

Edita:



© Centro Criptológico Nacional, 2018
NIPO: 083-19-020-7

Fecha de Edición: octubre de 2018

D. Carlos Galán y D. José Antonio Mañas han participado en la realización y modificación del presente documento y sus anexos.

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.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Octubre de 2018



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN	5
2. ÁMBITO DE APLICACIÓN	5
3. MEDIDAS COMPENSATORIAS.....	6
4. EVALUACIÓN Y AUDITORÍA.....	7
5. CUADRO DE COMPROBACIÓN DE LAS MEDIDAS COMPENSATORIAS.	8
6. EJEMPLOS	9
7. REFERENCIAS LEGALES Y NORMATIVAS	13

1. INTRODUCCIÓN

1. Como señala el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), la gestión de riesgos de los sistemas de información de su ámbito de aplicación posibilita el mantenimiento de un entorno controlado, minimizando tales riesgos hasta niveles aceptables. La reducción de estos niveles de riesgo se realiza mediante el despliegue de medidas de seguridad, que establecen un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y dichas medidas de seguridad.
2. El artículo 27.4 del ENS prescribe que, para cada sistema de información concernido, la relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado **Declaración de Aplicabilidad**, firmado por el Responsable de Seguridad.
3. El nuevo apartado 5 del artículo 27, introducido en virtud de la actualización del ENS, operada por Real Decreto 951/2015, de 23 de octubre, señala que:

Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor del riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los Capítulos II y III del ENS.

4. Añadiendo:

Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del Responsable de Seguridad.

5. El objetivo de la presente Guía es servir de ayuda a las entidades del ámbito de aplicación del ENS en la determinación e implantación de Medidas de Seguridad Compensatorias (a las que llamaremos en adelante **Medidas Compensatorias**), cuando no sea posible la adecuada implantación de las medidas de seguridad originariamente contempladas en el Anexo II del ENS, tal y como se detalla más adelante.

2. ÁMBITO DE APLICACIÓN

6. El ámbito subjetivo de aplicación de esta Guía alcanza a los sistemas de información de las entidades del Sector Público, según se encuentra definido en el artículo 2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público¹.

¹ Puede encontrarse una explicación más detallada sobre los ámbitos subjetivo y objetivo de aplicación del ENS en la “Guía CCN-STIC 830 Ámbito de aplicación del ENS”, descargable desde <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>

7. Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

3. MEDIDAS COMPENSATORIAS

8. Para lograr la conformidad con los principios básicos y requisitos mínimos establecidos en el ENS, deben aplicarse las medidas de seguridad indicadas en su Anexo II que, en todo caso, serán proporcionales a las dimensiones de seguridad relevantes y a la categoría del sistema de información a proteger.
9. No obstante, cuando una entidad del ámbito de aplicación del ENS, en base a razones técnicas, operativas, presupuestarias o de otro tipo, debidamente documentadas y justificadas, no esté en condiciones de aplicar alguna de las antedichas medidas de seguridad, podrá adoptar una *medida compensatoria* que, en todo caso, deberá satisfacer los siguientes

REQUISITOS:

1. Dar, al menos, cumplida respuesta al propósito de la medida de seguridad del Anexo II del ENS que compensa, en toda su extensión y rigurosidad.
 2. Proporcionar, al menos, un nivel de protección similar al de la medida de seguridad que compensa, de forma que la medida compensatoria adoptada contrarreste adecuadamente el riesgo que motivó la inclusión de aquella entre las medidas de seguridad originales del Anexo II del ENS que debían adoptarse.
10. La implantación de otras medidas de seguridad del Anexo II del ENS no debe interpretarse necesariamente como una medida compensatoria en sí misma. En concreto, las exigencias de seguridad satisfechas por otras medidas de seguridad del Anexo II del ENS:
- No pueden considerarse medidas compensatorias si las mismas exigencias de seguridad se hallan presentes en la medida que se pretende compensar.
 - Pueden considerarse medidas compensatorias si, requiriéndose para otro grupo de medidas de seguridad, no son exigibles para la concreta medida que se pretende compensar.
 - Pueden combinarse adecuadamente con controles adicionales, de forma que constituya una nueva medida compensatoria.
11. Además, es necesario valorar el riesgo adicional que podría suponer la implantación de la medida compensatoria en relación con la no implantación de la medida de seguridad prevista en el Anexo II del ENS.

4. EVALUACIÓN Y AUDITORÍA.

12. Durante la autoevaluación² o auditoría (bienal o extraordinaria)³ del sistema de información de que se trate, el Equipo Auditor, tomando en consideración los requisitos expresados en el epígrafe anterior, deberá analizar exhaustivamente las medidas compensatorias adoptadas, verificando que cada una de ellas hace frente adecuadamente al riesgo considerado en la medida de seguridad del Anexo II del ENS que se ha pretendido compensar, incluyendo los controles y procedimientos de comprobación que aseguren que tales medidas compensatorias permanecerán siendo eficaces tras la evaluación o auditoría⁴.

