Junta de Andalucía

MEDIDAS COMPENSATORIAS y/o COMPLEMENTARIAS DE VIGILANCIA EN EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Junta de Andalucía

ÍNDICE

Junta de Andalucía

1. CONCEPTO

Junta de Andalucía

1.1 Concepto. Medida compensatoria

Las Medidas Compensatorias son acciones o conjunto de acciones de seguridad que se implementan para mitigar los riesgos asociados a las debilidades o deficiencias identificadas en los sistemas de información.

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.
Pero, 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 medidas de seguridad del Anexo II, **podrá adoptar una medida compensatoria.**

Junta de Andalucía

1.2 Concepto. Medida complementaria de vigilancia

Una medida complementaria de vigilancia es aquella que complementa y equilibra los requisitos exigibles que se han implementado para una determinada medida de seguridad, ya sea de “BASE” o de “REFUERZO”, cuando éstos no son suficientes.

La finalidad de las medidas complementarias de vigilancia es poder alcanzar el cumplimiento del ENS para dicha medida. También pueden complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original.

Junta de Andalucía

2.REGULACIÓN

Junta de Andalucía

2.1 Artículo 28.3 RD 311/2022

Las Medidas Compensatorias se regulan en el artículo 28.3 Real Decreto 311/2022

Artículo 28. Cumplimiento de los requisitos mínimos.

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.

b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.

c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. 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. 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. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

2.2 Guía de Seguridad TIC CCN-STIC 808. Verificación del cumplimiento

La Guía CCN-STIC 808 relativa al cumplimiento establece la posibilidad de sustituir las medidas indicadas por otras compensatorias

LAS MEDIDAS COMPENSATORIAS DEBEN PROTEGER IGUAL O MEJOR LOS ACTIVOS, SUSTITUYENDO A LAS MEDIDAS DE SEGURIDAD

LAS MEDIDAS COMPLEMENTARIAS DE VIGILANCIA DEBEN COMPLEMENTAR LA BASE O EL REFUERZO DE LA MEDIDA DE SEGURIDAD

4.3 MEDIDAS COMPENSATORIAS

Las medidas de seguridad referenciadas en el anexo II del ENS podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, el riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del RD 311/2022, de 3 de mayo.

Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implementadas y las medidas del anexo II que compensan.

Por todo ello, para cada una de las medidas de seguridad del anexo II del ENS, se deberá indicar si se ha empleado alguna medida compensatoria que la reemplace.

El empleo y modo de justificar las medidas compensatorias, se desarrolla en la guía *CCN-STIC 819 Medidas Compensatorias*.

4.4 MEDIDAS COMPLEMENTARIAS DE VIGILANCIA

Una medida complementaria de vigilancia es aquella que complementa y equilibra los requisitos exigibles que se han implementado para una determinada medida de seguridad, ya sea de "BASE" o de "REFUERZO", cuando éstos no son suficientes, a juicio de la organización, para poder alcanzar el cumplimiento del ENS para dicha medida. También pueden complementar a una medida compensatoria que no consigue igualar o mejorar el riesgo de la medida original.

En ocasiones, dicha medida complementaria de vigilancia será transitoria (limitada en el tiempo) hasta que se puedan implementar todos los requisitos requeridos por la medida de seguridad del ENS o para la efectividad plena de la medida compensatoria que se haya decidido implementar como alternativa.

2.2 Guía de Seguridad TIC CCN-STIC 808. Verificación del cumplimiento. Anexo II

En la Guía de Seguridad TIC CCN-STIC 808 indica que es necesario **indicar estas medidas en la Declaración de Aplicabilidad**

Art. 28	Declaración de aplicabilidad		
	Aplica: SI ☐ NO ☐ Artículo auditado: SI ☐ NO ☐		
Art. 28.3	En el caso de aplicar medidas compensatorias, ¿se ha justificado formalmente en la Declaración de Aplicabilidad la necesidad de aplicar tales medidas compensatorias y la justificación de que dichas medidas protegen, igual o mejor, al riesgo sobre los activos y sobre el sistema de información en su conjunto?		☐ SI
	NOTA: Cómo justificar formalmente las medidas compensatorias se detalla en la guía “CCN-STIC 819 Medidas compensatorias”.		☐ NO
Apartado 4.4 de esta guía, avalado por el apartado 8 del Anexo II del RD 311/2022.	En el caso de aplicar medidas complementarias de vigilancia ¿se indica formalmente en la Declaración de Aplicabilidad si dichas medidas complementarias son transitorias, o no, y se justifica que la medida que ha sido complementada, tal vez por estar en proceso de implantación, protege de forma análoga al sistema de información?		☐ SI
			☐ NO

