centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 862

Criterios de Aplicabilidad de las medidas del ENS ante la amenaza cuántica



Noviembre 2026

Edita:

centro criptológico nacional

Firmado digitalmente por CCN
Fecha: 2026.11.16 13:20:44 +01'00'

© Centro Criptológico Nacional, 2026

Fecha de Edición: noviembre de 2026

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1 INTRODUCCIÓN 4
2 OBJETO, ALCANCE Y DESTINATARIOS 4
2.1 Objeto 4
2.2 Alcance 5
2.3 Destinatarios 5
3 CONCEPTOS 5
4 CRITERIOS GENERALES DE APLICABILIDAD 7
4.1 Criterios de aplicabilidad de las medidas del ENS 7
4.1.1 [org.3] – Procedimientos de seguridad 8
4.1.2 [op.pl.1] – Análisis de riesgos 8
4.1.3 [op.pl.2] – Arquitectura de seguridad 9
4.1.4 [op.pl.3] – Adquisición de nuevos componentes 9
4.1.5 [op.pl.5] – Componentes certificados 10
4.1.6 [op.acc.5] – Mecanismo de autenticación (usuarios externos) 10
4.1.7 [op.acc.6] – Mecanismo de autenticación (usuarios de la organización) 11
4.1.8 [op.exp.1] – Inventario de activos 11
4.1.9 [op.exp.2] – Configuración de seguridad 12
4.1.10 [op.exp.7] – Gestión de incidentes 12
4.1.11 [op.exp.8] – Registro de la actividad 13
4.1.12 [op.exp.10] – Protección de claves criptográficas 13
4.1.13 [op.ext.1] – Contratación y acuerdos de nivel de servicio 13
4.1.14 [op.ext.3] – Protección de la cadena de suministro 14
4.1.15 [op.cont.1] – Análisis de impacto 14
4.1.16 [op.cont.2] – Plan de continuidad 15
4.1.17 [op.cont.3] – Pruebas periódicas 15
4.1.18 [mp.per.3] – Concienciación 16
4.1.19 [mp.per.4] – Formación 16
4.1.20 [mp.com.2] – Protección de la confidencialidad 16
4.1.21 [mp.com.3] – Protección de la integridad y de la autenticidad 17
4.1.22 [mp.si.2] – Criptografía 17
4.1.23 [mp.sw.1] – Desarrollo de aplicaciones 18
4.1.24 [mp.sw.2] – Aceptación y puesta en servicio 18
4.1.25 [mp.info.3] – Firma electrónica 19
4.1.26 [mp.info.4] – Sellos de tiempo 19
4.2 Matriz de escenarios y medidas relacionadas 20
5 PRIORIZACIÓN DE LAS ACTUACIONES 21
6 DOCUMENTACIÓN, SEGUIMIENTO Y REVISIÓN 22

1 INTRODUCCIÓN

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, establece los principios básicos, requisitos mínimos y medidas de seguridad destinados a proteger adecuadamente la información tratada y los servicios prestados por los sistemas incluidos en su ámbito de aplicación. Su aplicación se basa en la gestión de riesgos, la prevención, detección, respuesta y conservación, la existencia de líneas de defensa, la vigilancia continua y la reevaluación periódica.

Los avances en computación cuántica hacen necesario preparar la transición de los mecanismos criptográficos susceptibles de verse afectados hacia soluciones adecuadas para un escenario postcuántico. Esta necesidad afecta especialmente a determinados mecanismos de criptografía de clave pública utilizados para el establecimiento de claves, la autenticación y la firma digital, y exige considerar desde el momento actual el riesgo asociado a la captura de información cifrada para su eventual descifrado futuro.

La respuesta a este riesgo no debe limitarse a la sustitución de algoritmos criptográficos. La transición postcuántica constituye un proceso progresivo de gestión del riesgo y transformación de los sistemas, que comprende la identificación de los usos y dependencias criptográficas, la evaluación de su exposición, la determinación de las prioridades de actuación, la planificación y ejecución de la migración, la gestión de la coexistencia entre mecanismos y la incorporación de capacidades de criptoagilidad que permitan responder de forma ordenada a futuros cambios criptográficos.

Muchos de los riesgos asociados a esta transición pueden abordarse mediante las medidas del anexo II del ENS, adaptando su interpretación, procedimientos y capacidades técnicas. La preparación para hacer frente a la amenaza cuántica requiere, en particular, disponer de un inventario criptográfico adecuado, incorporar dicha amenaza al análisis de riesgos, establecer una planificación de la transición y desarrollar capacidades que permitan sustituir o actualizar los mecanismos criptográficos de manera controlada.

Esta guía vincula la transición postcuántica con las medidas del ENS. Para cada medida considerada relevante se establecen criterios que permiten determinar cuándo y cómo debe tenerse en cuenta la amenaza cuántica, sin modificar por ello el catálogo de medidas ni el régimen de exigibilidad previsto en el ENS.

Las recomendaciones relativas a mecanismos y parámetros criptográficos concretos, su autorización, los calendarios de transición y las condiciones técnicas de implantación se establecerán en las correspondientes directrices y recomendaciones del Centro Criptológico Nacional (CCN).

En este marco, la disposición adicional segunda del Real Decreto 311/2022 prevé que el CCN elabore y difunda guías de seguridad de las tecnologías de la información y las comunicaciones para facilitar el cumplimiento de sus disposiciones. La presente guía se encuadra en esa función de orientación técnica.

2 OBJETO, ALCANCE Y DESTINATARIOS

2.1 Objeto

Esta guía tiene por objeto establecer **criterios para la aplicación y adaptación de las medidas del ENS** relevantes para hacer frente a la amenaza cuántica mediante la preparación, planificación, ejecución y supervisión de la transición postcuántica de los sistemas de información, de forma homogénea, proporcionada, verificable y basada en el riesgo.

