

1. Introducción

2. Los controles básicos de ciberseguridad (CBCS-2026)

3. Objetivos de la auditoría de los controles básicos de ciberseguridad

4. Alcance del trabajo de revisión

5. Metodología de trabajo

6. Bibliografía

Anexo 1 Por qué son importantes los controles básicos de ciberseguridad

Anexo 2 Ficha de revisión C.9.5: Centro de Operaciones de Ciberseguridad

Anexo 3 Los Centros de Operaciones de Ciberseguridad

Anexo 4 Comparabilidad entre los CBCS-2018 y los CBCS-2026

Anexo 5 Ejemplo de documento de inicio de la auditoría (DIA)

1. Introducción

En la *GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa* se destaca la importancia creciente que las cuestiones relacionadas con la ciberseguridad están adquiriendo en la gestión de las administraciones públicas y, en consecuencia, la atención creciente que los auditores públicos deben conceder a dicha materia. En la medida en que cada vez un mayor número de servicios públicos se presta on-line y la conectividad por internet se ha convertido en una característica esencial de todos los sistemas de información (contables, sanitarios, educativos, etc.) los auditores deben prestar cada vez más atención a las cuestiones relacionadas con la ciberseguridad.

A pesar del tiempo transcurrido desde la aprobación de dicha guía, en 2018, las afirmaciones anteriores no solo se mantienen plenamente vigentes, sino que la importancia de las razones para su publicación no ha cesado de aumentar, ya que los ciberataques dirigidos a las entidades públicas son cada vez más frecuentes, sofisticados y destructivos. En resumen, la ciberseguridad ha adquirido una importancia crítica para dichos entes y para los auditores de los OCEX.

Se señalan en la citada guía los distintos enfoques que los OCEX pueden adoptar a la hora de abordar una auditoría o una revisión de la ciberseguridad de los entes públicos. En síntesis, desde la perspectiva de un OCEX, se pueden adoptar tres enfoques principales:

- **La revisión de controles generales de tecnologías de la información (CGTI) en el marco de una auditoría financiera de cuentas anuales (o de elementos de las cuentas anuales) y/o de cumplimiento.**

Tal como se señala en el apartado 2.1 de la *GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información (CGTI) en un entorno de administración electrónica*, en estos casos “el **objetivo de la revisión** de los CGTI será obtener una seguridad razonable de que estos permiten y apoyan el funcionamiento continuo y apropiado del entorno de TI, **incluido el funcionamiento continuo y efectivo de los controles de procesamiento de la información** y la integridad de la información (es decir,

la completitud, exactitud y validez de la información) en el sistema de información de la entidad.”

Del mismo modo, este enfoque también podrá ser aplicado en auditorías operativas en las que la gestión auditada está sustentada fundamentalmente en sistemas informáticos y se plantean necesidades similares a las auditorías financieras y/o de cumplimiento.

El **alcance** de la revisión vendrá determinado por el auditor financiero respecto a su necesidad de obtener confianza sobre el funcionamiento efectivo de los CPI relevantes. Para ello se seguirá la metodología descrita en los apartados siguientes.

- **Auditoría de los CGTI como trabajo específico e independiente.**

También pueden utilizarse las GPF-OCEX 5330 a 5335 revisando los CGTI en su totalidad. Tal como se señala en el apartado 2.2 de la GPF-OCEX 5330, “los **objetivos** de una auditoría de los CGTI no integrada en una auditoría financiera, que también se puede denominar auditoría de seguridad de la información o auditoría de ciberseguridad, consisten en **auditar los controles de seguridad de acuerdo con los criterios establecidos en el ENS**, que se desarrollan en el apartado 14 de esta guía y en las GPF-OCEX 5331 a 5335. Todas las categorías de CGTI pueden ser relevantes según se establezca en el alcance de la auditoría.”

Aunque la metodología está basada en el ENS, **la finalidad de una auditoría de los CGTI no es replicar exactamente el ENS**. Si esta fuera la finalidad sería más práctico utilizar las guías CCN-STIC-802 y 808.

- **Revisión de los controles básicos de ciberseguridad**

La realización de auditorías de los CGTI como trabajo específico e independiente entraña una intensa dedicación de personal especializado tanto para el auditor como para el ente auditado, muy costoso en términos de tiempo de dedicación. Es por ello por lo que se plantea la revisión de los controles básicos de ciberseguridad.

Los controles básicos de ciberseguridad (CBCS) **son un subconjunto reducido** de los controles de ciberseguridad establecidos en el ENS y en las GPF-OCEX 5330-5335. Por esta razón, **un informe sobre la revisión de los CBCS no tiene el valor de auditoría que verifique el cumplimiento de los requisitos del ENS**, a la que se refiere el artículo 31.1 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS. Es decir, **no** es una certificación del ENS.

Su revisión permite formar una idea general de la situación en la entidad revisada y no requerirá la dedicación de excesivos recursos especializados, ni del auditor externo, ni del ente auditado en comparación con una auditoría generalizada de los CGTI. Además, será un trabajo más viable en entes que no dispongan de muchos recursos técnicos o humanos.

En 2018 se aprobó la *GPF-OCEX 5313 Revisión de los controles básicos de ciberseguridad*, (CBCS-2018 en adelante) con la finalidad de abordar este enfoque más simplificado, pero significativo, para revisar la ciberseguridad por parte de los OCEX.

Aunque el objetivo general y el planteamiento de los CBCS-2018 siguen plenamente vigentes, dado el tiempo transcurrido, existen diversas **circunstancias que motivan su actualización** y la reformulación de los CBCS-2026. Estas son:

- La actualización del ENS en el año 2022 mediante el Real Decreto 311/2022, de 3 de mayo.
- Como consecuencia de ello, en 2023 y 2024, se actualizaron las siguientes guías de revisión de los CGTI:
 - GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría
 - GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información en un entorno de administración electrónica
 - GPF-OCEX 5331 Gobernanza corporativa, gobernanza de las TI y su auditoría
 - GPF-OCEX 5332 Revisión de los CGTI del área B. Gestión de cambios en aplicaciones y sistemas
 - GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información
 - GPF-OCEX 5334 Revisión de los CGTI del área D. Controles de acceso a datos y programas
 - GPF-OCEX 5335 Revisión de los CGTI del área E. Continuidad del servicio.

Dado que los controles básicos de ciberseguridad son un subconjunto priorizado de los CGTI, es necesario actualizar la GPF-OCEX 5313 para mantener la coherencia entre las GPF-OCEX y su alineación con el ENS.

- La experiencia adquirida por los OCEX en los trabajos realizados desde el año 2018, que ha permitido identificar aquellos controles con mayor impacto en el nivel de ciberseguridad general. Esta experiencia ha permitido actualizar parcialmente algunos de los CBCS, tal como se explica en el siguiente apartado.
- El contexto de la ciberseguridad actual en el ámbito de las administraciones públicas, con ataques perpetrados a instituciones que han sufrido la paralización completa de los servicios prestados durante semanas e incluso meses, generando un gran impacto en el ciudadano, aconseja priorizar los controles relacionados con la disponibilidad y resiliencia de los servicios esenciales proporcionados por las entidades públicas al ciudadano en el diseño de los CBCS-2026.

2. Los controles básicos de ciberseguridad (CBCS-2026)

El desarrollo de esta GPF-OCEX 5313 se basa en la selección de un subconjunto de controles y metodologías de revisión que se encuentran recogidos, con el máximo detalle, en las guías de fiscalización *GPF-OCEX 5330 a 5335 y 5314*. **Los CBCS son, en definitiva, un subconjunto priorizado de los CGTI.**

Este conjunto de CBCS constituye una propuesta de mínimos que, tal y como se indica en el apartado 4. *Alcance del trabajo* de esta guía, el auditor deberá validar para cada uno de los trabajos. El auditor deberá, en función de los objetivos de la auditoría, reformular los controles a analizar, añadiendo si corresponde a los CBCS los controles o subcontroles adecuados.

Tal como se indica en la GPF-OCEX 5330, los controles descritos en esta guía están alineados con el ENS, que es de aplicación obligatoria en el sector público, y esta alineación facilita la realización de las auditorías de ciberseguridad y coadyuva a la implantación del ENS. La presente guía no modifica los controles incluidos en la GPF-OCEX 5330 (excepto en el caso que más adelante se indica) ni los procedimientos para su revisión, y se mantiene la coherencia con el ENS.

Coherencia CGTI/CBCS con el ENS

Se debe entender que esta “coherencia” con el ENS no se materializa de forma que la auditoría de los CGTI y/o CBCS permita sustituir o reemplazar los resultados de una auditoría completa del ENS.