Junta de Andalucía

2.2 Guía de Seguridad TIC CCN-STIC 808. Verificación del cumplimiento. Anexo II

En la Guía de Seguridad TIC CCN-STIC 808 se constata la posibilidad de indicar la/s medida/s compensatoria/s y/o la/s medidas complementarias de vigilancia

6.2 CUMPLIMIENTO DE MEDIDAS DE SEGURIDAD

6.2.1 Marco Organizativo

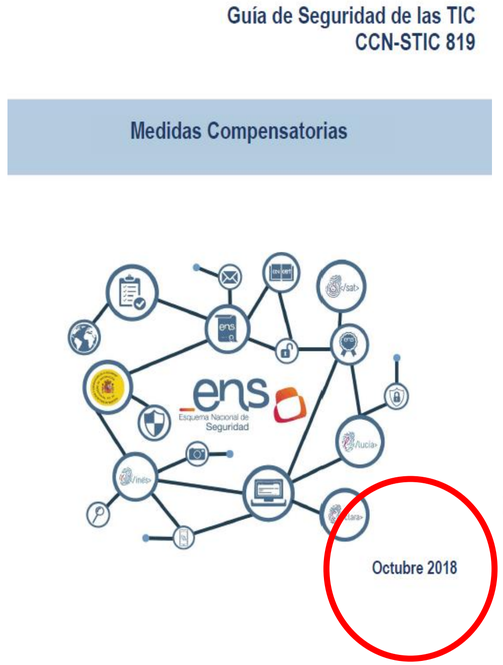
El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

Org.1	**Política de seguridad**
Categoría / dimensión Categoría	**Medida aplica:** SI ☐ NO ☐ **Medida auditada:** SI ☐ NO ☐ **Grado de implementación:** SI ☐ EN PROCESO ☐ NO ☐
	Medida compensatoria: SI ☐ NO ☐ **Medida complementaria de vigilancia:** SI ☐ NO ☐
Propuesta de evidencias	

Junta de Andalucía

2.3 Guía de Seguridad TIC CCN-STIC 819. Medidas Compensatorias

En la Guía de Seguridad TIC CCN-STIC 819 sirve de ayuda para determinar e implantar las Medidas Compensatorias cuando no es posible implantar las medidas de seguridad originalmente contempladas en el Anexo II del ENS



¡OJO!

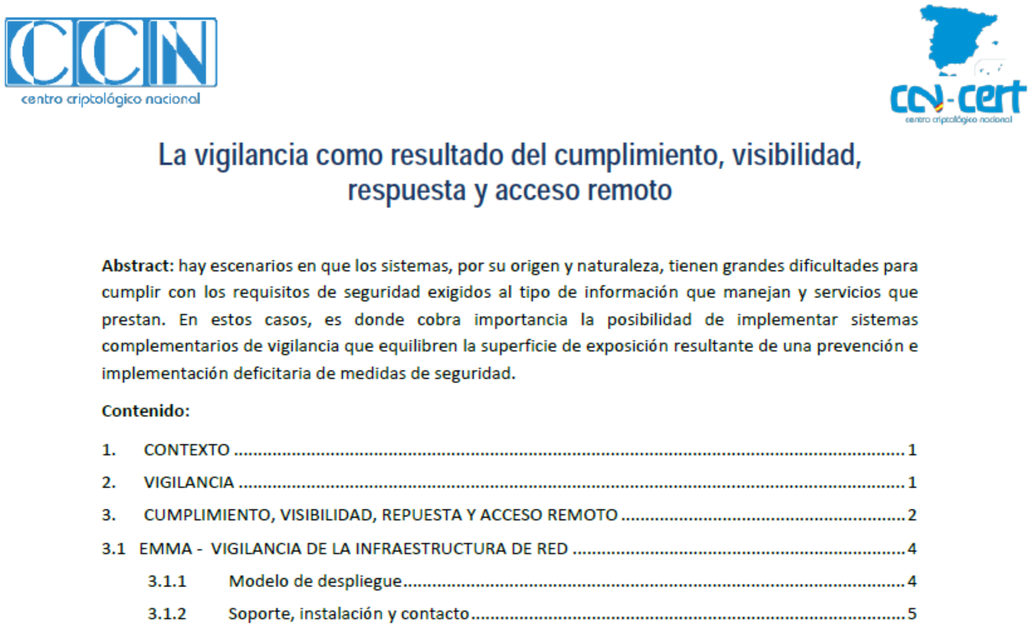
Junta de Andalucía

2.4 Medidas Complementarias de vigilancia

Debido al origen y naturaleza de algunos sistemas, estos tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos al tipo de información que manejan y servicios que prestan.
EN ESTOS CASOS es necesario adoptar medidas complementarias.