² Preceptivo para sistemas de información de categoría BÁSICA (Anexo II, apartado 2.1, ENS)

³ Preceptivo para sistemas de información de categorías MEDIA o ALTA (Anexo II, apartado 2.2, ENS).

⁴ Puede encontrarse más información en relación con la Auditoría de Seguridad y la Conformidad con el ENS en la “Guía CCN-STIC 802 Auditoría de seguridad” y la “Guía CCN-STIC 809 Conformidad con el ENS”, descargables desde <https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html>

5. CUADRO DE COMPROBACIÓN DE LAS MEDIDAS COMPENSATORIAS.

13. Para cada medida compensatoria que pretenda adoptarse se incluirá la siguiente información, que deberá incorporarse a la Declaración de Aplicabilidad, en el lugar de la medida de seguridad original del Anexo II del ENS que pretenda compensar.

	Información requerida
1. Ámbito de aplicación	Señalar la(s) medida(s) de seguridad del Anexo II del ENS que se pretende(n) compensar.
2. Limitaciones o restricciones	Enumerar las limitaciones o restricciones que impiden el cumplimiento con la medida de seguridad original del Anexo II del ENS.
3. Objetivo	<ol style="list-style-type: none"> 1. Definir el objetivo de la medida de seguridad original del Anexo II del ENS. 2. Identificar el objetivo satisfecho por la medida compensatoria.
4. Riesgo identificado	Identificar cualquier riesgo adicional que suponga la ausencia de la medida de seguridad original del Anexo II del ENS.
5. Definición de la(s) medida(s) compensatoria(s)	Definir la(s) medida(s) compensatoria(s), explicando de qué manera se alcanzan los objetivos de la medida de seguridad original del Anexo II del ENS que compensan y el riesgo asumido, si lo hubiere.
6. Validación de la medida(s) compensatoria(s)	Definir el proceso de validación y prueba de la(s) medida(s) compensatoria(s).
7. Mantenimiento	Definir los procedimientos y controles precisos para asegurar la permanente eficacia de la(s) medida(s) compensatoria(s) adoptada(s).

6. EJEMPLOS

14. A continuación, se desarrollan algunos escenarios a modo de ejemplo. Ni pretenden ni pueden ser imperativos en el sentido de establecer la imposibilidad de satisfacer una medida de seguridad, ni de imponer una cierta solución. El responsable de la seguridad del sistema deberá asesorarse por expertos en el aspecto concreto y aprobar la solución alternativa que le parezca conveniente.

15. **IMPORTANTE**, siempre:

La idoneidad de las medidas compensatorias siempre será objeto de evaluación específica en la auditoría prescriptiva del sistema, en donde se revisará el fundamento para proponerla como compensatoria, la idoneidad de los procesos operativos de seguridad que la acompañan y la resolución de los incidentes que se hayan detectado al respecto desde la última auditoría.

Ejemplo 1. Segregación de funciones

16. La medida [op.acc.3] establece:

dimensiones nivel	I C A T		
	bajo	medio	alto
	no aplica	aplica	=

Nivel MEDIO

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.

En concreto, se separarán al menos las siguientes funciones:

- a) Desarrollo de operación.
- b) Configuración y mantenimiento del sistema de operación.
- c) Auditoría o supervisión de cualquier otra función.

17. Ante la falta de personal para designar personas diferentes a estas funciones, se opta por potenciar los mecanismos de registro de actividad. Lo que no se puede prevenir, será detectado.

	Justificación
1. Ámbito de aplicación	[op.acc.3] Segregación de funciones y tareas
2. Limitaciones o	No hay personal disponible.