Conviene dejar claro que una auditoría de seguridad del ENS y las auditorías de los CGTI/CBCS presentan las siguientes diferencias:

- **El objetivo.**

En las auditorías del ENS el objetivo es certificar que en el ente auditado existen las condiciones necesarias para garantizar adecuadamente la seguridad de los servicios prestados a la ciudadanía y de la información tratada, y se cumplen las cinco dimensiones de la seguridad.

El objetivo de una revisión de los CGTI, es obtener una seguridad razonable de que estos permiten y apoyan el funcionamiento continuo y apropiado del entorno de TI, incluido el funcionamiento continuo y efectivo de los controles de procesamiento de la información y la integridad de la información (es decir, la completitud, exactitud y validez de la información) en el sistema de información de la entidad.

Por su parte, el objetivo de la revisión de los CBCS es concluir sobre si el nivel de madurez de los controles revisados es el adecuado a las características y categoría de seguridad de la entidad auditada.

- **Alcance de la auditoría.**

En las auditorías del ENS el **alcance, entendido como los sistemas a incluir en la auditoría**, viene fijado por la normativa, mientras que en las auditorías de los CGTI/CBCS el alcance lo fija el auditor en función de los objetivos y necesidades de la auditoría.

Del mismo modo, **el conjunto de los controles que serán revisados**, en las auditorías del ENS viene fijado en la propia normativa, en función de la categorización del sistema y las condiciones específicas de la entidad. En las auditorías de CGTI/CBCS es el auditor, en función de los objetivos y necesidades de la auditoría el que establece qué controles serán revisados.

- Paralelamente, **el enfoque establecido en los CGTI/CBCS prioriza ciertas medidas de seguridad frente a otras**. Esto hace que medidas de seguridad que el ENS puede no exigir para sistemas de categoría básica o media, en las auditorías de CGTI/CBCS sí que se considere necesario que se encuentren implantadas (por ejemplo, las asociadas a garantizar la continuidad y resiliencia).

Del mismo modo, para una medida de seguridad, los requisitos para considerarla adecuada en una revisión de los CGTI/CBCS pueden diferir ligeramente, de los establecidos en la normativa, priorizando los distintos requisitos fijados en el ENS.

Sin embargo, una vez presentadas las diferencias conviene destacar que, en esencia, **los CGTI/CBCS están alineados con el ENS**. Los objetivos de control que persiguen ambos enfoques son los mismos, y las medidas de seguridad propuestas son en su práctica totalidad las mismas, estando identificadas en las guías 533X la casuística concreta en la que hay alguna diferencia.

De esta forma, el enfoque común que comparte la metodología para realizar revisiones de CGTI/CBCS y el ENS permite:

- Facilitar la comunicación con el fiscalizado, dado que no es necesario verificar controles no recogidos en la norma que les es de aplicación.
- Reforzar el apoyo al cumplimiento del ENS.

Paralelamente, la actualización de los CBCS de 2026 mantiene la máxima compatibilidad con la versión de los CBCS-2018, lo que permite realizar el seguimiento de los CBCS de entidades auditadas y analizar su evolución en el tiempo, con las consideraciones que se realizan más adelante.

Cambios en los CBCS-2026 respecto de los CBCS-2018

Los cambios introducidos en esta GPF-OCEX 5313 (2026) son los siguientes:

- **Reorganización de los CBCS y sus subcontroles, que pasan de ocho a seis**, con objeto de agrupar los subcontroles existentes en la GPF-OCEX 5313 (2018) en áreas de control más coherentes con los objetivos de control identificados y en línea con la **propuesta** de agrupación de controles proporcionada por el **Center for Internet Security¹ en seis componentes de “sentido común”**, adaptada a la realidad de nuestro sector público.
- Los CBCS 1 y 2 de la GPF-OCEX 5313 (2018) se han unido ahora en el **CBCS 1 Inventario y control de activos**. En la práctica las medidas de seguridad relacionadas con los inventarios físicos y lógicos se gestionan de forma cuasi unificada, muchas veces con las mismas herramientas, y su auditoría se puede realizar de forma simultánea. En el ENS se corresponde con una única medida de seguridad, la *op.exp.1.1*.
- El nuevo **CBCS 2 Seguridad de los activos** se corresponde con los anteriores **CBCS 3 y 5**. Se han unificado en un solo CBCS con objeto de agrupar el conjunto de medidas que tienen un impacto en el nivel de seguridad individual de los activos y que, en general, suelen compartir la gestión o parte de ella. Este control incluye la gestión de vulnerabilidades y de configuraciones, y se ha reforzado con un nuevo subcontrol, el CGTI C3.3 Mantenimiento.
- El nuevo **CBCS 3 Gestión de usuarios y privilegios (de administración)** se corresponde con el CBCS 4 de la GPF-OCEX 5313 (2018) pero se ha ampliado su alcance, con subcontroles correspondientes a la gestión de usuarios, por dos motivos principales: de manera general, la gestión de usuarios “ordinarios” y de usuarios administradores disponen de medidas o procesos comunes, como la identificación o la autenticación o la gestión de cuentas, por lo que su revisión se realiza de manera simultánea; además, la gestión de usuarios funcionales y sus derechos de acceso es un control imprescindible en cualquier auditoría financiera o

¹ Ver APPENDIX G. CIS Critical Security Controls Grouped as Common-Sense Components. A Guide to Defining Reasonable Cybersecurity Version 1.1.

de cumplimiento que incluya la revisión de los CGTI, por lo que su revisión resulta de especial interés.

- Se modifica el anterior CBCS 6 Registro de la actividad de los usuarios, considerado inicialmente para la identificación de incidentes de seguridad mediante el análisis a posteriori de registros (*logs*) de actividad, que es sustituido por el control **CBCS 4 Monitorización y respuesta**.

Se amplía el objetivo de control – anteriormente limitado a la activación almacenamiento de *logs* y registros de actividad- para considerar el conjunto de procesos, medios y herramientas que permitan la monitorización continuada del estado de la seguridad y la detección de incidentes, así como el conjunto de planes, procedimientos y medios que, en caso de detección de incidentes, permitan una respuesta organizada al mismo para minimizar su impacto.

Además, con objeto de adecuar el control al contexto actual en materia de ciberseguridad, se añade un nuevo subcontrol, no incluido en la GPF-OCEX 5330 y que se codifica como **C.9.5: Centro de Operaciones de Ciberseguridad**. Se incluye en el anexo 2 la ficha para la revisión de este subcontrol, que también se incluirá en la GPF-OCEX 5333.

Los centros de operaciones de ciberseguridad (SOC), se definen² como un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad a su comunidad, se han constituido en los últimos años como una de las herramientas más efectivas adoptadas por las entidades públicas³. Además, su implantación y explotación se encuentra impulsada por el CCN-CERT mediante la creación de la Red Nacional de SOC, que permite la federación de los SOC del territorio nacional, optimizando los recursos disponibles y maximizando su capacidad de detección y respuesta.

- Se modifica el control CBCS 7 Copias de seguridad de datos y sistemas, considerado para analizar los procesos y herramientas para realizar la copia de seguridad de la información crítica que permita la recuperación de la información en tiempo oportuno, que es sustituido por el control **CBCS 5 Continuidad y resiliencia**.

Dado el creciente aumento de incidentes de seguridad en sistemas de información de entidades del sector público que han conllevado, en algunos casos, la indisponibilidad absoluta de los servicios prestados al ciudadano y de procesos administrativos internos durante un periodo de tiempo inaceptable, resulta aconsejable enfatizar la consideración de la disponibilidad en el CBCS 5 de los CBCS-2026.

En este sentido, se refuerza y amplía el objetivo de control para, además de asegurar la realización de las copias de seguridad, considerar la gestión sistemática del proceso de recuperación de los servicios críticos de la entidad, incluyendo los medios materiales y los recursos organizativos necesarios.

² Los conceptos relativos a los SOC recogidos en esta guía están basados en la información publicada por el Centro Criptológico Nacional (CCN) en su [página web sobre la Red Nacional de SOC](#) y particularmente en el documento [Centros de operaciones de ciberseguridad \(SOC\) y Red Nacional de SOC \(RNS\)](#).

³ En los últimos años se han desarrollado en el sector local, como consecuencia de algunos de los proyectos promovidos por el Plan de Recuperación, Transformación y Resiliencia (PRTR).

- El CBCS 8 Cumplimiento de la legalidad, de la GPF-OCEX 5313 (2018), se reajusta para hacerlo coherente con la GPF-OCEX 5330 y la GPF-OCEX 5314, y se redenomina **CBCS 6 Gobernanza de la ciberseguridad**, que incluye los controles A.2: Cumplimiento normativo (Anexo GPF-OCEX 5314, apartado 5. Cumplimiento legal) y A.3: Gobernanza de la ciberseguridad (Anexo GPF-OCEX 5314, apartados 1 a 4, 6 y 7). Se ha eliminado la verificación del cumplimiento de la ley de factura electrónica por considerar que en estos momentos no tiene relevancia a efectos de la ciberseguridad.