A efectos de esta guía, hacer frente a la amenaza cuántica requiere la identificación de los usos y dependencias criptográficas, la evaluación de exposición, la priorización de las actuaciones, la planificación y ejecución de la migración hacia mecanismos adecuados y la incorporación de capacidades de criptoagilidad que permitan responder a la evolución de los mecanismos, estándares y recomendaciones criptográficas.

Los criterios establecidos en esta guía **no sustituyen ni eximen de la categorización de los sistemas** de información conforme al ENS ni de la realización del correspondiente análisis y gestión de riesgos. La exigibilidad de las medidas vendrá determinada por la categoría del sistema, las dimensiones de seguridad, los niveles correspondientes y, cuando proceda, el análisis de riesgos. Los criterios establecidos en esta guía permiten determinar cuándo la implantación de una medida aplicable debe considerar específicamente los riesgos y necesidades asociados a la amenaza cuántica.

2.2 Alcance

Los criterios de aplicabilidad tienen un **alcance específico y complementario**, limitado a orientar la aplicabilidad, adaptación o, cuando proceda, refuerzo de determinadas medidas de seguridad afectadas por los riesgos derivados de la computación cuántica.

La evaluación deberá considerar el horizonte de protección de la información y las evidencias, la vigencia esperada de los mecanismos criptográficos y el tiempo necesario para sustituirlos. Se prestará especial atención a aquellas situaciones en las que **el horizonte de protección requerido, unido al tiempo estimado de migración, pueda superar el horizonte durante el cual resulte razonable confiar en el mecanismo criptográfico utilizado**.

2.3 Destinatarios

La guía está dirigida a las **entidades y organizaciones comprendidas en el ámbito de aplicación del ENS,** así como a los responsables que intervienen en el análisis y gestión de riesgos y en la implantación, operación y supervisión de las medidas de seguridad.

El ENS no solo es de aplicación a los sistemas de información del sector público, sino también a aquellos del **sector privado** que, en virtud de una relación contractual, presten servicios competenciales a las entidades del sector público, tal y como establece el artículo 2.3 del Real Decreto 311/2022. Asimismo, cualquier organización puede optar por aplicar voluntariamente el ENS como marco de referencia para mejorar la seguridad de sus sistemas.

3 CONCEPTOS

Para facilitar una interpretación homogénea de los criterios de aplicabilidad, los términos recogidos en la siguiente tabla se entenderán, a efectos de esta guía, con el significado que se indica, sin perjuicio de las definiciones establecidas en el ENS y en su normativa de desarrollo.

Concepto	Definición operativa
Amenaza cuántica	Riesgo para la seguridad de la información, las comunicaciones y las evidencias electrónicas derivado del desarrollo de capacidades de computación cuántica capaces de reducir o comprometer la seguridad proporcionada por determinados mecanismos criptográficos.

Concepto	Definición operativa
Criptografía postcuántica	Conjunto de mecanismos criptográficos diseñados para proporcionar seguridad frente a adversarios que dispongan tanto de capacidades de computación clásica como cuántica, de acuerdo con los estándares, mecanismos autorizados y directrices de los organismos competentes.
Transición postcuántica	Proceso planificado de identificación, evaluación, priorización, adaptación y sustitución de los mecanismos y dependencias criptográficas afectados por la amenaza cuántica, incluyendo la preparación, prueba, coexistencia, migración, retirada y seguimiento de los mecanismos utilizados.
Criptoagilidad	Capacidad de un sistema, producto, servicio u organización para sustituir o actualizar algoritmos, protocolos, parámetros, claves, certificados, bibliotecas o componentes criptográficos de forma controlada y con un impacto asumible sobre la seguridad, interoperabilidad, continuidad y operación del sistema.
Inventario criptográfico	Registro estructurado y actualizado de los usos de criptografía del sistema, incluyendo algoritmos, protocolos, bibliotecas, módulos, certificados, servicios, productos, interfaces y dependencias criptográficas, así como la información necesaria para determinar su finalidad, ubicación, responsable, ciclo de vida y necesidad de transición, sin incorporar material criptográfico secreto.
Horizonte de protección	Periodo durante el cual deben mantenerse las propiedades de seguridad requeridas para la información, las comunicaciones o las evidencias protegidas mediante mecanismos criptográficos.
Captura presente y descifrado futuro	Obtención y conservación de información cifrada en el presente con el propósito de intentar descifrarla posteriormente cuando se disponga de capacidades criptanalíticas o de computación cuántica suficientes.
Dependencia criptográfica	Dependencia directa o indirecta de algoritmos, protocolos, bibliotecas, módulos, certificados, claves, productos, servicios o infraestructuras criptográficas necesaria para el funcionamiento o la seguridad de un sistema.
Migración criptográfica	Conjunto de actuaciones técnicas y organizativas mediante las que un mecanismo criptográfico es sustituido por otro, incluyendo las fases de preparación, prueba, coexistencia, despliegue, retirada y verificación.
Modo híbrido	Uso combinado de mecanismos criptográficos clásicos y postcuánticos durante determinadas fases de la transición, cuando así lo establezcan las directrices aplicables, con el objetivo de facilitar la migración y gestionar los riesgos de seguridad e interoperabilidad.
Criterio de aplicabilidad	Pauta que orienta cuándo y cómo aplicar, adaptar o reforzar una medida o refuerzo del anexo II del ENS sin modificar el catálogo de medidas ni su régimen de exigibilidad.

Concepto	Definición operativa
Medida compensatoria	Salvaguarda alternativa o provisional que reduce el riesgo mientras no pueda implantarse la actuación prevista.
Declaración de Aplicabilidad	Relación de las medidas de seguridad del anexo II del ENS seleccionadas para un sistema, de acuerdo con su categoría y con el análisis de riesgos.

