o adquisición realizadas, la evaluación de alternativas y la imposibilidad objetiva de financiarlas dentro del plazo.

La falta de MFA nativo, el costo o las licencias adicionales no constituirán, por sí solos, impedimentos suficientes. La carga ordinaria de enrolamiento no constituirá, en ningún caso, un impedimento suficiente.

El régimen general de extensión previsto en este artículo tendrá carácter residual frente a los supuestos regulados en el artículo décimo. En estos últimos se aplicará el plazo diferenciado de ese artículo, sin perjuicio de que, si se solicita una extensión adicional, se apliquen el procedimiento, los requisitos de documentación, la evaluación por la Agencia y las medidas compensatorias establecidos en este artículo.

La solicitud deberá presentarse antes de que venza la mitad del plazo de implementación aplicable y, en todo caso, antes de su vencimiento. En ella se deberán singularizar los sistemas, aplicaciones, accesos y cuentas afectados; describir y acreditar el impedimento; señalar las alternativas técnicas y centralizadas evaluadas y las gestiones realizadas para superarlo; documentar los riesgos de compromiso de credenciales, escalamiento de privilegios y movimiento lateral; y acompañar un plan de implementación con medidas concretas, responsables y plazos definidos.

BORRADOR

La extensión solicitada no podrá exceder de noventa días corridos contados desde el vencimiento del plazo aplicable ni determinar, en ningún caso, que el plazo total exceda de doscientos setenta días corridos desde su inicio.

La Agencia podrá formular observaciones u objetar el plan presentado y requerir su modificación cuando los antecedentes aportados, las medidas propuestas o los plazos comprometidos resulten insuficientes.

El plazo adicional se contará desde el vencimiento del plazo original, con sujeción a los límites del inciso segundo, y en ningún caso la presentación de la solicitud suspenderá el plazo de implementación.

Mientras subsista el impedimento, el sujeto obligado deberá adoptar y mantener medidas compensatorias proporcionales al riesgo, que comprenderán, a lo menos, según la naturaleza del acceso respectivo:

a) La segmentación y restricción de las comunicaciones entre redes, sistemas y aplicaciones, limitando el acceso a los componentes estrictamente necesarios para la operación.

b) La limitación de las cuentas autorizadas, la asignación de privilegios mínimos necesarios y la revisión periódica de dichas autorizaciones.

c) La aplicación de controles contra intentos automatizados de autenticación.

d) La conservación y revisión de los registros de autenticación disponibles.

e) La restricción de los accesos entre redes y sistemas internos, especialmente cuando permitan acceder a información sensible o a sistemas críticos, mediante segmentación y controles de comunicación.

Los accesos de terceros proveedores a sistemas o información institucional deberán contar con MFA. Si un tercero no puede implementarlo, el sujeto obligado deberá impedir su acceso al sistema afectado mientras subsista esa condición.

Cuando las medidas compensatorias no permitan reducir suficientemente los riesgos asociados al acceso sin un MFA, el sujeto obligado deberá

BORRADOR

impedir dicho acceso hasta contar con un mecanismo de autenticación que cumpla las exigencias del presente instrumento, adoptando las medidas necesarias para resguardar la continuidad de los servicios esenciales.

El régimen excepcional de este artículo no será aplicable a cuentas con privilegios administrativos ni a accesos remotos desde redes externas. Estos deberán cumplir los plazos establecidos en la letra a) del artículo duodécimo. La solicitud no suspenderá las obligaciones de seguridad ni impedirá que la Agencia ejerza sus facultades de fiscalización.

Artículo décimo. Régimen diferenciado para determinados sistemas internos. Las cuentas de usuario final sin privilegios administrativos cuyo acceso esté restringido a redes internas podrán acogerse al plazo de ciento ochenta días previsto en la letra c) del artículo duodécimo cuando correspondan a alguno de los sistemas señalados en el presente artículo y se acrediten las condiciones indicadas.

Si el sujeto obligado no pudiere implementar un MFA dentro de dicho plazo, podrá solicitar la extensión prevista en el artículo noveno. La solicitud se regirá por el procedimiento y las medidas compensatorias establecidos en el artículo noveno.

La falta de MFA nativo no será suficiente por sí sola; deberán evaluarse previamente soluciones externas o centralizadas de autenticación.

a) Sistemas y aplicaciones heredados: cuando su arquitectura o sus limitaciones técnicas impidan incorporar oportunamente un MFA nativo o externo, o cuando su modificación inmediata pueda comprometer gravemente la continuidad operacional.

b) Sistemas clínicos y estaciones hospitalarias: únicamente sistemas de ficha clínica electrónica o de gestión de pacientes que funcionen exclusivamente dentro de redes internas hospitalarias, cuando la implementación del MFA pueda afectar gravemente los tiempos de atención y no existan alternativas rápidas y

BORRADOR

técnicamente viables, como tarjetas inteligentes, tarjetas NFC u otros mecanismos equivalentes.