El CCN-CERT pone a disposición de los usuarios su solución **EMMA**, encargada de la vigilancia de deficiencias en:

- la capa de acceso y electrónica (cumplimiento), conectividad a la red (visibilidad),
- capacidad de respuesta ante eventos (respuesta)
- acceso remoto seguro.



La vigilancia como resultado del cumplimiento, visibilidad, respuesta y acceso remoto

Abstract: hay escenarios en que los sistemas, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos al tipo de información que manejan y servicios que prestan. En estos casos, es donde cobra importancia la posibilidad de implementar sistemas complementarios de vigilancia que equilibren la superficie de exposición resultante de una prevención e implementación deficitaria de medidas de seguridad.

Contenido:

Junta de Andalucía

3.REQUISITOS

Junta de Andalucía

3.1 Requisitos. Medida compensatoria

RAZONES TECNICAS, ORGANIZATIVAS O PRESUPUESTARIAS

NO ES POSIBLE APLICAR LA MEDIDA PROPUESTA EN EL ANEXO II

APLICAR MEDIDA COMPENSATORIA

CUMPLIR OBJETIVOS DE LA MEDIDA DE SEGURIDAD

NIVEL DE PROTECCIÓN SIMILAR A LA MEDIDA DE SEGURIDAD

VALORAR EL RIESGO DE IMPLANTAR LA MEDIDA COMPENSATORIA

INCLUIR EN LA DECLARACIÓN DE APLICABILIDAD

3.2 Requisitos. Medida complementaria de vigilancia

MEDIDA DEFICITARIA

NO ES POSIBLE APLICAR ADECUADAMENTE LA MEDIDA PROPUESTA EN EL ANEXO II O PARA MEJORAR UNA MEDIDA COMPENSATORIA

APLICAR MEDIDA COMPLEMENTARIA DE VIGILANCIA

INCLUIR EN LA DECLARACIÓN DE APLICABILIDAD

- DEFICIENCIA EN LOS ACCESOS
- VISIBILIDAD Y PERFILADO DE TODO LO CONECTADO
- CAPACIDAD DE RESPUESTA ANTE EVENTOS
- ACCESO REMOTO SEGURO

4.APLICACIÓN

Junta de Andalucía

4.1. Aplicación

En la Guía de Seguridad TIC CCN-STIC 808 se constata la posibilidad de indicar la/s medida/s compensatoria/s y/o la/s medidas complementarias de vigilancia

- SI LA/S MEDIDAS COMPENSATORIA/S TIENEN LAS MISMAS EXIGENCIAS QUE LA MEDIDA ORIGINAL
- IMPLANTAR OTRAS MEDIDAS NO EXIGIBLES
- SI NO CONTRARRESTA EL RIESGO O SUPONE UN RIESGO PARA LOS ACTIVOS QUE SE PRETENDEN PROTEGER, NO SE DARÁ POR VÁLIDA

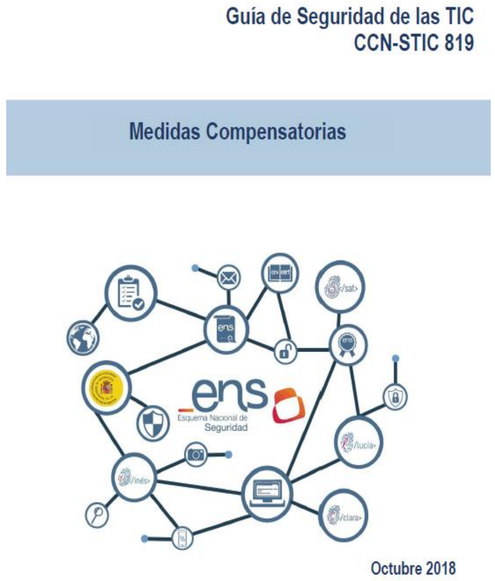
4.1. Aplicación

La implantación de otras medidas de seguridad del Anexo II del ENS no debe interpretarse necesariamente como una medida compensatoria en sí misma. 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 (por ejemplo, medidas de seguridad aplicables para nivel medio en un grupo de controles que se utilicen como medida compensatoria de una medida de nivel básico).
- Pueden combinarse adecuadamente con controles adicionales, de forma que constituya una nueva medida compensatoria (una medida de seguridad a la que se le añaden controles puede convertirse en una medida compensatoria para otra medida).