restricciones	
<p>3. Objetivo</p>	<p>El objetivo de la medida original es prevenir que una persona tenga capacidad para completar por su cuenta un proceso crítico, requiriendo la colusión de 2 o más personas lo que reduce drásticamente la probabilidad de que ocurra.</p> <p>La medida compensatoria que se propone es registrar de forma fiable todas las actuaciones sobre el sistema de información en un registro inviolable que es analizado posteriormente para detectar actividades incorrectas y tomar medidas de corrección. La medida, originalmente de carácter preventivo, se reemplaza por medidas de detección y reacción.</p>
<p>4. Riesgo identificado</p>	<p>La eficacia de la medida compensatoria depende de que todo se registre y de que el registro sea inviolable en el sentido de que la fecha sea fehaciente y no se puedan eliminar registros.</p>
<p>5. Definición de la(s) medida(s) compensatoria(s)</p>	<p>Toda la actividad de los operadores se recoge en un registro de actividad tipo blockchain, operado por una entidad externa. Dicho registro garantiza la fecha y hora de entrada e impide la eliminación de entradas.</p> <p>Los registros se analizan diariamente para detectar comportamientos sospechosos. Este análisis es automático y remite un informe firmado al responsable de la seguridad del sistema.</p> <p>Ver medidas [op.exp.8] y [op.exp.10], aplicadas como si fuera categoría ALTA.</p>
<p>6. Validación de la medida(s) compensatoria(s)</p>	<p>El auditor verificará que todas y cada una de las actividades queda reflejada en la cadena de blockchain.</p> <p>El auditor verificará que las actividades sospechosas son recogidas en el informe diario.</p> <p>El auditor verificará que se sigue un procedimiento de estudio y aplicación, en su caso, de medidas correctoras sobre el proceso afectado y disciplinarias sobre el operador.</p>
<p>7. Mantenimiento</p>	<p>El auditor verificará que todo el equipamiento está efectivamente configurado para dejar registro.</p> <p>Verificará igualmente que existe y se emplea un procedimiento de configuración en todo equipamiento que entra en el sistema.</p>

Ejemplo 2. Firma electrónica

18. La medida [mp.info.4] establece requisitos para todos los niveles de seguridad:

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.

En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del Artículo 27.

19. Nos encontramos con un problema de medios para generar firmas electrónicas con los niveles de seguridad requeridos y satisfacer al tiempo los requisitos para un servicio ágil.

20. Recurriremos a un mecanismo de códigos de verificación segura, que son códigos singulares, asociados al documento cuya integridad y autenticidad se desea ratificar, y que pueden ser remitidos a un servicio de validación online.

	Justificación
1. Ámbito de aplicación	[mp.info.4] Firma electrónica
2. Limitaciones o restricciones	No hay recursos para satisfacer todos los requisitos.
3. Objetivo	<p>El objetivo de la medida original es garantizar que la autenticidad y la autoría del documento pueden ser verificadas en cualquier momento del futuro por parte de cualquiera con acceso al documento en formato electrónico.</p> <p>La medida compensatoria que se propone es utilizar un código seguro de verificación, que es un código único, vinculado al documento, que puede ser sometido a un servicio en línea para su validación.</p> <p>En lugar de que el documento sea auto-verificable, pasamos a un procedimiento que requiere una consulta en línea. Como valor añadido, el documento puede estar impreso o en</p>

	formato de imagen, y ser perfectamente validable.
4. Riesgo identificado	La medida compensatoria requiere que el servicio de verificación en línea sea fiable.
5. Definición de la(s) medida(s) compensatoria(s)	<p>Cuando se genera el documento, se le asigna un código único de verificación, que se incorpora al documento y se guarda en una base de datos (que puede ser del mismo organismo o de un proveedor externo). En la base de datos se guarda al menos el documento, el código y la fecha de entrada.</p> <p>El servicio de validación permite al usuario recabar una copia igualmente válida del documento original a partir del código de validación a fin de evitar ataques de tipo corta-pega de códigos válidos en documentos manipulados.</p> <p>La seguridad del servidor se garantiza con las medidas pertinentes del ENS apropiadas a la categoría del sistema que estamos compensando. En particular [mp.s.2], relativa a la protección de servicios y aplicaciones web.</p>
6. Validación de la medida(s) compensatoria(s)	<p>El auditor verificar que existe la normativa habilitante correspondiente que legitime el procedimiento.</p> <p>El auditor verificará que los documentos se generan, distribuyen y almacenan según el proceso descrito arriba, así como que la verificación del documento es positiva si existe y negativa si no.</p> <p>El auditor verificará que el documento incluye de forma clara e inequívoca tanto el código de validación como las instrucciones para acceder al servicio de validación.</p> <p>El auditor verificará que el servicio de validación es capaz de suministrar una copia igualmente válida del documento original a partir del código de validación.</p> <p>El auditor verificará o recabará una certificación de cumplimiento de las medidas de seguridad requeridas para el sistema de información que hospeda el servicio de verificación.</p>
7. Mantenimiento	<p>El auditor verificará que documentos antiguos siguen siendo debidamente validados dentro del plazo de validez indicado en el documento.</p> <p>Verificará igualmente que se mantiene actualizada según normativa la auditoría del sistema que provee el servicio de validación.</p>

7. REFERENCIAS LEGALES Y NORMATIVAS

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- PCI Security Standards Council. Payment Card Industry (PCI). Data Security Standard. Requirements and Security Assessment Procedures, Version 3.2. April, 2016.