Sin duda una auditoría completa de los CGTI, de las previstas en el apartado 2.2 de la GPF-OCEX 5330, o una auditoría siguiendo el ENS⁴, proporcionará una mayor seguridad sobre la situación del ente auditado frente a las ciberamenazas y su nivel de ciber-resiliencia. Pero, como ya se ha señalado, el esfuerzo requerido en la ejecución de trabajos con ese amplio alcance limita su aplicación en la práctica.

Por esta razón, una alternativa con mejor relación coste/beneficio consiste en diseñar un plan de trabajo basado en los seis CBCS-2026, criterio que recoge esta guía.

Tal y como se ha indicado anteriormente, los CBCS-2026 se han rediseñado considerando la agrupación de subcontroles de la GPF-OCEX 5330 en áreas de control más coherentes con los objetivos de control identificados. La Tabla 1 recoge la nueva estructura de los CBCS-2026.

En el anexo 4 se incluye una tabla con la correspondencia entre los CBCS-2018 y los CBCS-2026 para poder elaborar **informes comparativos** con los resultados obtenidos en años anteriores.

3. Objetivos de la auditoría de los controles básicos de ciberseguridad

El objetivo de la auditoría de los CBCS-2026 es determinar si el nivel de madurez de los controles revisados es el adecuado a las características y categoría de seguridad de la entidad auditada. La revisión de los controles CBCS proporciona una **evaluación sobre su diseño, implementación y la eficacia operativa** y permite:

- La identificación de deficiencias de control que puedan afectar negativamente a la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los datos, la información y los activos de la entidad.
- La identificación de incumplimientos normativos relacionados con la ciberseguridad.

Dado el carácter limitado de la revisión, el objetivo no es emitir una opinión de seguridad razonable sobre la confianza que merece el conjunto del entorno de control TI existente. En este sentido, un resultado satisfactorio en la revisión de los CBCS no garantiza la seguridad de los sistemas de la entidad frente a ataques o incidentes.

⁴ De acuerdo con la *Guía de auditoría del ENS CCN-STIC-802*.

Tabla 1. Estructura de los controles básicos de ciberseguridad

Control		Objetivo de control	Ref.	Subcontroles de los CBCS/CGTI
CBCS 1	Inventario y control de activos	Gestionar activamente todos los activos hardware y software en la entidad, posibilitando la aplicación de controles posteriores a dichos activos.	5333	C.1.1: Inventario de activos físicos autorizados
				C.1.2: Inventario de activos SW
				C.1.3: Control de HW no autorizados
				C.1.4: Control de SW no autorizados
CBCS 2	Seguridad de los activos	Gestionar activamente la configuración, el estado de la seguridad y las medidas aplicadas a los activos de la entidad.	5333	C.2.1: Gestión de vulnerabilidades
				C.2.2: Parcheo
				C.2.3: SW soportado por el fabricante
				C.3.1: Configuración de seguridad
CBCS 3	Gestión de usuarios y privilegios de administración	Disponer de un proceso de gestión de usuarios de la entidad, su identificación, autenticación y la asignación de derechos de acceso, particularmente para los administradores de los sistemas.	5334	C.3.2: Gestión y mantenimiento de la configuración de seguridad
				D.1.1: Inventario y control de cuentas de administración
				D.1.2: Uso dedicado de cuentas de administración
				D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización
				D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos
				D.2.1: Procedimiento de gestión de usuarios
				D.2.2: Identificación
CBCS 4	Monitorización y respuesta	Disponer de procesos y herramientas que permitan la monitorización activa de eventos de seguridad y la gestión de la respuesta en caso de materialización de las amenazas.	5333	D.2.5: Gestión de derechos de acceso
				C.4.4: Centralización y revisión de logs
				C.9.3: Vigilancia
				C.9.4: Monitorización y correlación
				C.9.5: Centro de Operaciones de Ciberseguridad
CBCS 5	Continuidad y resiliencia	Disponer del conjunto de planes, procedimientos y herramientas que, en caso de incidente de seguridad, permitan la recuperación de los sistemas en tiempo y forma adecuados para limitar el impacto en el servicio hasta un nivel aceptable.	5335	C.8.1: Procedimiento, notificación, detección y respuesta de incidentes
				E.1.1: Realización de copias de seguridad
				E.1.2: Realización de pruebas de recuperación
				E.1.3: Protección de las copias de seguridad
				E.2.1: Identificación de elementos críticos del negocio
				E.2.2: Plan de recuperación de desastres (DRP). Pruebas.
CBCS 6	Gobernanza de la ciberseguridad	Disponer de un conjunto de responsabilidades y actividades que tienen como finalidad proporcionar una dirección estratégica en materia de seguridad y garanticen la consecución de los objetivos establecidos.	5314	E.2.3: Plan de continuidad. Pruebas.
				A.2: Cumplimiento normativo. (Anexo GPF-OCEX 5314, apartado 5. Cumplimiento legal)
				A.3: Gobernanza de la ciberseguridad. (Anexo GPF-OCEX 5314, apartados 1 a 4, 6 y 7)

Los procedimientos realizados en una auditoría de seguridad limitada son reducidos en comparación con los que se requieren para obtener una seguridad razonable, pero se espera que **el nivel de seguridad sea, conforme al juicio profesional del auditor, significativo para los destinatarios del informe**⁵. En este sentido, la auditoría de los CBCS-2026 proporcionará información relevante sobre el grado de ciberseguridad y ciber-resiliencia de la entidad y sobre posibles acciones de mejora aconsejables.

De acuerdo con la ISSAI-ES 100, un informe de seguridad limitada transmitirá el carácter limitado de la seguridad dada.

Valoración del nivel de madurez

El cálculo del nivel de madurez de los controles se realiza, tal y como se indica en la GPF-OCEX 5330, siguiendo el modelo propuesto por el ENS.

Para calcular el nivel de madurez de los CBCS, y de otros posibles controles revisados, será necesario realizar una valoración de la madurez de cada uno de los subcontroles y medidas que componen los controles, siendo la madurez de cada control la media ponderada de los subcontroles que lo constituyen. La valoración de los subcontroles será incluida o no en los informes según el criterio del auditor, dependiendo de los objetivos de la auditoría y especialmente de la sensibilidad de las medidas revisadas, evitando generar situaciones de riesgo por exposición pública de las deficiencias de control de la entidad auditada.

4. Alcance del trabajo

Dada la naturaleza del objeto material a revisar, los sistemas de información de un ente público, y su gran amplitud y diversidad, es necesario concretar qué sistemas en particular van a revisarse. Por tanto, **en la planificación de cada trabajo de revisión de los controles básicos de ciberseguridad se definirá el alcance concreto** de acuerdo con los objetivos fijados.

A la hora de seleccionar los sistemas a revisar podrán adoptarse distintos enfoques, dependiendo, fundamentalmente, de si la revisión de ciberseguridad está enmarcada en el ámbito de una auditoría financiera, de un proceso en concreto o de una auditoría operativa o si, por el contrario, se trata de una auditoría horizontal de ciberseguridad.

Atendiendo a lo anterior, los criterios generales para definir el alcance serán los siguientes:

- a) En el contexto de una auditoría financiera y/o de cumplimiento, es decir la revisión de los CBCS-2026 se realiza en el marco de una auditoría financiera o de cumplimiento, se seleccionarán:
 - Los sistemas que sustentan los procesos de gestión más relevantes desde el punto de vista de las necesidades del control externo de las cuentas públicas (por ejemplo: contabilidad, personal-nóminas, compras, gestión de ingresos).
 - Una muestra de sistemas que, sin dar soporte específico a los procesos de gestión, son elementos críticos del entorno de TI de cualquier ente.
- b) En el marco de una auditoría de un proceso específico o una auditoría operativa, se seleccionarán:

⁵ ISSI-ES 100, apartado 21.

- Los sistemas directamente relacionados con la actividad auditada (por ejemplo, en un hospital las aplicaciones de gestión de historias médicas, de asistencia médica, etc.; en un ayuntamiento la gestión tributaria, el padrón, etc. en una universidad las matrículas, los expedientes académicos, etc.)
 - Una muestra de sistemas que, sin dar soporte específico a los procesos de gestión, son elementos críticos del entorno de TI de cualquier ente.
- c) En el caso de una auditoría horizontal específica sobre ciberseguridad, que será el caso más frecuente, se seleccionarán:
- Los sistemas que se espera que tengan todos los entes a revisar, con objeto de poder realizar análisis comparativos. Por ejemplo, en caso de ayuntamientos, se pueden seleccionar contabilidad y recaudación.
 - Una muestra de sistemas que, sin dar soporte específico a los procesos de gestión, son elementos críticos del entorno de TI de cualquier ente.