4.2 Proceso de aplicación

La/s Medida/s Compensatoria/s que se pretendan implantar debe recoger la siguiente información:



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	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).

Junta de Andalucía

4.2 Proceso de aplicación

Pasos para la aplicación de las Medidas Compensatorias

1. Identificación de la Necesidad de Medidas Compensatorias
- *Evaluación de Riesgos:* Se realiza una evaluación de riesgos para identificar las vulnerabilidades y las amenazas potenciales a la seguridad de la información

- *Análisis de Requisitos de Seguridad:* Se determinan los requisitos de seguridad necesarios basados en el nivel de riesgo y el impacto potencial en la organización.

2. Desarrollo de Medidas Compensatorias
- *Selección de Medidas*: Basado en el análisis previo, se seleccionan medidas compensatorias adecuadas para mitigar los riesgos identificados.

- *Implementación:* Se implementan las medidas seleccionadas. Esto puede incluir cambios en los procesos, la adopción de nuevas tecnologías o la mejora de las existentes

4.2 Proceso de aplicación

Pasos para la evaluación y auditoria de las Medidas Compensatorias

3. Evaluación de la Eficacia

- *Verificación de la Implementación:* Se verifica que las medidas compensatorias se hayan implementado correctamente y de acuerdo con los estándares establecidos.

- *Evaluación de la Eficacia*: Se evalúa la eficacia de las medidas implementadas para garantizar que los riesgos se mitiguen adecuadamente.

4. Auditoría

- Auditorías Internas: Se realizan auditorías internas para revisar y evaluar la eficacia de las medidas de seguridad implementadas, incluyendo las compensatorias. OBLIGATORIO A CATEGORÍA MEDIA Y ALTA.

4.2 Proceso de aplicación

Del cuadro de comprobación es IMPORTANTE REALIZAR **UNA AUDITORIA DEL SISTEMA**

IDONEIDAD DE LOS PROCESOS OPERATIVOS DE LA MEDIDA

RESOLUCIÓN DE INCIDENTES

Junta de Andalucía

4.3. Evaluación y auditoría

Se precisará el análisis de la idoneidad de las medidas compensatorias durante la finalización del proceso de adecuación, según categoría:

- Sistemas de información de categoría BÁSICA: durante la AUTOEVALUACIÓN

- Sistemas de información de categoría MEDIA O ALTA: durante la AUDITORÍA POR ENTIDAD DE CERTIFICACIÓN

El equipo auditor deberá comprobar todos los apartados vistos anteriormente, comprobando no solo la idoneidad de la medida y el grado de compensación del riesgo considerado, si no también si tales medidas serán eficaces en el futuro (GUÍA CCN-STIC 802 AUDITORÍA DE SEGURIDAD).

5.EJEMPLOS

Junta de Andalucía

5.1. EJEMPLO 1

SUPUESTO DE HECHO:
Medida de control: op.acc.3. Segregación de funciones y tareas
En un sistema de categoría MEDIA o ALTA se exige 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 o no autorizada.

La falta de personal de la entidad que se pretende certificar impide que se puedan separar funciones como el desarrollo de operaciones, la configuración del sistema de operación y/o la auditoría de funciones

5.1. EJEMPLO 1.1

APLICACIÓN DE MEDIDA COMPENSATORIA:

	Justificación
1. Ámbito de aplicación	[op.acc.3] Segregación de funciones y tareas
2. Limitaciones o	No hay personal disponible.
3. Objetivo	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. 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.
4. Riesgo identificado	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.
5. Definición de la(s) medida(s) compensatoria(s)	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. 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. Ver medidas [op.exp.8] y [op.exp.10], aplicadas como si fuera categoría ALTA.
6. Validación de la medida(s) compensatoria(s)	El auditor verificará que todas y cada una de las actividades queda reflejada en la cadena de blockchain. El auditor verificará que las actividades sospechosas son recogidas en el informe diario. 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.
7. Mantenimiento	El auditor verificará que todo el equipamiento está efectivamente configurado para dejar registro. Verificará igualmente que existe y se emplea un procedimiento de configuración en todo equipamiento que entra en el sistema.