4 CRITERIOS GENERALES DE APLICABILIDAD

Los criterios de aplicabilidad proporcionan un marco para determinar, **de forma proporcionada y basada en el riesgo**, cuándo resulta necesario aplicar, adaptar o reforzar las medidas del ENS afectadas por la amenaza cuántica, teniendo en cuenta las características del sistema, la información y los servicios protegidos, su exposición, el horizonte de protección y la evolución de las capacidades tecnológicas y criptográficas. Con ello se pretende facilitar una aplicación homogénea y verificable del ENS, preservando al mismo tiempo su **estabilidad y neutralidad tecnológica**.

Las orientaciones deberán considerarse **durante todo el ciclo de vida del sistema y de los servicios afectados**, desde su planificación, diseño, desarrollo, adquisición y contratación hasta su operación, supervisión, actualización, continuidad, sustitución o retirada.

La mera disponibilidad o estandarización de mecanismos postcuánticos no determinará por sí sola su implantación. La selección y utilización de mecanismos criptográficos deberá atender a las directrices del Centro Criptológico Nacional, su autorización para el caso de uso correspondiente, la madurez técnica, la interoperabilidad, el rendimiento, la categoría del sistema y los riesgos identificados.

La transición postcuántica se apoyará especialmente en **cuatro capacidades transversales**:

1. **Inventario criptográfico**, que permita conocer qué mecanismos y dependencias criptográficas existen y dónde se utilizan.
2. **Evaluación del riesgo criptográfico y cuántico**, que permita determinar su exposición y prioridad de tratamiento.
3. **Planificación de la transición**, que establezca la hoja de ruta, responsables, recursos, dependencias, hitos y condiciones de migración.
4. **Criptoagilidad**, que permita sustituir o actualizar los mecanismos criptográficos de forma controlada y con un impacto asumible.

La implantación deberá priorizar, entre otros, los servicios esenciales, la información que requiera confidencialidad prolongada, las infraestructuras de clave pública, los servicios de identidad y firma electrónica y aquellos activos expuestos al riesgo de captura presente y descifrado futuro.

Los criterios de aplicabilidad propuestos determinan cuándo la implantación de una medida aplicable debe considerar específicamente los riesgos y necesidades derivados de la amenaza cuántica.

4.1 Criterios de aplicabilidad de las medidas del ENS

Para cada medida se indican los **criterios de aplicabilidad específicos para hacer frente a la amenaza cuántica** y su justificación. La selección de medidas recogidas en esta guía no tiene carácter exhaustivo. Las medidas no incluidas seguirán siendo aplicables cuando corresponda conforme al ENS.

Los criterios establecidos en esta guía no determinan por sí mismos la exigibilidad de una medida del ENS. Esta vendrá determinada por la categoría del sistema, las dimensiones de seguridad, los niveles correspondientes y, cuando proceda, el análisis de riesgos.

La selección no es exhaustiva: las medidas no incluidas seguirán siendo aplicables cuando corresponda conforme al ENS. Se debe **evitar considerar que la amenaza cuántica afecta de forma uniforme a todos los mecanismos.**

4.1.1 [org.3] – Procedimientos de seguridad

Código	Medida del ENS
[org.3]	**Procedimientos de seguridad**

Criterio de aplicabilidad
Los procedimientos de seguridad contemplarán la identificación, sustitución, renovación o revocación de algoritmos, protocolos, claves y certificados afectados por la amenaza cuántica, así como la coexistencia de mecanismos clásicos y postcuánticos. Se mantendrán actualizados, serán coherentes con la política, el análisis de riesgos y la arquitectura, y se ajustarán a las directrices de los organismos competentes y a la hoja de ruta de transición. Los procedimientos de seguridad deberán incorporar el gobierno de la transición criptográfica: responsables, coordinación, aprobación de cambios, gestión de excepciones, coexistencia temporal de mecanismos clásicos y resistentes a la computación cuántica, reversión segura y migración de emergencia.

Justificación
La transición criptográfica exige actuaciones repetibles, coordinadas y auditables. Mantener los procedimientos actualizados evita cambios incompletos o incompatibles y la reintroducción de configuraciones que hayan dejado de ser seguras.

4.1.2 [op.pl.1] – Análisis de riesgos

Código	Medida del ENS
[op.pl.1]	**Análisis de riesgos**

Criterio de aplicabilidad
Cuando la seguridad de los usos o dependencias criptográficas pueda verse comprometida durante el periodo de protección de la información o las evidencias, el análisis de riesgos incluirá los activos, los casos de uso y el inventario de dependencias internas y externas. Se evaluarán los plazos de confidencialidad y validez de la información y las evidencias, la vigencia esperada de los mecanismos, el riesgo de captura presente y descifrado futuro y el tiempo necesario para migrar. La transición será **especialmente prioritaria** cuando la suma del periodo de protección requerido y el tiempo de migración pueda superar el plazo durante el cual sea razonable confiar en la seguridad del mecanismo criptográfico utilizado.

El análisis permitirá definir prioridades, hitos, recursos, medidas compensatorias y criterios para acelerar la transición. La aceptación de mecanismos con resistencia insuficiente será expresa, motivada, temporal y revisable.

Justificación
La amenaza cuántica requiere iniciar las actividades de preparación antes de que existan capacidades cuánticas criptográficamente relevantes. En particular, la información cifrada capturada en el presente puede conservarse para intentar descifrarla posteriormente. La evaluación conjunta del horizonte de protección, la vigencia esperada de los mecanismos y el tiempo necesario para ejecutar la migración permite identificar los casos en los que la transición debe iniciarse anticipadamente y establecer prioridades proporcionadas al riesgo.