Para los distintos procesos de gestión seleccionados en cada caso, la revisión debe incluir **necesariamente** los controles relacionados con:

- la aplicación informática de gestión
- la base de datos subyacente
- los sistemas operativos instalados en cada uno de los sistemas que soportan la aplicación de gestión (ej. servidores web, de aplicación, de base de datos).

Y para la muestra de los sistemas de información no específicos de un determinado proceso de gestión, sino que forman parte de la infraestructura TI general, que da servicio a todos los procesos de gestión de una entidad, se considerarán los siguientes tipos de elementos:

- controlador de dominio
- software de virtualización
- equipos de usuario
- elementos de la red de comunicaciones (ej. router, switches, punto de acceso a red wifi, etc.)
- elementos de seguridad (ej: firewall, IPS, proxy de correo, proxy de navegación, servidores de autenticación, infraestructura de generación de certificados, etc.)

Del mismo modo que son seleccionados los sistemas a revisar durante la planificación del trabajo, se deben concretar los controles a revisar. Para cada trabajo el **auditor debe**, en función de los objetivos y necesidades de la auditoría, **establecer qué controles** serán evaluados.

Los **CBCS constituyen una propuesta de mínimos** que de manera general serán adecuados para satisfacer los objetivos del trabajo. No obstante, el auditor debe, **para cada uno de los trabajos** a realizar, **confirmar la idoneidad de** los controles propuestos por **los CBCS**, y/o **reformular el conjunto de** controles y subcontroles a revisar en caso de que lo considere necesario para cumplir con los objetivos de la auditoría. Los criterios que deberá considerar para la selección de controles serán:

- La categoría, conforme al ENS, de los sistemas involucrados en el trabajo de auditoría. Particularmente para los sistemas de categoría ALTA, de manera que se aborden riesgos que tengan un impacto muy grave sobre los activos de la organización, sobre algún individuo o sobre la capacidad de la organización para desarrollar eficazmente sus funciones y competencias
- Los riesgos identificados derivados de la utilización de las TI, particularmente tras adquirir el conocimiento necesario sobre la entidad y su entorno de control.

A modo de ejemplo, exponemos la siguiente situación:

“En el contexto de una auditoría de sistemas de la aplicación económico-financiera de reciente implantación en una entidad, se incluyen inicialmente los CBCS en la definición del alcance del trabajo. Pero al iniciar los trabajos y tras alcanzar un conocimiento de la entidad y su entorno, se identifica que la entidad ha realizado la migración de la aplicación contable a una versión más actualizada, proceso con una dificultad técnica intrínseca y sujeto a riesgos que pueden afectar a la integridad de la información contable. En esta situación, el auditor deberá incluir en su trabajo la revisión de los controles B.3.1 Procedimientos para la gestión de cambios y B.3.2: Responsabilidades para la gestión de cambios de aplicaciones o sistemas.”

A modo de resumen, destacar que, en función del tipo de auditoría y el nivel de profundidad de la revisión, se definirá el alcance concreto del trabajo, que **deberá quedar claramente documentado en los papeles de trabajo y reflejado en el informe resultante.**

5. Metodología de trabajo

Tal y como se ha indicado, los CBCS-2026 son un subconjunto priorizado de subcontroles CGTI, por lo que su revisión y la metodología y los procedimientos a utilizar, se encuentran ampliamente detallados en la GPF-OCEX 5330 y siguientes.

Para revisar los CBCS-2026 se utilizarán las fichas de revisión incluidas en las GPF-OCEX 5333 a 5335 y en la GPF-OCEX 5314, tal como se indica a continuación:

- GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información.
Aplicable para los **CBCS 1, 2 y 4.**

En el caso del CBCS 4 se utilizará la ficha de revisión adicional, la C.9.5: Centro de Operaciones de Ciberseguridad, incluida en esta guía. Este subcontrol no se encuentra incluido en la guía GPF-OCEX 5330, pero será incorporado al aprobarse la presente guía.
- GPF-OCEX 5334 Revisión de los CGTI del área D. Controles de acceso a datos y programas.
Aplicable para el **CBCS 3.**
- GPF-OCEX 5335 Revisión de los CGTI del área E. Continuidad del servicio.
Aplicable para el **CBCS 5.**
- GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría.
Aplicable para el **CBCS 6.**

En general la metodología de trabajo será la establecida en la GPF-OCEX 5330. En particular, los apartados

10. Evaluación del diseño e implementación (D+I) de los CGTI relevantes
11. Revisión de la eficacia operativa de los CGTI relevantes
16. Evaluación de las deficiencias de control interno detectadas
17. Importancia relativa de las deficiencias de control a efectos de la auditoría
18. Recomendaciones

Al iniciar el trabajo se enviará un **documento de inicio de la auditoría (DIA)**. En el anexo 5 se incluye un ejemplo de DIA que en cada OCEX se adaptará al modelo que se tenga oficialmente aprobado y a las circunstancias del trabajo. Este DIA ejemplo incluye a su vez varios anexos, entre los cuales:

- Dos anexos, 1 y 2, informativos sobre los CBCS.
- Una tabla/cuestionario que debe cumplimentar el auditado (anexo 3).
- Una tabla para documentar el conocimiento del entorno TI (anexo 4).

6. Bibliografía

- [Centro Criptológico Nacional](#):
 - Guía CCN-STIC-802, ENS. Guía de auditorías de cumplimiento, Junio 2025.
 - Guía CCN-STIC-808, ENS. Verificación del cumplimiento, Junio 2025.
- [Código de Derecho de la Ciberseguridad](#), BOE, abril 2025.
- [Esquema Nacional de Seguridad](#). Real Decreto 311/2022, de 3 de mayo.
- [GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa](#).
- [GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría](#), 19/10/2023.
- [GPF-OCEX 5330 Revisión de los controles generales de tecnologías de información \(CGTI\) en un entorno de administración electrónica](#), 26/06/2024.
 - GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información.
 - GPF-OCEX 5334 Revisión de los CGTI del área D. Controles de acceso a datos y programas.
 - GPF-OCEX 5335 Revisión de los CGTI del área E. Continuidad del servicio.
- [The Center for Internet Security](#):
 - [A Guide to Defining Reasonable Cybersecurity Version 1.1](#), 2024.
 - CIS Critical Security Controls Version 8.1, 2024.
- [Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información](#).

Anexo 1. Por qué son importantes los controles básicos de ciberseguridad (CBCS)

CBCS 1 Inventario y control de activos

Objetivo de control: Gestionar activamente todos los dispositivos hardware y software en la entidad, posibilitando la aplicación de controles posteriores a dichos activos.

Los atacantes, que pueden estar ubicados en cualquier parte del mundo, están escaneando continuamente las redes de las organizaciones objetivo, esperando que nuevos y desprotegidos sistemas se incorporen a esas redes, buscando versiones vulnerables de hardware y software que puedan explotarse remotamente.

Buscan dispositivos, como los portátiles, que se conectan y desconectan de las redes corporativas, y es más probable que no dispongan de los últimos parches y actualizaciones de seguridad, aprovechando el lapso transcurrido hasta su actualización.

Es más probable que las máquinas mal controladas estén ejecutando software que no sea necesario para los fines de la entidad (introduciendo posibles fallos de seguridad), o ejecutando malware introducido por un atacante después de que un sistema haya sido comprometido.

Una vez que una máquina ha sido comprometida, los atacantes la utilizan a menudo como punto para recoger información sensible del sistema en el que está integrada y de otros sistemas conectados a él. Además, las máquinas comprometidas se utilizan como punto de lanzamiento para el movimiento a través de la red y de las redes conectadas. De esta manera, los atacantes pueden rápidamente convertir una máquina comprometida en muchas.

Este control permite a las organizaciones definir la base de activos que es necesario defender. Sin conocer qué dispositivos están conectados, no pueden ser defendidos.

El inventario debe ser tan completo como sea posible: en organizaciones con un nivel de madurez básico el inventario puede ser realizado y mantenido con procedimientos manuales y, en otras más maduras, utilizando herramientas de escaneo (tanto activos como pasivos) que detecten los dispositivos conectados a la red corporativa y agentes que permitan la detección del software instalado en los activos hardware.

El conocimiento de los activos existentes en la red permite, mediante la comparación con el listado de activos autorizados, identificar aquellos que no forman parte de la organización, incluyendo tanto los activos hardware como los activos software. Una vez identificados los activos no autorizados es posible aplicar controles y medidas que impidan su acceso a la red corporativa, en el caso de los activos hardware, y la ejecución únicamente de aplicaciones contenidas en la lista blanca, en el caso de los activos software. Limitar el acceso o la ejecución únicamente a aquellos activos que se encuentran controlados permite asegurar que todos los activos individuales disponen de las medidas de seguridad y de las configuraciones necesarias, limitando la superficie de exposición.