ENS 2010

Junta de Andalucía

5.1. EJEMPLO 1.2

APLICACIÓN DE MEDIDA COMPENSATORIA:

Ámbito de aplicación	op.acc.3 segregación de funciones
Limitaciones o restricciones	En la ORGANIZACIÓN el personal TIC se limita a dos personas, lo que no hace posible la segregación de funciones requerida por la norma.
Objetivo	La segregación de funciones tiene como objetivo evitar que una tarea crítica recaiga en una sola persona, evitando de este modo que este usuario autorizado pueda abusar de sus derechos y cometer acciones ilícitas. Las medidas compensatorias adoptadas tienen como objetivo auditar las acciones que realizan las dos personas TIC para evitar que puedan hacer uso ilícito de sus privilegios al no participar una segunda persona en la ejecución de las tareas críticas, de manera que se genere un registro fiable de las acciones que realizan y se detecten acciones incorrectas, pudiendo adoptar medidas correctoras y, en su caso, disciplinarias.
Riesgo identificado	**La ausencia de la segregación de funciones o de medidas compensatorias implica un riesgo, ya que posibilita que usuarios autorizados con privilegios de acceso puedan cometer acciones ilícitas y, además, no se detecten por la organización, suponiendo un riesgo para la seguridad.** **Debe tenerse en cuenta que muchas acciones relacionadas están externalizadas, como por ejemplo la configuración y mantenimiento de la electrónica de red dentro del contrato XXX o de los dispositivos de comunicaciones dentro del contrato XXX.** **Los servicios de operación y monitorización de servidores están externalizados dentro del contrato XXX.** **El desarrollo, mantenimiento, operación y monitorización del sistema XXX está contratado externamente y lo realiza el proveedor del SaaS.** **En cuanto al portal web, cuando se han realizado desarrollos se ha contratado externamente, el último contrato el XXX.** **Las labores de auditoría, hasta ahora, han sido servicios contratados externamente, lo que minimiza el riesgo, al recaer estas funciones en terceros** **En el caso de los equipos de usuarios, sí que es el personal TIC quien realiza las funciones de configuración y mantenimiento.** **La eficacia de la medida compensatoria depende de que todo se registre, no se produzcan alteraciones de los registros y se revisen periódicamente**
Definición de las medidas compensatorias	Se han definido diferentes medidas compensatorias: - Revisión periódica de los logs de los dos miembros TIC que permita tener una trazabilidad de las acciones que han llevado a cabo. Se llevará un registro en la Excel logs.xlsx de las revisiones y los resultados serán remitidos al comité de seguridad. - Supervisión mutua entre los dos miembros TIC, de manera que cada acción que realicen en desarrollo, configuración, mantenimiento, operación y auditoria, sea verificada por el usuario que no ha participado en ella, evitando acciones no autorizadas. Se llevará un registro en la Excel Supervisión.xlsx de las supervisiones y los resultados serán remitidos al comité de seguridad.
Validación de la medida compensatoria	Los registros obtenidos de la medida compensatoria (revisión de logs y verificación de las acciones realizadas) serán examinados por el Comité de Seguridad, que valorará su efectividad, teniendo en cuenta para ello, si las tareas realizadas por el personal siempre se verifican por la otra persona que se ajusta a lo establecido.
Mantenimiento	Verificar periódicamente que la generación de los logs se mantiene activada, enviando la evidencia de ello al Comité de Seguridad.

MEDIDAS DE VIGILANCIA

Junta de Andalucía

5.2. EJEMPLO 2

SUPUESTO DE HECHO:
Medida de control: mp.info.4. Firma electrónica

Requisitos
Los sistemas de información deben garantizar por medio de la firma electrónica la integridad y autenticidad de los documentos.
1.1. En una Administración Pública, debe usarse un certificado electrónico reconocido o cualificado, que reúna los requisitos exigidos por la legislación de firma electrónica, según se determina en el art. 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
1.2 En un proveedor de la Administración Pública deben emplearsr certificados electrónicos reconocidos o cualificados.
Y en categoría media, se emplearán certificados electrónicos cualificados de proveedores que consten en española (Ley 6/2020, de 11 de noviembre) o europea (Reglamento IDAS)

Situación: la entidad no puede generar firmas electrónicas con los niveles de seguridad exigidos

Junta de Andalucía

5.3. EJEMPLO 2

APLICACIÓN DE MEDIDA COMPENSATORIA:

	Justificación
1. Ámbito de aplicación	[mp.info.4] Firma electrónica
2. Limitaciones o restricciones	No hay recursos para satisfacer todos los requisitos.
3. Objetivo	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. 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. 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
	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)	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 guara al menos el documento, el código y la fecha de entrada. 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. 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.
6. Validación de la medida(s) compensatoria(s)	El auditor verificar que existe la normativa habilitante correspondiente que legitime el procedimiento. 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. 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. 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. 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.
7. Mantenimiento	El auditor verificará que documentos antiguos siguen siendo debidamente validados dentro del plazo de validez indicado en el documento. Verificará igualmente que se mantiene actualizada según normativa la auditoría del sistema que provee el servicio de validación.

5.3. EJEMPLO 3

SUPUESTO DE HECHO:
Medida de control: op.acc.6. Mecanismos de autenticación

La entidad no puede implementar el doble factor de autenticación (2FA) fuera del perímetro de seguridad del Organismo

Junta de Andalucía

5.3. EJEMPLO 3

APLICACIÓN DE MEDIDA COMPENSATORIA:

Ámbito de aplicación	op.acc.6 mecanismtos de autenticación (usuarios de la organización)
Limitaciones o restricciones	En la actualidad, la ENTIDAD no puede abordar las acciones necesarias para implantar un doble factor de autenticación (2FA en adelante) en el acceso a través de la VPN
Objetivo	El implantar un 2FA tiene como objetivo reforzar la seguridad en el acceso de los usuarios al sistema, requiriendo dos factores de autenticación distintos. De este modo, si un atacante llegara a tener el identificador y la contraseña de un usuario de la ENTIDAD, necesitaría hacerse con el segundo factor de autenticación para tener éxito en su acceso. La medida compensatoria adoptada tiene como objetivo aumentar la seguridad en el acceso al sistema, haciendo necesario, no sólo el identificador y la contraseña del usuario, sino que además el acceso deba realizarse desde un dispositivo de la ENTIDAD, los cuales están todos identificados por su dirección MAC e incluidos en una lista blanca.
Riesgo identificado	La ausencia de un 2FA facilita que un atacante pueda acceder a los servicios de la ENTIDAD simplemente obteniendo un identificador de usuario de la ENTIDAD y consiguiendo descifrar su contraseña. Para mitigar este riesgo, se adopta la medida compensatoria descrita, que requiere realizar el acceso con los dispositivos autorizados en la lista blanca de la institución.
Definición de las medida compensatoria	En el firewall de la institución, se ha creado una política de grupo en la que se incluirán todos los dispositivos asignados a los empleados de la ENTIDAD tanto equipos de puesto de usuario como terminales móviles. En esta lista se identifica a los equipos según su dirección MAC, por lo que habrá que tener en cuenta que, para cada equipo, se deberán añadir tanto la MAC de su conexión cableada como la MAC de su conexión inalámbrica.
Validación de la medida compensatoria	Se revisará periódicamente por el responsable de seguridad y el responsable de sistemas que sólo se han producido accesos de los dispositivos autorizados, bloqueándose el intento de acceso desde otros dispositivos.
Mantenimiento	Verificar periódicamente la actualización de la lista blanca con los dispositivos autorizados

MEDIDAS DE VIGILANCIA

Junta de Andalucía

5.4. EJEMPLO 4

SUPUESTO DE HECHO:
Medida de control: op.mon.3 vigilancia op.pl.5 componentes certificados

Requisitos
- Disponer de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos: un SIEM, paneles de control de monitorización de eventos en soluciones Cloud, etc.

<u>Situación: la entidad no dispone de un SIEM incluido en el catálogo de productos certificados de la Guía CCN-STIC 105</u>

Junta de Andalucía

5.4. EJEMPLO 4

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Está buscando estos filtros:

Documento: 140 x

Total: 9 documentos Mostrar: 20 Pág. 1 de 1

Documento	Categoría	Publicado desde	Actualizado desde
CCN-STIC-140 Taxonomia de referencia para productos de Seguridad TIC	100 Procedimientos	Nov 2017	Sep 2023

Anexos:

Control de acceso

- Anexo A.1: Dispositivos de Control de Acceso a Red
- Anexo A.1M: Dispositivos de Control de Acceso a Red
- Anexo A.2: Dispositivos Biométricos
- Anexo A.3: Dispositivos Single Sign-On

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC –
Anexo B.6: Sistemas de gestión de eventos de seguridad