c) Sistemas industriales y de tecnologías operacionales: sistemas SCADA, estaciones de ingeniería y otros componentes que operen exclusivamente en redes internas segregadas, cuando la implementación inmediata pueda comprometer gravemente la seguridad física, los procesos críticos o la continuidad de servicios esenciales, y no existan alternativas técnicamente viables.

d) Sistemas administrativos heredados: aplicaciones internas de recursos humanos, contabilidad, gestión documental u otras de naturaleza administrativa que no admitan oportunamente MFA nativo o externo. La antigüedad del sistema, su costo o la necesidad de adquirir licencias adicionales no justificarán, por sí solos, la aplicación de este régimen.

e) Aplicaciones internas de uso masivo: únicamente cuando la migración o modificación tecnológica necesaria para implementar un MFA dentro del plazo pueda provocar interrupciones graves de servicios esenciales. El número de usuarios y las tareas ordinarias de enrolamiento, capacitación y soporte no justificarán, por sí solos, la aplicación de este régimen.

La evaluación deberá singularizar los sistemas y las cuentas afectadas y acreditar las condiciones previstas para la categoría respectiva. El plan de implementación deberá identificar responsables y plazos, y prever medidas para reducir los riesgos de compromiso de credenciales, escalamiento de privilegios y movimiento lateral. La máxima autoridad del sujeto obligado, o quien cuente con atribuciones suficientes, deberá aprobar la evaluación y el plan.

La aplicación de este régimen no sustituirá la obligación de implementar MFA ni eximirá al sujeto obligado de sus deberes legales de ciberseguridad o de la responsabilidad que pudiera corresponder por la falta de medidas adecuadas de prevención, gestión o mitigación. La obsolescencia, la incompatibilidad tecnológica o la existencia de vulnerabilidades conocidas no constituirán, por sí solas, una eximente de responsabilidad. El vencimiento del plazo de implementación aplicable, incluida la prórroga expresamente concedida, si la hubiere sin que se haya implementado MFA pondrá

BORRADOR

término a la situación excepcional, sin perjuicio de las facultades de fiscalización y sanción de la Agencia conforme a la Ley N.° 21.663.

Artículo undécimo. Cumplimiento y supervisión. Los sujetos obligados deberán adoptar las medidas necesarias para asegurar la implementación efectiva y oportuna de las obligaciones establecidas en el presente instrumento, debiendo coordinar su ejecución y documentar su cumplimiento.

En los servicios esenciales y operadores de importancia vital del sector público, corresponderá al órgano directivo o jefe superior del organismo velar por el cumplimiento del presente estándar, de conformidad con el artículo 47 de la Ley N.° 21.663.

Las instituciones privadas deberán identificar y dejar constancia del directorio u otro órgano o persona que, conforme a su régimen de administración, ejerza la administración superior y vele por el cumplimiento del presente estándar. La institución deberá definir quién coordinará la implementación técnica, cómo se verificará su cumplimiento y cómo se informarán y corregirán las brechas detectadas.

La asignación de estas funciones no altera la calidad de la institución como sujeto obligado ni las funciones del delegado de ciberseguridad cuando corresponda.

Artículo duodécimo. Plazos de implementación. Los sujetos obligados deberán implementar y exigir el uso de un MFA dentro de los siguientes plazos máximos, contados desde la publicación del presente instrumento en el Diario Oficial:

a) Treinta días corridos: para todas las cuentas con privilegios administrativos y para todos los accesos remotos comprendidos en el ámbito de aplicación del presente instrumento.

b) Noventa días corridos: para las demás cuentas de usuario final comprendidas en el ámbito de aplicación del presente instrumento.

BORRADOR

c) Ciento ochenta días corridos: para las cuentas de usuario final sin privilegios administrativos cuyo acceso esté restringido a redes internas y que correspondan a los sistemas señalados en el artículo décimo, cuando se acrediten las condiciones previstas en dicho artículo. El sujeto obligado deberá implementar medidas compensatorias desde el inicio del plazo.

Los plazos diferenciados de las letras b) y c) no serán aplicables a cuentas administrativas ni a accesos remotos desde redes externas, que deberán cumplir el plazo de la letra a). La extensión solicitada conforme al artículo noveno no podrá ser sucesiva ni renovarse.

Artículo décimo tercero. Vigencia. El presente estándar entrará en vigencia desde su publicación en el Diario Oficial, sin perjuicio de los plazos de implementación establecidos en el artículo duodécimo.

Respecto de las instituciones que queden sujetas por primera vez al presente instrumento después de su entrada en vigencia, los plazos se contarán desde el día siguiente a aquel en que adquieran la calidad de prestadores de servicios esenciales o de operadores de importancia vital, según corresponda. La calificación posterior como operador de importancia vital no reiniciará los plazos ya iniciados ni reabrirá los vencidos respecto de las mismas obligaciones.

BORRADOR

ANÓTESE Y PUBLÍQUESE

MICHELLE BORDACHAR BENOIT
DIRECTORA NACIONAL (S)
AGENCIA NACIONAL DE CIBERSEGURIDAD