Además, disponer de un inventario actualizado de activos permite aplicar sobre todos ellos controles posteriores que posibilitan alcanzar el nivel de seguridad individual requerido.

Referencias

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

- C.1.1: Inventario de activos físicos autorizados
- C.1.2: Inventario de activos SW
- C.1.3: Control de HW no autorizados
- C.1.4: Control de SW no autorizados

CBCS 2 Seguridad de los activos

Objetivo de control: Gestionar activamente la configuración, el estado de la seguridad y las medidas aplicadas a los activos de la entidad.

Los ciberdefensores deben operar en un flujo constante de información nueva: actualizaciones de software, parches, avisos de seguridad, boletines de amenazas, etc. La comprensión y gestión de las vulnerabilidades se ha convertido en una actividad continua, que requiere tiempo, atención y recursos significativos.

Los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre la aparición de nuevos conocimientos y la remediación. Por ejemplo, cuando los investigadores reportan nuevas vulnerabilidades, comienza una carrera entre todas las partes, incluyendo: atacantes (para "armarse", desplegar un ataque, y explotarlo); proveedores (para desarrollar, implementar parches o firmas y actualizaciones), y defensores (para evaluar riesgos, parches de prueba, e instalarlos).

Las organizaciones que no escanean las vulnerabilidades y abordan de forma proactiva los defectos encontrados se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos. Los defensores se enfrentan a desafíos particulares en cuanto a escalar el remedio en toda una entidad, y priorizar las acciones con conflictos de prioridades y, a veces, efectos secundarios inciertos.

Además, la seguridad de los activos se complementa con una configuración adecuada, que minimice o elimine posibles vulnerabilidades. Sin embargo, fabricantes y vendedores entregan sus productos sin esta consideración. Las configuraciones predeterminadas para los sistemas operativos y las aplicaciones están normalmente orientadas a la facilidad de operación y a la facilidad de uso, no a la seguridad. Cuando se entrega un software es habitual encontrarse con controles poco robustos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos (vulnerables), preinstalación de software innecesario; todos estos aspectos son vulnerables en su estado predeterminado.

El desarrollo de opciones de configuración con buenas propiedades de seguridad es una tarea compleja más allá de la capacidad de los usuarios individuales, requiriendo análisis a veces complejos para tomar buenas decisiones.

Incluso si se desarrolla e instala una configuración inicial fuerte, debe ser revisada y actualizada continuamente para evitar el deterioro de la seguridad, en particular cuando el software es actualizado o parcheado, se divulgan las nuevas vulnerabilidades de la seguridad, o las configuraciones se "ajustan" para permitir la instalación de nuevo software o para dar soporte a nuevos requerimientos operacionales. Si no se revisa y actualiza de forma continua, los atacantes encontrarán oportunidades para explotar tanto los servicios accesibles a la red como el software cliente.

La finalidad de este control es asegurar que todos los activos autorizados de la entidad, incluyendo activos hardware y activos software, dispongan de manera individual de un nivel de seguridad adecuado, minimizando la superficie de exposición de las organizaciones y limitando la probabilidad de materialización de las amenazas.

La seguridad de activos depende principalmente de dos aspectos: la gestión del mantenimiento, las vulnerabilidades y el parcheo, por una parte, y la configuración segura por otra.

La gestión de vulnerabilidades tiene como objeto conocer y eliminar debilidades técnicas que existen en los sistemas de información de la organización, reduciendo la probabilidad de que los sistemas sigan siendo vulnerables. Las organizaciones implementan procesos de gestión y utilizan sistemas de administración de parches y actualizaciones que cubren vulnerabilidades tanto de sistemas operativos como aplicaciones de terceros.

En cuanto a la configuración de los sistemas, la mayoría de los sistemas están configurados por defecto para facilitar su uso y no necesariamente considerando criterios de seguridad. Para implantar este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad que minimicen la probabilidad de sufrir ataques mediante la explotación de configuraciones vulnerables.

Las organizaciones que no gestionan activamente las vulnerabilidades y configuraciones de los sistemas y abordan de forma proactiva los defectos encontrados, no minimizan la superficie de exposición frente a

las amenazas externas y se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos.

Referencias

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

- C.2.1: Gestión de vulnerabilidades
- C.2.2: Parcheo
- C.2.3: SW soportado por el fabricante
- C.3.1: Configuración de seguridad
- C.3.2: Gestión y mantenimiento de la configuración de seguridad

CBCS 3 Gestión de usuarios y privilegios (de administración)

Objetivo de control: Disponer de un proceso de gestión de usuarios de la entidad, su identificación, autenticación y la asignación de derechos de acceso, particularmente para los administradores de los sistemas.

El uso inadecuado de privilegios administrativos es un método primario para que los atacantes se propaguen dentro de una entidad objetivo. Dos técnicas de ataque muy comunes aprovechan los privilegios administrativos incontrolados.

En la primera, un usuario que opera como administrador de su equipo, abre un adjunto de correo electrónico malicioso, descarga y abre un archivo de un sitio web malicioso, o simplemente navega en un sitio web que aloja contenido del atacante que puede explotar automáticamente navegadores. El archivo o exploit contiene código ejecutable que se ejecuta en el equipo de la víctima ya sea automáticamente o engañando al usuario para que ejecute el contenido del atacante. Si la cuenta del usuario de la víctima tiene privilegios administrativos, el atacante puede apoderarse completamente de la máquina de la víctima e instalar los registradores de teclas, los sniffers y el software de control remoto para encontrar contraseñas administrativas y otros datos sensibles. Ataques similares ocurren con el correo electrónico. Un administrador abre inadvertidamente un correo electrónico que contiene un archivo adjunto infectado y se utiliza para obtener un punto de pivote dentro de la red que se utiliza para atacar otros sistemas.

La segunda técnica común utilizada por los atacantes es la elevación de privilegios al adivinar o romper una contraseña de un usuario administrativo para conseguir el acceso a un equipo de destino. Si los privilegios administrativos se distribuyen de forma holgada y amplia, o son idénticos a las contraseñas utilizadas en sistemas menos críticos, al atacante le cuesta mucho menos tomar el control total de los sistemas, porque hay muchas más cuentas que pueden actuar como vías para el atacante para comprometer privilegios administrativos.

Este control tiene como objeto garantizar que existe un proceso para gestionar los usuarios de la entidad, incluyendo su identificación, que los mecanismos de autenticación implantados son adecuados y seguros y que los privilegios de las aplicaciones y sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan.

Además, el control debe ser particularmente estricto sobre los usuarios que desempeñan tareas relacionadas con la administración de los sistemas, dado que los privilegios de los que disponen dan acceso a funciones que tienen un impacto muy significativo en la seguridad.

Desafortunadamente, para facilitar la agilidad y la comodidad, muchas organizaciones permiten que su personal tenga derechos de administrador tanto a nivel de la aplicación de gestión, como en los sistemas que le dan soporte (sistema operativo, base de datos, etc.) así como en sus equipos.

La situación anterior deriva en la existencia del riesgo de acceso y cambios no autorizados a los sistemas, que puede materializarse desde dos puntos diferentes:

- Desde el punto de vista externo, cuya puerta de entrada es el usuario, y en el que se aprovechan los privilegios de administración de los usuarios en sus equipos, para acceder desde fuera a la red interna de la entidad.
- Desde el punto de vista interno, es decir, desde dentro de la red de la entidad (bien por parte de un empleado con acceso autorizado o bien como consecuencia de un ciberataque que se ha iniciado externamente aprovechando la debilidad descrita en el párrafo anterior). En este caso, la gestión inadecuada de los privilegios de administración en los sistemas operativos, base de datos, etc. da a los atacantes la oportunidad de acceder y realizar cambios no autorizados en los sistemas corporativos que sustentan los procesos de gestión.

Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, bases de datos, sistemas operativos y equipos de usuario deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

Referencias

GPF-OCEX 5334 Revisión de los CGTI del área D. Operaciones de los sistemas de información

- D.1.1: Inventario y control de cuentas de administración
- D.1.2: Uso dedicado de cuentas de administración
- D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización
- D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos
- D.2.1: Procedimiento de gestión de usuarios
- D.2.2: Identificación
- D.2.5: Gestión de derechos de acceso

CBCS 4 Monitorización y respuesta

Objetivo de control: Disponer de procesos y herramientas que permitan la monitorización activa de eventos de seguridad y la gestión de la respuesta en caso de materialización de las amenazas.

Los sistemas y aplicaciones disponen de mecanismos que permiten el registro de trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo se ejecutan acciones o se producen eventos en los sistemas.