4.1.3 [op.pl.2] – Arquitectura de seguridad

Código	Medida del ENS
[op.pl.2]	**Arquitectura de seguridad**

Criterio de aplicabilidad
Cuando la arquitectura de seguridad incluya mecanismos criptográficos o relaciones de confianza que puedan verse afectados por la amenaza cuántica, se identificarán sus componentes, interfaces y dependencias, y se incorporará la criptoagilidad al diseño. La arquitectura de transición preverá mecanismos postcuánticos o híbridos cuando proceda, conforme a las directrices de los organismos competentes. Contemplará la interoperabilidad, el rendimiento, la gestión de claves y certificados y la coexistencia temporal, e impedirá la degradación a mecanismos no autorizados. Las alternativas de recuperación evitarán reintroducir configuraciones que hayan perdido su seguridad.

Justificación
Documentar la arquitectura permite identificar los mecanismos de protección y las relaciones de confianza y vincularlos al análisis de riesgos. Si la criptografía de clave pública está distribuida entre aplicaciones, comunicaciones, autenticación e infraestructuras de confianza, su sustitución coordinada evita migraciones parciales que dejen puntos vulnerables o interrumpan servicios.

4.1.4 [op.pl.3] – Adquisición de nuevos componentes

Código	Medida del ENS
[op.pl.3]	**Adquisición de nuevos componentes**

Criterio de aplicabilidad
Al adquirir componentes con mecanismos o dependencias criptográficas que puedan verse afectados durante su vida útil prevista, se definirán requisitos de criptoagilidad, actualización criptográfica, documentación de dependencias, interoperabilidad y soporte para la migración, conforme al análisis de riesgos y a la arquitectura.

Se incluirán mecanismos postcuánticos o híbridos cuando proceda. Los aspectos técnicos, contractuales, formativos y financieros se planificarán conjuntamente, de acuerdo con los hitos de transición.

Justificación
Las nuevas adquisiciones pueden generar dependencias de algoritmos o componentes difíciles de sustituir y dificultar la migración. Planificar su evolución y soporte durante toda su vida útil ayuda a evitar estas dependencias y a coordinar los recursos de la transición.

4.1.5 [op.pl.5] – Componentes certificados

Código	Medida del ENS
[op.pl.5]	**Componentes certificados**

Criterio de aplicabilidad
En la selección de productos y servicios de seguridad se atenderá a los requisitos de cualificación que resulten aplicables conforme al ENS y a las directrices del CCN. Cuando la transición postcuántica resulte relevante para el caso de uso, se valorará la capacidad del producto o servicio para incorporar los mecanismos criptográficos autorizados, su criptoagilidad, su soporte de actualización y la hoja de ruta del fabricante o proveedor.

Justificación
La cualificación de un producto o servicio ofrece garantías sobre su seguridad, pero no acredita por sí sola que sus mecanismos criptográficos resistan la amenaza cuántica. Priorizar los componentes cualificados que además empleen mecanismos resistentes, conforme a las guías del CCN, reduce el riesgo de adquirir elementos que deban sustituirse durante su vida útil y facilita una transición ordenada.

4.1.6 [op.acc.5] – Mecanismo de autenticación (usuarios externos)

Código	Medida del ENS
[op.acc.5]	**Mecanismo de autenticación (usuarios externos)**

Criterio de aplicabilidad
Cuando la autenticación de usuarios externos dependa de certificados digitales u otros mecanismos de clave pública potencialmente afectados por la amenaza cuántica, se identificarán los certificados, protocolos y cadenas de confianza implicados y se planificará su sustitución según la categoría del sistema y el análisis de riesgos. La migración preservará la interoperabilidad e impedirá la degradación a mecanismos no autorizados. Los métodos no basados en clave pública mantendrán su tratamiento ordinario.

Justificación

El debilitamiento de los algoritmos que verifican la identidad de los usuarios externos puede comprometer la autenticación y facilitar la suplantación. Una migración coordinada preserva la confianza y la interoperabilidad de los accesos.

4.1.7 [op.acc.6] – Mecanismo de autenticación (usuarios de la organización)

Código	Medida del ENS
[op.acc.6]	Mecanismo de autenticación (usuarios de la organización)

Criterio de aplicabilidad
La planificación de la transición incluirá la autenticación de los usuarios de la organización, también en el acceso remoto. Se identificarán los certificados, claves públicas, protocolos y cadenas de confianza afectados por la amenaza cuántica y se programará su sustitución sin interrumpir el servicio. Cuando sea aplicable el refuerzo **[op.acc.6.r9.2],** se cifrará el tráfico de acceso remoto y su adaptación incorporará capacidades de criptografía postcuántica. La transición de la autenticación de dispositivos, servicios y procesos se planificará de forma coordinada con la arquitectura, las comunicaciones y la gestión de claves, sin incluirla automáticamente en esta medida. Se revisarán sus certificados, claves, protocolos y cadenas de confianza para distinguir los métodos afectados de los que conserven una resistencia adecuada.

Justificación
La autenticación depende de la confianza en las credenciales y los mecanismos de acceso. Las dependencias de clave pública, también habituales en API, comunicaciones entre sistemas y cargas de trabajo, pueden ser numerosas y difíciles de sustituir. Inventariarlas y dotarlas de criptoagilidad permite coordinar su transición.

4.1.8 [op.exp.1] – Inventario de activos

Código	Medida del ENS
[op.exp.1]	Inventario de activos

Criterio de aplicabilidad
Cuando los activos del sistema incluyan usos o dependencias criptográficas que deban evaluarse para la transición, el inventario recogerá los activos criptográficos relevantes y un mapa de sus dependencias. Indicará su finalidad, versión, ubicación y proveedor, sin incluir información secreta que pueda comprometerlos. Cuando sea aplicable el **refuerzo R4 Lista de componentes software**, la relación formal de componentes software y servicios de despliegue complementará el inventario.

Justificación
El conocimiento de los usos y dependencias criptográficas es necesario para evaluar la exposición, priorizar sistemas y planificar una transición completa, evitando que permanezcan componentes afectados sin identificar.