Junta de Andalucía

5.4. EJEMPLO 4

APLICACIÓN DE MEDIDA COMPENSATORIA:

Ámbito de aplicación	Op.mon.3 Vigilancia; Op.pl5 Componentes certificados
Limitaciones o restricciones	Se dispone de un sistema automático de recolección de eventos de seguridad que permite la correlación de los mismos, así cómo también permite determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración. En este caso, el sistema utilizado se denomina XXX y no dispone de un nivel de certificación conforme al CPSTIC o Common Criteria.
Objetivo	El objetivo que se busca es servir de apoyo a la monitorización de la seguridad, de forma que se facilite el proceso de recopilar, analizar y cotejar, así como de salvaguardar la información sobre eventos de seguridad y anomalías que puedan indicar un compromiso de la seguridad en los sistemas. A través de la medida compensatoria propuesta, se busca que el SIEM en cuestión cumpla con los requisitos que debería cumplir cualquier herramienta de la misma categoría que esté certificada, de forma que se garantice un nivel de seguridad adecuado al nivel medio del ENS.
Riesgo identificado	• Acceso no autorizado de administrador: Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio. • Mecanismos criptográficos débiles: Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta. • Protocolos de comunicación no autorizados: Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto. • Actualización maliciosa: Un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto. • Actividades no detectadas: Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador. • Compromiso de la integridad del software/firmware: Un atacante puede intentar comprometer la integridad del producto a través de un software sin privilegios ejecutado en la misma plataforma en la que se ejecuta el producto • Compromiso de parámetros de seguridad críticos: Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos • Acceso no autorizado de usuario: Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio. • Compromiso de credenciales: Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.

Definición de las medidas compensatorias	• **El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos: Al inicio y finalización de las funciones de auditoría; Login y logout de usuarios registrados; Cambios en las credenciales de usuarios; Cambios en la configuración del producto [asignación: listado de cambios]. ; Eventos relativos a la funcionalidad del producto [asignación: listado de eventos].; Si el SISTEMA gestiona claves criptográficas, [selección: generación; importación; cambio; eliminación de claves criptográficas; ningún otro].**
	  ○ **De esta forma se evitarían los accesos no autorizados a la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.**
	  ○ **De esta forma se garantizaría la integridad de la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **A los registros de auditoría se aplicará la siguiente política de acceso: a) Lectura: usuarios autorizados. b) Modificación: ningún usuario. c) Borrado: [selección: solo administradores; ningún usuario]**
	  ○ **De esta forma se evitarían los accesos no autorizados a la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **El SISTEMA debe ser capaz de almacenar en sí mismo la información de auditoría generada y [selección: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].**
	  ○ **De esta forma se garantiza que no se produzca un compromiso de los parámetros de seguridad de la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **El SISTEMA deberá [selección: sobrescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.**
	  ○ **De esta forma se produzca una actualización maliciosa de la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **El SISTEMA deberá ser capaz de recibir, identificar e interpretar eventos procedentes de múltiples fuentes. Debe soportar, al menos, los protocolos: Syslog sobre TLS y SNMP (Simple Network Management Protocol). También debe ser suficientemente configurable para interpretar y normalizar información procedente de aplicaciones o herramientas propietarias.**
	  ○ **De esta forma se evitarían los compromisos de credenciales, de parámetros de seguridad críticos y la integridad del software/firmware de la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **Para la funcionalidad de análisis y correlación de eventos, el SISTEMA facilitará la creación de [selección: alarmas; notificaciones] en el caso de detectar potenciales riesgos para la seguridad.**
	  ○ **De esta forma se detectarían fácilmente los accesos no autorizados a la plataforma, así como los eventos de seguridad que comprometan la aplicación, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **Para la funcionalidad de análisis de eventos, el sistema deberá ser capaz de analizar los datos recolectados en función de reglas definidas, para identificar usos indebidos y actividades maliciosas, y registrar el resultado de los análisis.**
	  ○ **De esta forma se evitarían los accesos no autorizados, Protocolos de comunicación, Actualización maliciosa, Actividades no detectadas, Compromiso de la integridad del software/firmware, Compromiso de parámetros de seguridad críticos, Acceso no autorizado de usuario, Compromiso de credenciales a la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **Para la funcionalidad de análisis de eventos y correlación, el SISTEMA debe proteger los eventos almacenados de accesos, modificaciones y borrados no autorizados, así como prevenir la pérdida de eventos por el llenado del espacio de almacenamiento. Deben utilizarse técnicas criptográficas seguras.**
	  ○ **De esta forma se evitarían los mecanismos criptográficos débiles en la plataforma, alcanzándose un nivel de seguridad similar respecto de este riesgo garantizado a través de la certificación CPSTIC.**
	• **El SISTEMA deberá ser capaz de sellar los registros de auditoria con una fuente de tiempo fiable.**
	  ○ **De esta forma se evitarían protocolos de comunicación no autorizados.**
	
	De esta comprobación se dejará constancia a través del “Lista comprobación SIEM xxx”. Dicha lista se revisará al menos anualmente.