El análisis continuado y centralizado de los registros de actividad de los principales sistemas de las entidades permite monitorizar el estado de la seguridad y detectar en tiempo real, mediante herramientas que disponen de algoritmos que correlacionan el conjunto de todos los registros, posibles situaciones de compromiso de la seguridad.

Incluir en el análisis de los registros de actividad a los activos críticos de la organización resulta clave para la efectividad de los algoritmos de detección, y se deberían incorporar en este análisis, como mínimo, los registros de los equipos de seguridad perimetral, el clúster de servidores que gestiona los servicios de directorio y los sistemas de seguridad de equipos de usuarios y servidores (EDR, EDPR, XDR).

Además, la monitorización del estado de la seguridad puede ser incluido en el conjunto de servicios proporcionados por un centro de operaciones de ciberseguridad (SOC). Un SOC se define como un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad a su comunidad. La explotación de los servicios de SOC mejora significativamente el nivel de seguridad general de las entidades y la efectividad de las medidas de detección de incidentes en particular.

Adicionalmente a la detección de situaciones de compromiso, es necesario, para realizar una adecuada gestión de estos eventos, disponer de un conjunto de procesos, procedimientos y herramientas que permitan articular una respuesta óptima en caso de incidente. La gestión organizada de incidentes resulta crucial y requiere de procedimientos claramente establecidos que detallen todas las fases, incluyendo la valoración, la clasificación, el escalado, el tratamiento, la resolución y la notificación. Y para la correcta articulación de dichos procedimientos se debe disponer de los recursos técnicos y personales necesarios, y establecer formalmente las responsabilidades de los distintos implicados.

Sin una monitorización de los sistemas mediante el análisis continuado de los registros de actividad, un ataque puede pasar desapercibido por tiempo indefinido y los daños infringidos pueden ser irreversibles.

A veces estos registros son la única evidencia de un ataque exitoso. Muchas organizaciones mantienen los registros de auditoría para fines de cumplimiento, pero los atacantes confían en el hecho de que estas organizaciones rara vez analizan los registros de auditoría, por lo que no saben que sus sistemas han sido comprometidos. Debido a deficientes o inexistentes procesos de análisis de registros, los atacantes controlan a veces máquinas víctima durante meses o años sin que nadie se percate en la organización del destino, a pesar de que la evidencia del ataque se ha registrado en dichos registros no examinados.

Cuando el incidente es detectado y los sistemas comprometidos identificados, la reacción posterior es primordial. El tiempo de respuesta juega un papel crucial para minimizar los daños sufridos en un ataque. Para dar una respuesta adecuada, las organizaciones deben articular metódicamente la respuesta. Los pasos tras el incidente deben estar definidos, el personal prevenido, las responsabilidades asignadas y asumidas, y es necesario un entrenamiento del conjunto para asegurar la eficacia de la respuesta.

Las organizaciones que obvian la organización de la respuesta al incidente recaen inevitablemente en la improvisación, lo que conlleva retrasos en las acciones, decisiones erróneas y falta de liderazgo por indefinición de responsabilidades. El resultado de una gestión improvisada implica que el impacto del incidente no se gestiona adecuadamente y los resultados para la organización suelen ser catastróficos.

Referencias

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

- C.4.4: Centralización y revisión de logs
- C.9.3: Vigilancia
- C.9.4: Monitorización y correlación
- C.9.5: Centro de Operaciones de Ciberseguridad
- C.8.1: Procedimiento, notificación, detección y respuesta de incidentes

CBCS 5

Continuidad y resiliencia

Objetivo de control: Disponer del conjunto de planes, procedimientos y herramientas que, en caso de incidente de seguridad, permitan la recuperación de los sistemas en tiempo y forma adecuados para limitar el impacto en el servicio hasta un nivel aceptable.

Cuando los mecanismos de monitorización y gestión de incidentes no impiden la materialización de la amenaza y el incidente genera un impacto en los sistemas y servicios de la entidad, es necesario disponer de planes, procedimientos y herramientas que permitan su recuperación.

La gestión de los incidentes de seguridad que han producido un impacto en los sistemas y en la organización necesitan una planificación estricta. El manejo adecuado del impacto de un incidente requiere de respuestas precisas y en un corto espacio de tiempo, lo que impide en general improvisar la respuesta, que debe estar claramente definida con anterioridad al incidente.

La gestión de la respuesta requiere, en primer lugar, identificar los elementos que son críticos para el funcionamiento de la organización. Esto permite, en un contexto de urgencia para limitar los efectos de un incidente, priorizar aquellas acciones que permiten la recuperación de los servicios esenciales de la

organización y minimizar las consecuencias, como pérdidas financieras, tiempo de inactividad operativa, daño a la reputación e incumplimiento normativo.

Una vez identificados los elementos críticos de la organización, se debe organizar la respuesta a distintos niveles, el nivel técnico, mediante los planes de recuperación de desastres y el nivel de negocio, mediante los planes de continuidad del negocio. Los planes de recuperación de desastres articulan de manera detallada la respuesta para la recuperación de los sistemas que dan soporte a los servicios esenciales de la organización, y deben de elaborarse tantos planes como sistemas se identifiquen.

En cuando a los planes de continuidad de negocio, estos articulan la respuesta de la corporación en cuanto a medidas operacionales y organizativas con el objeto de gestionar el mantenimiento de las operaciones y los servicios esenciales, y activan los planes técnicos en caso necesario.

Entre las medidas que siempre se deben articular para gestionar la continuidad de los servicios y sistemas, se encuentra la utilización de copias de copias de seguridad. Sobre la gestión de las copias que permitan su utilización efectiva en caso de necesidad tras un incidente, resulta de especial relevancia tres aspectos:

- La definición de políticas de copias para sistemas que satisfagan los requisitos de negocio identificados y que se expresan mediante indicadores como el RTO (Objetivo de Tiempo de Recuperación) y el RPO (Objetivo de Punto de Recuperación).
- La realización de pruebas de recuperación periódicas y planificadas, que incluyan todos los tipos de copia realizados, y que permitan asegurar la viabilidad de las recuperaciones y que los indicadores de continuidad de negocio son satisfechos.
- La protección de las copias mediante medidas de seguridad adecuadas, que impidan ataques dirigidos y que tengan como objeto eliminar la capacidad de recuperación mediante copias.

Una de las medidas críticas para la gestión de la recuperación es la realización de copias de seguridad. Estas permiten la recuperación de datos y sistemas que proporcionan los servicios críticos. No obstante, la mera realización de copias no es suficiente, las organizaciones deben asegurar que las copias son correctas y recuperables, y que a su vez se encuentran especialmente protegidas frente ataques.

Los ciberataques mediante ransomware⁶ se vuelven inefectivos cuando se dispone de copia de seguridad de los datos secuestrados. Por ello, los ciberdelincuentes han mejorado los programas que utilizan para cifrar, de forma que estos se conectan a todos los repositorios accesibles vía la red de comunicaciones, con el fin de conseguir cifrar también las copias de seguridad. Este tipo de ataques "mejorados" ha sido utilizado con efectos devastadores en las últimas oleadas de ransomware. Por ello, el contar con una copia de seguridad que no se encuentre accesible a nivel de red, es decir, se encuentre aislada, es una medida de protección adicional a las de cifrado y seguridad física.

Referencias

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

- E.2.1: Identificación de elementos críticos del negocio
- E.2.2: Plan de recuperación de desastres (DRP). Pruebas.
- E.2.3: Plan de continuidad. Pruebas.
- E.1.1: Realización de copias de seguridad
- E.1.2: Realización de pruebas de recuperación
- E.1.3: Protección de las copias de seguridad

⁶ Un ransomware es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de eliminar esta restricción.

CBCS 6 Gobernanza de la ciberseguridad

Objetivo de control: Disponer de un conjunto de responsabilidades y actividades que tienen como finalidad proporcionar una dirección estratégica en materia de seguridad y garantizar la consecución de los objetivos establecidos.

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

Algunas de las ventajas que la existencia de un marco efectivo de gobernanza proporciona a las entidades serían:

- Posibilita la alineación de las actividades relativas a la seguridad de la información con los objetivos estratégicos de la entidad.
- Facilita la coordinación entre distintas áreas de la organización y los implicados en materia de seguridad de la información.
- Posibilita que el conjunto de actividades realizadas y medidas de seguridad aplicadas constituyan un Sistema de Gestión de la Seguridad de la Información que trasciende las iniciativas individuales.
- Establece las responsabilidades del personal implicado, necesarias para garantizar que se cumplen los objetivos y se alcanza el nivel de seguridad requerido.
- Ayuda a fomentar una cultura en materia de ciberseguridad en las organizaciones.