No es posible evaluar ni planificar una transición criptográfica completa sin conocer dónde y para qué se utiliza la criptografía. Un inventario estructurado permite identificar dependencias directas e indirectas, priorizar las actuaciones y evitar que permanezcan mecanismos vulnerables o no actualizados por no haber sido identificados durante la planificación.

4.1.9 [op.exp.2] – Configuración de seguridad

Código	Medida del ENS
[op.exp.2]	**Configuración de seguridad**

Criterio de aplicabilidad
Las configuraciones de seguridad establecerán los mecanismos, parámetros y protocolos autorizados, deshabilitarán las opciones obsoletas e impedirán degradaciones de seguridad. Los cambios se controlarán y documentarán para garantizar su trazabilidad, conforme al plan de transición. Si la configuración permite protocolos, suites, algoritmos o mecanismos criptográficos cuya retirada esté prevista en el plan de transición, se eliminarán o desactivarán en coordinación con las pruebas de interoperabilidad y continuidad.

Justificación
La homogeneidad de las configuraciones evita el uso de algoritmos vulnerables, reduce la exposición y facilita el despliegue coordinado. Retirar de forma coordinada los mecanismos heredados limita esa exposición y facilita la migración a configuraciones resistentes a la amenaza cuántica, sin comprometer la interoperabilidad ni la continuidad del servicio.

4.1.10 [op.exp.7] – Gestión de incidentes

Código	Medida del ENS
[op.exp.7]	**Gestión de incidentes**

Criterio de aplicabilidad
La gestión de incidentes abordará la pérdida de confianza criptográfica que pueda afectar a algoritmos, claves, certificados, firmas, comunicaciones e infraestructuras o servicios de confianza. Los procedimientos diferenciarán la transición planificada de la migración de emergencia y preverán la revocación, la sustitución urgente, la preservación de evidencias y la coordinación con terceros. En coordinación con las capacidades de continuidad, se preparará y ensayará una migración acelerada con criterios de activación y recuperación que impidan restaurar configuraciones vulnerables.

Justificación
Un avance criptoanalítico o un cambio de directrices puede comprometer la confianza en los mecanismos criptográficos y exigir actuaciones urgentes y simultáneas en múltiples servicios,

componentes y terceros. La gestión de incidentes permite coordinar esta respuesta y complementa, sin sustituirla, la migración planificada.

4.1.11 [op.exp.8] – Registro de la actividad

Código	Medida del ENS
[op.exp.8]	**Registro de la actividad**

Criterio de aplicabilidad
Para supervisar y acreditar la transición y el ciclo de vida de claves, certificados y mecanismos criptográficos, se conservarán evidencias suficientes de su generación, uso, renovación, revocación, sustitución y configuración, vinculadas a los cambios, aprobaciones, pruebas y resultados. Los periodos de conservación serán coherentes con las obligaciones aplicables y el valor probatorio de la información.

Justificación
La trazabilidad permite acreditar qué mecanismo protegía cada operación, investigar fallos y demostrar la ejecución de la hoja de ruta.

4.1.12 [op.exp.10] – Protección de claves criptográficas

Código	Medida del ENS
[op.exp.10]	**Protección de claves criptográficas**

Criterio de aplicabilidad
Si el sistema gestiona claves de mecanismos cuya seguridad deba revisarse ante la amenaza cuántica, se evaluará su ciclo de vida completo. Se planificarán su rotación, invalidación, sustitución ordenada, respaldo y recuperación, de acuerdo con la transición y los mecanismos autorizados. Se evaluarán por separado el establecimiento de claves, la firma digital, el cifrado simétrico y las funciones hash, atendiendo a sus dependencias, parámetros, requisitos de interoperabilidad y criterios de aceptación. Conforme a las directrices del CCN, se comprobarán la autorización del mecanismo, la adecuación del producto y la conformidad de su implementación. Las soluciones híbridas se evaluarán en conjunto.

Justificación
La custodia correcta de una clave no compensa la pérdida de seguridad del algoritmo asociado. Cada función presenta dependencias y criterios de aceptación diferentes.

4.1.13 [op.ext.1] – Contratación y acuerdos de nivel de servicio

Código	Medida del ENS
[op.ext.1]	**Contratación y acuerdos de nivel de servicio**

Criterio de aplicabilidad
Cuando la evolución de los componentes, plataformas o dependencias criptográficas de los servicios contratados requiera la intervención de un proveedor, los contratos y acuerdos definirán el servicio, las responsabilidades, los niveles mínimos y las consecuencias del incumplimiento. Incluirán compromisos de mantenimiento, evolución y actualización criptográfica, soporte, interoperabilidad, notificación de vulnerabilidades, actualización y sustitución de certificados, sustitución de algoritmos, fin de soporte criptográfico y colaboración en pruebas y migraciones. Estas obligaciones se extenderán a los subcontratistas y a las dependencias esenciales.

Justificación
La entidad depende de sus proveedores para modificar plataformas, productos y servicios. Definir sus obligaciones antes de que la migración sea urgente permite coordinar responsabilidades y contar con el soporte necesario para ejecutarla.

4.1.14 [op.ext.3] – Protección de la cadena de suministro

Código	Medida del ENS
[op.ext.3]	Protección de la cadena de suministro

Criterio de aplicabilidad
Cuando la cadena de suministro incluya bibliotecas, módulos criptográficos, PKI, HSM, firmware, dispositivos o servicios externos potencialmente afectados por la amenaza cuántica, se evaluarán los proveedores y la procedencia, el soporte y la capacidad de sustitución de estos componentes y servicios, así como las dependencias de subcontratación, la hoja de ruta y los compromisos y plazos de migración.

Justificación
Una dependencia no identificada o un proveedor sin ruta de actualización puede impedir o retrasar la transición completa.