Validación de la medida compensatoria	Los registros que genere la herramienta SIEM deberán ser revisados mensualmente por el Resp de Seguridad para garantizar su correcto funcionamiento.
Mantenimiento	Anualmente el Comité de Seguridad verificará la idoneidad de las acciones compensatorias propuestas y analizará la eficacia de las mismas.

Junta de Andalucía

5.5. EJEMPLO 5. Medida complementaria de vigilancia

SUPUESTO DE HECHO:

Se cuenta con un producto de seguridad que no cumple con el op.pl.5 componentes certificados, pero es de un fabricante reputado (se entiende esto como incumplimiento parcial del requisito, no precisando medida compensatoria, pero si complementaria de vigilancia).

Se justifican las siguientes medidas complementarias de vigilancia:

- Acta del Comité de Seguridad incorporando la decisión de adquirir componentes certificados cuando se precise la renovación de los existentes.
- Incrementar la monitorización de los activos referenciados (productos de seguridad existentes y/o los activos sobre los cuales estos repercutan).
- Atención prioritaria a los avisos de CVE (Common Vulnerabilities and Exposures), así como de otras vulnerabilidades que puedan afectar a dichos activos notificadas por el CERT (CCN-Cert o INCIBE-Cert) o del propio fabricante.
- Priorizar el mantenimiento de los componentes involucrados, aplicando parches y actualizaciones de seguridad de forma más rápida.

EN EL CASO DE SI PRECISAR MEDIDA COMPENSATORIA (VER EJEMPLO 4), ESTAS MEDIDAS PUEDEN SER ADICIONALES A LA MEDIDA COMPENSATORIA ESTABLECIDA

6. CONCLUSIONES

Junta de Andalucía

6. Conclusiones

OBJETIVO DE LAS MEDIDAS COMPENSATORIAS Y/O COMPLEMENTARIAS DE VIGILANCIA

1.- **Mitigar Riesgos:** Brindar una alternativa viable para reducir la exposición a amenazas y vulnerabilidades cuando las medidas de seguridad preferidas no se pueden implementar. Esto ayuda a mantener el riesgo dentro de niveles aceptables para la organización.

2.- **Mantener la Conformidad:** Permitir a las organizaciones cumplir con los requisitos regulatorios, legales, y de estándares de la industria en situaciones donde las soluciones estándar no son viables, asegurando que aún puedan alcanzar o acercarse al cumplimiento normativo a través de otros medios.

3.- **Proteger los Activos de Información:** Salvaguardar la confidencialidad, integridad, y disponibilidad de la información crítica y los sistemas de la organización mediante la implementación de controles alternativos que proporcionen un nivel de seguridad comparable.

6. Conclusiones

OBJETIVO DE LAS MEDIDAS COMPENSATORIAS

4.- **Asegurar la Continuidad del Negocio:** Facilitar la continuidad de las operaciones comerciales al asegurar que los sistemas críticos y los datos permanezcan seguros y accesibles, incluso frente a restricciones que impidan la aplicación de medidas de seguridad óptimas.

5.- **Optimización de Recursos:** Ofrecer soluciones que permitan a la organización utilizar de manera más eficiente sus recursos limitados, equilibrando entre el coste de implementación de las medidas de seguridad y el nivel de protección alcanzado.

6.- **Flexibilidad y Adaptabilidad:** Proporcionar a las organizaciones la capacidad de adaptarse a entornos cambiantes y a emergentes amenazas de seguridad, ofreciendo opciones para ajustar su enfoque de seguridad conforme evolucionan sus necesidades y capacidades.

7. REFERENCIAS

7. Referencias

- BOE del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

- Guia de Seguridad TIC CCN-STIC 808. Verificación del cumplimiento

- Guia de Seguridad TIC CCN-STIC 819. Medidas compensatorias

8. RUEGOS Y PREGUNTAS

Junta de Andalucía


Junta de Andalucía