Por el contrario, aquellas entidades que no disponen de un marco de gobernanza adecuadamente definido e implantado tienen una alta probabilidad de experimentar las siguientes carencias:

- El principal riesgo consiste en que la entidad sea vulnerable frente a ciberataques por carecer de un sistema de controles coherente y aceptado por toda la organización.
- Probable uso ineficiente de los recursos, dado que, independientemente de la idoneidad de dichos recursos con respecto a las necesidades identificadas, no existen mecanismos que aseguren que estos son utilizados de manera adecuada para responder a necesidades alineadas con los objetivos estratégicos.
- No asegura la existencia de mecanismos de coordinación interna entre las distintas áreas de la organización y los responsables de la seguridad, lo que impide garantizar que las necesidades sean adecuadamente identificadas en tiempo y forma. Además, posibilita que existan áreas que, de manera inadecuada, realicen una gestión no coordinada de la seguridad al margen las políticas y normas de seguridad de la organización.
- No se asegura que el conjunto de medidas y procesos de seguridad implantados constituyan un Sistema de Gestión de la Seguridad de la Información, integrado y coherente, lo que implica un riesgo de que no existan mecanismos de control que velen por la eficacia de dichas medidas y procesos.
- En caso de no haberse definido responsabilidades al nivel directivo adecuado, existe un riesgo de que las necesidades con respecto a la seguridad de la información identificadas por sus responsables no sean debidamente atendidas por la organización.
- No se asegura que existan mecanismos que independicen las medidas y procesos de seguridad de las personas encargadas de gestionarlas, de modo que existe un riesgo de que ante determinadas ausencias, las medidas de seguridad no sean aplicadas.

Por lo tanto, una gobernanza adecuadamente establecida proporciona a las entidades mecanismos que garantizan que la seguridad es entendida como un sistema integrado, continuado y proactivo, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad. La inexistencia de este marco de gobernanza, independientemente de los esfuerzos y recursos dedicados a la seguridad, impide asegurar su eficacia e idoneidad.

Referencias

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

- A.2: Cumplimiento normativo (Anexo GPF-OCEX 5314, apartado 5. Cumplimiento legal)
- A.3: Gobernanza de la ciberseguridad (Anexo GPF-OCEX 5314, apartados 1 a 4, 6 y 7)

Anexo 2. Centro de Operaciones de Ciberseguridad

Se incorpora a los CGTI un nuevo subcontrol.

C.9.5: Centro de Operaciones de Ciberseguridad (SOC)

La entidad dispone de, o está integrada en un Centro de Operaciones de Ciberseguridad (SOC) que dispone de los medios materiales organizativos necesarios y proporciona servicios de prevención, protección, detección, respuesta y gestión de la seguridad. (ver Anexo 3)

Requisitos:

	Se dispone de un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad y constituyen un SOC operativo.
	Se han contratado servicios externos de seguridad que incluyen la provisión de servicios de SOC.

Propuesta de evidencias:

☐	Contrato para la provisión de servicios de SOC externo.
☐	Solicitud adhesión a la Red Nacional de SOC (RNSOC).
☐	Solicitud de adhesión a SOC de orden superior.
☐	Planes operativos para gestión de incidente y eventos de seguridad.
☐	Certificados de Servicios de Seguridad Gestionados emitidos por el CCN.
☐	Solicitud de acceso a herramienta de autoevaluación para certificación de Servicios de Seguridad Gestionados.
☐	Resultado de autoevaluación de los Servicios de Seguridad Gestionados mediante herramienta del CCN.
☐	Solicitud de auditoría para certificación de Servicios de Seguridad Gestionados remitida al CCN.
☐	Declaración de aplicabilidad que incluya las 36 medidas de seguridad y sus posibles refuerzos obligatorios que son de aplicación para los sistemas de información desde los que se despliegan los servicios de seguridad gestionados, en caso de no disponer de certificación del ENS.
☐	Declaración de aplicabilidad que incluya los requisitos específicos complementarios que son de aplicación para los sistemas de información desde los que se despliegan los SSG certificados por el CCN.

Procedimientos de auditoría (aspectos a evaluar):

¿Se dispone de un Centro de Operaciones de Ciberseguridad (SOC)? NOTA Verificar si el Centro de Operaciones de Ciberseguridad está constituido mediante medios propios, medios externos o una combinación de ambos. ☐ SI ☐ NO Espacio disponible para la redacción de la respuesta
--

	¿Se ha dotado a la organización de los recursos internos necesarios para la explotación de los servicios de SOC?
	¿Se han dotados los presupuestos para cubrir de los gastos de explotación del SOC o los gastos de contratación del servicio?
	¿Se han desarrollado los procedimientos necesarios para regular la operación del SOC?
	¿Se dispone de las herramientas necesarias para la explotación del SOC? Considerando: • Herramientas de Monitorización. (EDR, IDS, SIEM, APT...) • Herramientas de Auditoría (ANA CCN) • Herramienta propia de gestión del SOC (ticketing) • Herramientas específicas de participación en la RNS (MIPS, LUCIA CCN)
	¿Se ha integrado en otros SOC de orden superior?
	¿Se ha integrado el SOC en la Red Nacional de SOC (RNSOC)? ¿Dispone de personal con competencias asignadas para gestionar la comunicación con al RNSOC? ¿Se cumplen los criterios de permanencia y se realiza una comunicación y participación activa con la RNSOC?
	En caso de que los servicios de SOC sean prestados por una entidad proveedora externa y esta se encuentre integrada en la Red Nacional de SOC (RNSOC), ¿qué nivel de participación tiene esta entidad proveedora? ☐ Nivel Oro ☐ Nivel Plata de Detección (requerido para SOC Básico, Avanzado y Completo) ☐ Inhabilitado
	¿Se han certificado, por parte del CCN, los Servicios de Seguridad Gestionados que proporciona el SOC? En caso afirmativo, ¿qué servicios han sido certificados? ☐ Servicio de Gestión de la Ciberseguridad (requerido para SOC Básico, Avanzado y Completo) ☐ Servicio de Detección (requerido para SOC Básico, Avanzado y Completo) ☐ Servicio de Prevención (requerido para SOC Avanzado y Completo) ☐ Servicio de Respuesta (requerido para SOC Avanzado y Completo) ☐ Servicio de Protección (requerido para SOC Completo)
	Con el objeto de obtener la certificación del CCN de los Servicios de Seguridad Gestionados (PCE-SSG) y en caso de no disponer de certificación del ENS correspondiente (ver CBCS 6, subcontrol A.2: Cumplimiento normativo), ¿se han implementado las 36 medidas de seguridad y sus posibles refuerzos obligatorios que son de aplicación para los sistemas de información desde los que se despliegan los servicios de seguridad gestionados, tal y como se especifica en la “Guía de Seguridad de las TIC CCN-STIC 896 Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG”?
	¿Se han implementado, con el objeto de obtener la PCE-SSG, los requisitos específicos complementarios que son de aplicación para los sistemas de información desde los que se despliegan los SSG, tal y como se especifica en la “Guía de Seguridad de las TIC CCN-STIC 896 Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG”?
	¿Se ha solicitado y obtenido al Centro Criptológico Nacional el reconocimiento de un nivel de madurez del SOC? En caso afirmativo, ¿qué nivel se ha reconocido? ☐ SOC Básico ☐ SOC Avanzado ☐ SOC Completo

Anexo 3. Los Centros de Operaciones de Ciberseguridad.

Certificación de Servicios de Seguridad Gestionados (SSG). Nivel de madurez de un Centro de Operaciones de Ciberseguridad (SOC). Integración en la Red Nacional de SOC.

El CCN entiende que un **centro de operaciones de ciberseguridad (SOC)** es un **conjunto de tecnologías, procesos y personas** que mediante su interrelación, cooperación y coordinación **prestan servicios de ciberseguridad** a su comunidad.

Los servicios que presta un SOC, llamados **servicios de seguridad gestionados (SSG)**⁷, se definen como aquellos servicios prestados a un tercero que consisten en llevar a cabo o proporcionar asistencia para actividades relacionadas con la gestión de riesgos de ciberseguridad.

El Centro Criptológico Nacional considera que, “de una parte, **una organización prestadora de SSG debe de poder evidenciar sus capacidades operativas, así como su competencia técnicas en relación a los SSG que presta** en el ámbito de la ciberseguridad, garantizando que éstos serán de calidad; y de otra, los medios empleados por la organización para poder prestar los SSG deberán cumplir los requisitos necesarios de seguridad que garanticen a su vez que están protegidos y son confiables para realizar su desempeño de forma segura para la propia entidad y para aquellas que contraten sus servicios”⁸.

Con objeto de dar respuesta a esta necesidad, **el Centro Criptológico Nacional ha dispuesto un mecanismo que permite certificar la idoneidad de los servicios de SOC prestados**. Las iniciativas que componen este mecanismo son: la publicación de una guía STIC sobre SSG, la habilitación de un proceso de certificación de SSG y de un proceso de reconocimiento del nivel de madurez del SOC.