4.1.15 [op.cont.1] – Análisis de impacto

Código	Medida del ENS
[op.cont.1]	Análisis de impacto

Criterio de aplicabilidad
Cuando la obsolescencia criptográfica, la pérdida de confianza en los mecanismos o una migración urgente puedan afectar a la disponibilidad de los servicios, el análisis de impacto evaluará las posibles interrupciones, incluidas las de los servicios dependientes de PKI y certificados. Se identificarán los elementos críticos, las dependencias comunes, los tiempos máximos admisibles de interrupción y las alternativas operativas.

Justificación

La pérdida de confianza en un mecanismo compartido puede afectar simultáneamente a múltiples servicios críticos.

4.1.16 [op.cont.2] – Plan de continuidad

Código	Medida del ENS
[op.cont.2]	**Plan de continuidad**

Criterio de aplicabilidad
Cuando la transición criptográfica o la pérdida de confianza en sus mecanismos puedan afectar al mantenimiento o la recuperación de los servicios críticos, el plan de continuidad incluirá la sustitución urgente de claves y certificados, los mecanismos alternativos, la migración de emergencia y la verificación de integridad. Se definirán los criterios de activación de una migración acelerada y los procedimientos de recuperación que eviten restaurar configuraciones vulnerables. Estos procedimientos se coordinarán con los equipos técnicos, los responsables de PKI, los proveedores y los titulares de los servicios, y se ensayarán con los terceros participantes.

Justificación
Una transición no planificada puede provocar indisponibilidad o reintroducir mecanismos cuya seguridad se haya perdido.

4.1.17 [op.cont.3] – Pruebas periódicas

Código	Medida del ENS
[op.cont.3]	**Pruebas periódicas**

Criterio de aplicabilidad
Cuando el plan de continuidad contemple la transición criptográfica o la pérdida de confianza en algoritmos o infraestructuras, se ensayarán la migración, la renovación masiva, la revocación, la coexistencia, la migración acelerada, la recuperación y la reversión segura. Las pruebas verificarán los criterios de activación de la migración acelerada, la coordinación con terceros y la recuperación sin restaurar configuraciones vulnerables. Sus resultados servirán para actualizar el inventario, el análisis de riesgos, los procedimientos, el plan de continuidad y la hoja de ruta.

Justificación
Las pruebas permiten detectar dependencias ocultas o no inventariadas, incompatibilidades y plazos de transición o recuperación poco realistas, y corregir las deficiencias del plan antes de ejecutar la transición.

4.1.18 [mp.per.3] – Concienciación

Código	Medida del ENS
[mp.per.3]	Concienciación

Criterio de aplicabilidad
Cuando los responsables o usuarios deban aplicar decisiones de transición criptográfica o gestionar criptografía o información de larga vida útil, la concienciación abordará la necesidad de renovar claves, credenciales, certificados y evidencias, los riesgos de retrasar estas actuaciones y los canales para comunicar anomalías o instrucciones de migración.

Justificación
La transición afecta a usuarios y responsables no técnicos y requiere comprensión de las decisiones y plazos.

4.1.19 [mp.per.4] – Formación

Código	Medida del ENS
[mp.per.4]	Formación

Criterio de aplicabilidad
Cuando las funciones del personal requieran competencias para preparar, ejecutar o verificar la transición criptográfica, la formación se adaptará a los responsables de PKI, firma, arquitectura, desarrollo, sistemas, contratación, continuidad, conservación y auditoría. Incluirá inventario criptográfico, criptoagilidad, migración, pruebas, preservación y respuesta de emergencia. Su eficacia se comprobará mediante ejercicios, pruebas y evidencias de ejecución.

Justificación
La complejidad técnica y organizativa de la transición exige competencias especializadas y coordinación entre equipos.

4.1.20 [mp.com.2] – Protección de la confidencialidad

Código	Medida del ENS
[mp.com.2]	Protección de la confidencialidad

Criterio de aplicabilidad
Si la confidencialidad de la información transmitida depende de mecanismos potencialmente vulnerables a la amenaza cuántica, se identificarán las comunicaciones y categorías de información afectadas, su sensibilidad, exposición histórica y periodo de protección. Se priorizará la migración a mecanismos resistentes autorizados, especialmente para la información que requiera confidencialidad prolongada y esté expuesta a captura presente y descifrado futuro. Las posibles capturas previas recibirán un tratamiento diferenciado.

La decisión se documentará según el tipo de información, su exposición y periodo de protección, considerando las dimensiones y niveles de seguridad pertinentes y, cuando corresponda, la categoría del sistema. La protección de la información almacenada se coordinará con las medidas de soportes y claves.

Justificación
La información cifrada puede capturarse hoy para descifrarla en el futuro. La migración adquiere mayor prioridad si la confidencialidad debe mantenerse más allá de la vigencia prevista del mecanismo criptográfico. Migrar reduce la exposición futura, pero no elimina por sí solo el riesgo asociado a la información ya interceptada, que requiere un tratamiento diferenciado.

4.1.21 [mp.com.3] – Protección de la integridad y de la autenticidad

Código	Medida del ENS
[mp.com.3]	Protección de la integridad y de la autenticidad

Criterio de aplicabilidad
Cuando la protección del origen, la integridad o la autenticidad de las comunicaciones dependa de firmas o mecanismos de clave pública potencialmente afectados por la amenaza cuántica, se inventariarán y se evaluará su verificabilidad futura. Su sustitución se planificará en coordinación con la gestión de PKI y claves y con los responsables de firma electrónica, sellado de tiempo y preservación de evidencias.

Justificación
La amenaza cuántica puede debilitar los algoritmos de firma y autenticación y comprometer la confianza en la información y las comunicaciones. Estos mecanismos deben seguir siendo adecuados para su uso durante todo el periodo en que sea necesario verificar el origen, la integridad y la autenticidad de la información.

4.1.22 [mp.si.2] – Criptografía

Código	Medida del ENS
[mp.si.2]	Criptografía

Criterio de aplicabilidad
Si la protección criptográfica de la información en soportes requiere revisión ante la amenaza cuántica, se identificarán el cifrado empleado, las dependencias de clave pública, la gestión y recuperación de claves y el horizonte de protección. La evaluación atenderá tanto a las condiciones de aplicabilidad como a la categoría del sistema. La selección de algoritmos y parámetros se basará en el inventario y seguirá las recomendaciones de los organismos competentes, considerando la priorización, la criptoagilidad y la revisión de parámetros simétricos y funciones hash. Solo se contemplarán mecanismos postcuánticos o híbridos

cuando proceda y estén autorizados. Las actuaciones se coordinarán con las medidas pertinentes de comunicaciones, firma y protección de claves.

Justificación
La estandarización de un mecanismo no garantiza que esté autorizado ni que el producto o su implementación sean conformes para un uso concreto en el ENS. La información almacenada puede requerir protección durante más tiempo del que los mecanismos criptográficos que la protegen seguirán siendo seguros. La transición debe prepararse, por tanto, antes de que exista capacidad cuántica relevante, con especial atención a las dependencias de clave pública en el cifrado, el intercambio de claves y la firma.

4.1.23 [mp.sw.1] – Desarrollo de aplicaciones

Código	Medida del ENS
[mp.sw.1]	**Desarrollo de aplicaciones**

Criterio de aplicabilidad
Si las aplicaciones utilizan mecanismos o dependencias criptográficas que requieran adaptación a la amenaza cuántica, su desarrollo incorporará seguridad desde el diseño y control de componentes. Las primitivas criptográficas se separarán de la lógica de negocio para permitir sustituir bibliotecas, algoritmos, parámetros, claves y certificados sin rediseñar la aplicación. Durante el ciclo de desarrollo se documentarán y controlarán las dependencias criptográficas, evitando vínculos rígidos o sin documentar. Las políticas criptográficas se centralizarán siempre que sea posible.

Justificación
Diseñar aplicaciones sin dependencias criptográficas rígidas facilita la sustitución de sus mecanismos y reduce el coste, el plazo y el riesgo de migración. Integrar la criptoagilidad desde el desarrollo permite adaptar las aplicaciones a nuevas recomendaciones o a la pérdida de seguridad de determinados mecanismos sin rediseñarlas por completo.

4.1.24 [mp.sw.2] – Aceptación y puesta en servicio

Código	Medida del ENS
[mp.sw.2]	**Aceptación y puesta en servicio**

Criterio de aplicabilidad
Antes de poner en producción soluciones o cambios con mecanismos criptográficos afectados por la transición, se comprobarán los mecanismos, algoritmos y parámetros utilizados, la ausencia de dependencias obsoletas y la capacidad de actualización. Se realizarán pruebas de interoperabilidad, rendimiento, compatibilidad, coexistencia, reversión y continuidad en entornos controlados y aislados.

Las pruebas incluirán las configuraciones híbridas cuando proceda, y se conservarán las evidencias correspondientes.

Justificación
Los mecanismos postcuánticos pueden modificar los tamaños de los datos, la latencia, el consumo de memoria, los protocolos y las cadenas de confianza. La aceptación debe demostrar, antes del despliegue, que la solución cumple los criterios de seguridad y permite incorporar cambios sin interrumpir los servicios ni degradar la confidencialidad, autenticidad o integridad.

4.1.25 [mp.info.3] – Firma electrónica

Código	Medida del ENS
[mp.info.3]	**Firma electrónica**

Criterio de aplicabilidad
Cuando se generen o conserven firmas electrónicas cuyos mecanismos puedan perder seguridad durante el periodo de verificación requerido, se distinguirá entre la generación de nuevas firmas y la preservación de las históricas. Para las firmas históricas, se conservarán y documentarán los datos de validación, las cadenas de confianza, las referencias temporales y las renovaciones realizadas. La renovación o el resellado se planificarán y se evaluará su oportunidad y eficacia antes de la pérdida de confianza, conforme a las condiciones técnicas y jurídicas aplicables.

Justificación
La firma electrónica protege la autenticidad, la integridad y la identidad del firmante, garantías que deben poder acreditarse durante todo el periodo de conservación. Una renovación o un resellado tardíos no restablecen las evidencias cuya autenticidad o integridad ya no pueda acreditarse.

4.1.26 [mp.info.4] – Sellos de tiempo

Código	Medida del ENS
[mp.info.4]	**Sellos de tiempo**

Criterio de aplicabilidad
Cuando se generen o conserven sellos de tiempo cuyos mecanismos puedan perder seguridad durante el periodo de verificación requerido, se evaluarán sus algoritmos, claves y cadenas de confianza. Se distinguirá entre la generación de nuevos sellos y la conservación de evidencias históricas. Se documentarán los datos de validación, la cadena de confianza, la referencia temporal y las renovaciones realizadas. Se definirán procedimientos de renovación o resellado para mantener la continuidad de la evidencia durante el periodo requerido, y se evaluarán su oportunidad y eficacia antes de la pérdida de confianza, conforme a las condiciones técnicas y jurídicas aplicables.

Justificación
Los sellos de tiempo aportan una referencia temporal para verificar las evidencias y preservar su valor probatorio, pero también dependen de mecanismos de clave pública. Su conservación exige mantener estas garantías: la renovación o el resellado no restablecen por sí solos la integridad o autenticidad de evidencias que ya no puedan acreditarse.

4.2 Matriz de escenarios y medidas relacionadas

La siguiente matriz facilita una propuesta de trazabilidad entre escenarios de riesgo y medidas de seguridad. **No sustituye al análisis de riesgos, no** modifica la exigibilidad de las medidas y no constituye una lista cerrada.

Escenario	Descripción	Medidas relacionadas
Captura presente y descifrado futuro	Interceptación y conservación de información cifrada para descifrarla cuando exista capacidad cuántica suficiente.	[op.pl.1] Análisis de riesgos [op.exp.1] Inventario de activos [mp.com.2] Protección de la confidencialidad [mp.si.2] Criptografía
Ruptura de autenticación y firma	Pérdida de confianza en certificados, firmas o mecanismos de autenticación basados en algoritmos vulnerables.	[op.acc.5] Mecanismos de autenticación (usuarios externos) [op.acc.6] Mecanismos de autenticación (usuarios de la organización) [mp.com.3] Protección de la integridad y de la autenticidad [mp.info.3] Firma electrónica [mp.info.4] Sellos de tiempo
Dependencias criptográficas desconocidas	Uso de mecanismos, bibliotecas, certificados o protocolos no identificados que impiden planificar la transición.	[op.exp.1] Inventario de activos [op.pl.1] Análisis de riesgos [op.pl.2] Arquitectura de seguridad [mp.per.4] Formación [op.ext.3] Protección de la cadena de suministro
Falta de criptoagilidad	Imposibilidad de sustituir mecanismos sin rediseñar sistemas, aplicaciones o integraciones.	[op.pl.2] Arquitectura de seguridad [op.pl.3] Adquisición de nuevos componentes [op.pl.5] Componentes certificados [mp.sw.1] Desarrollo de aplicaciones [mp.sw.2] Aceptación y puesta en servicio [mp.si.2] Criptografía
Migración incompleta o inconsistente	Convivencia no controlada de mecanismos clásicos y postcuánticos, con degradaciones o retornos a opciones débiles.	[org.3] Procedimientos de seguridad [op.exp.2] Configuración de seguridad [mp.sw.1] Desarrollo de aplicaciones [mp.sw.2] Aceptación y puesta en servicio [mp.per.3] Concienciación

Escenario	Descripción	Medidas relacionadas
		[mp.per.4] Formación
Compromiso de claves o certificados	Exposición o gestión incorrecta de claves y certificados durante renovación, sustitución o revocación.	[op.exp.8] Registro de la actividad [op.exp.10] Protección de claves criptográficas [mp.per.3] Concienciación [op.exp.7] Gestión de incidentes
Pérdida de validez de evidencias	Deterioro futuro de la autenticidad o valor probatorio de documentos, registros, firmas y sellos conservados.	[mp.info.3] Firma electrónica [mp.info.4] Sellos de tiempo [mp.com.3] Protección de la integridad y de la autenticidad [op.exp.8] Registro de la actividad
Bloqueo por proveedores o productos	Dependencia de componentes sin soporte, actualización o ruta de migración.	[op.ext.1] Contratación y acuerdos de nivel de servicio [op.ext.3] Protección de la cadena de suministro [op.pl.3] Adquisición de nuevos componentes
Impacto en rendimiento y disponibilidad	Aumento de tamaños, latencia, memoria o consumo de recursos al desplegar mecanismos postcuánticos.	[mp.sw.2] Aceptación y puesta en servicio [op.cont.1] Análisis de impacto [op.cont.2] Plan de continuidad [op.cont.3] Pruebas periódicas
Interoperabilidad insuficiente	Fallos entre sistemas que adoptan estándares, parámetros o calendarios distintos.	[op.pl.2] Arquitectura de seguridad [mp.sw.2] Aceptación y puesta en servicio [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [op.exp.2] Configuración de seguridad
Migración criptográfica de emergencia	Necesidad de sustitución acelerada por pérdida de confianza o cambio urgente de directrices.	[op.exp.7] Gestión de incidentes [op.cont.2] Plan de continuidad [op.cont.3] Pruebas periódicas [mp.per.4] Formación

5 PRIORIZACIÓN DE LAS ACTUACIONES

Una vez determinada la aplicabilidad, la entidad priorizará las actuaciones de transición postcuántica necesarias para hacer frente a la amenaza cuántica, atendiendo a la reducción del riesgo que proporcionen y a la necesidad de ejecutar la migración con suficiente antelación.

Para ello, se seguirá un **procedimiento de cinco pasos**:

1. **Identificar usos y dependencias criptográficas:** inventariar los mecanismos, protocolos, certificados y componentes afectados, así como sus dependencias internas y externas.
2. **Evaluar la exposición y el horizonte de protección:** determinar durante cuánto tiempo debe protegerse la información o las evidencias y su exposición a captura presente y descifrado futuro.

3. **Determinar la necesidad y la urgencia de la transición:** comparar el horizonte de protección con la vigencia esperada del mecanismo y el tiempo de migración.
4. **Priorizar sistemas y casos de uso:** ordenarlos según su criticidad, la dificultad de sustitución, las dependencias y la criptoagilidad.
5. **Planificar y ejecutar la migración y verificar el riesgo residual:** definir y ejecutar las actuaciones y comprobar después el riesgo residual, aplicando medidas compensatorias cuando proceda.

6 DOCUMENTACIÓN, SEGUIMIENTO Y REVISIÓN

Las decisiones de aplicabilidad, adaptación, prioridad y aceptación se justificarán en el análisis de riesgos y se reflejarán, cuando corresponda, en la **Declaración de Aplicabilidad, los planes de tratamiento del riesgo y el plan de transición criptográfica.** Se documentarán responsables, recursos, plazos, dependencias, hitos, pruebas, criterios de aceptación, excepciones, medidas compensatorias y riesgo residual.

La aceptación del riesgo derivado de mecanismos vulnerables será expresa, motivada, temporal y revisable. El seguimiento utilizará indicadores verificables y se revisará al menos anualmente y ante cambios relevantes en la amenaza, los estándares, los mecanismos autorizados, los proveedores, la arquitectura, los incidentes o los resultados de las pruebas.

Las evidencias incluirán inventarios, procedimientos, arquitecturas, configuraciones, contratos, registros, informes de pruebas, decisiones de aceptación y resultados de ejercicios. Los resultados de la implantación y las pruebas realimentarán el inventario, el análisis de riesgos y el plan de transición.