La “Guía de Seguridad de las TIC CCN-STIC 896. Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG”, elaborada y publicada en agosto de 2025, proporciona un perfil de cumplimiento específico que incluye los requisitos necesarios para garantizar la confiabilidad y competencia técnica en el despliegue de SSG y acreditar la conformidad con las normativas nacionales o europeas que demanden evidencias de seguridad en los SSG (PCE-SSG).

Sobre el **proceso de certificación de SSG**, este se ha habilitado por parte del CCN para entidades públicas y para entidades del sector privado, cuando estas últimas presten servicios o provean soluciones de seguridad a las entidades del sector público o cuando formen parte de la cadena de suministro de tales servicios.

Dado que un Centro de Operaciones de Seguridad (SOC) pueden estar operando simultáneamente una o varias entidades u organizaciones, es esencial que para cada SSG prestado se verifique que se satisface lo dispuesto en el PCE-SSG, con lo que se garantizará la seguridad global de los SSG que se proporcionen al cliente final. Por tanto, las certificaciones **se emitirán individualmente para cada uno de los servicios** proporcionados por el SOC, que son los siguientes:

- Servicio de Gestión de la ciberseguridad.
- Servicio de Prevención.
- Servicio de Protección.
- Servicio de Detección.
- Servicio de Respuesta.

Una vez certificados los servicios prestados por el SOC, la entidad podrá solicitar al Centro Criptológico Nacional el **reconocimiento de un nivel de madurez del SOC. Dependiendo de los servicios SSG que sean certificados**, se podrán reconocer los siguientes niveles:

- SOC Básico: Se requiere presentar la certificación del Servicio de Gestión de la Ciberseguridad y del Servicio de Detección.

⁷ REGLAMENTO (UE) 2025/37 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 19 de diciembre de 2024 por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados.

⁸ Guía de Seguridad de las TIC CCN-STIC 896. Perfil de Cumplimiento Específico para Servicios de Seguridad Gestionados / PCE-SSG.

- SOC Avanzado: Se requiere presentar la certificación del Servicio de Gestión de la Ciberseguridad, Servicio de Prevención, Servicio de Detección y Servicio de Respuesta.
- SOC Completo: Se requiere presentar la certificación de todos los servicios. Servicio de Gestión de la Ciberseguridad, Servicio de Prevención, Servicio de Protección, Servicio de Detección y Servicio de Respuesta.

Por otra parte, el Centro Criptológico Nacional ha impulsado la creación de la **Red Nacional de SOC (RNS)**, iniciativa para integrar a todos los SOC del territorio nacional, ya sean públicos o privados y cuyo objetivo principal es impulsar el servicio de protección de sus miembros mediante el bloqueo de cualquier indicio de actividad anómala que se esté detectando en cualquier punto de la Administración.

El **aspecto más relevante** en la adhesión a la Red Nacional de SOC es la **participación activa** de las entidades adheridas, compartiendo información novedosa y relevante con el resto de la red en los foros y herramientas de intercambio. Esta participación es además **evaluada periódicamente** y resulta determinante para permanecer en la Red Nacional de SOC.

Esta valoración, que se mide a través de la información técnica compartida por cada SOC, se valora y puntúa en función de la naturaleza de esta información y su relevancia. En base a esta valoración de la participación, **se clasifican las entidades** en los siguientes niveles:

- Oro. Nivel asignado a las entidades privadas y proveedoras con un nivel alto de participación.
- Plata. Nivel asignado a las entidades privadas y proveedoras con un nivel de participación normal.
- Inhabilitado. Nivel asignado a las entidades privadas y proveedoras que han dejado de participar en la compartición de información.

Anexo 4. Comparabilidad entre los CBCS-2018 y los CBCS-2026

CBCS-2026		Subcontroles	CBCS-2018	Comentarios
CBCS 1	Inventario y control de activos	C.1.1: Inventario de activos físicos autorizados	CBCS 1	Se han refundido en un único control por similitud en la gestión de los controles, facilitando la revisión.
		C.1.3: Control de HW no autorizados		
		C.1.2: Inventario de activos SW	CBCS 2	
		C.1.4: Control de SW no autorizados		
CBCS 2	Seguridad de los activos	C.2.3: SW soportado por el fabricante	CBCS 3	Se han refundido en un único control los CBCS 3 y 5, y se ha añadido la revisión del mantenimiento, ya que son medidas que impactan en el nivel de seguridad individual de los activos y que comparten parcialmente la gestión.
		C.2.1: Gestión de vulnerabilidades		
		C.2.2: Parcheo	CBCS 5	
		C.3.1: Configuración de seguridad		
		C.3.2: Gestión y mantenimiento de la configuración de seguridad		
CBCS 3	Gestión de usuarios y privilegios (de administración)	D.1.1: Inventario y control de cuentas de administración	CBCS 4	Se eliminan subcontroles que se encuentran incluidos en otros CBCS y se añaden, por interés general, subcontroles relativos a la gestión de usuarios “ordinarios”, adicionalmente a los usuarios administradores.
		D.1.2: Uso dedicado de cuentas de administración		
		D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización		
		D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos		
		D.2.1: Procedimiento de gestión de usuarios	Nuevos	
		D.2.2: Identificación		
		D.2.5: Gestión de derechos de acceso		
CBCS 4	Monitorización y respuesta	C.4.4: Centralización y revisión de logs	CBCS 6	Se eliminan subcontroles que por su simplicidad se encuentran ampliamente superados por medidas técnicas y organizativas de mayor calado. Se incluyen subcontroles relativos a la monitorización continuada del estado de la seguridad y la detección de incidentes, así como la respuesta organizada a los mismos para minimizar su impacto.
		C.9.4: Monitorización y correlación		
		C.9.3: Vigilancia	Nuevos	
		C.9.5: Centro de Operaciones de Ciberseguridad		
		C.8.1: Procedimiento, notificación, detección y respuesta de incidentes		
CBCS 5	Continuidad y resiliencia	E.1.1: Realización de copias de seguridad	CBCS 7	Se han incluido subcontroles sobre la gestión sistemática del proceso de recuperación de los servicios críticos.
		E.1.2: Realización de pruebas de recuperación		
		E.1.3: Protección de las copias de seguridad		
		E.2.1: Identificación de elementos críticos del negocio	Nuevos	
		E.2.2: Plan de recuperación de desastres (DRP). Pruebas.		
		E.2.3: Plan de continuidad. Pruebas.		
CBCS 6	Gobernanza de la ciberseguridad	A.2: Cumplimiento normativo	CBCS 8	Se ha actualizado el subcontrol para añadir la gobernanza, con objeto de verificar la existencia de un marco de gobierno que asegure la efectividad del resto de medidas y procesos de seguridad. Se elimina la revisión del cumplimiento de la ley de factura electrónica por su limitada relevancia en materia de ciberseguridad.
		A.3: Gobernanza de la ciberseguridad		

Anexo 5 Ejemplo de documento de inicio de la auditoría (DIA)

Excmo. Sr. XXXX

La Cámara/Sindicatura de Cuentas de XXXX, en virtud de las disposiciones del artículo XXX de la Ley XXX, y de acuerdo con lo previsto en el Programa Anual de Actuación de 20XX (PAA20XX), realizará una auditoría sobre la situación de los controles básicos de ciberseguridad (CBCS) a 31 de diciembre de 20XX.

1. Procedimiento para comunicar el inicio de la auditoría

El artículo “Inicio de la fiscalización”, del Reglamento de Régimen Interior (RRI) de la Cámara/Sindicatura establece en el apartado 1 que el síndico o la síndica competente notificará a los cuentadantes de las entidades que tengan que ser fiscalizadas en sus propias dependencias, el comienzo de la actividad, con una antelación mínima de diez días hábiles.

El propósito de realizar la comunicación inicial a través de este procedimiento es establecer unas reglas iniciales que permiten realizar la auditoría de manera eficiente. En consecuencia, **se pretende favorecer la existencia de unas condiciones previas en el momento de inicio del trabajo** o en una fase incipiente de este, que suponen tanto la realización de una auditoría adecuada a la normativa técnica de aplicación como un mejor entendimiento entre el auditor y la entidad auditada, para que los dos comprendan y consideren los efectos y consecuencias en la realización de la auditoría.

2. Objetivos y alcance de la auditoría

La auditoría que vamos a iniciar tiene como objetivo realizar una auditoría sobre la revisión de los controles básicos de ciberseguridad (CBCS) y determinar su índice de madurez a 31 de diciembre de 20XX.

3. Responsabilidades de la Cámara/Sindicatura de Cuentas

La responsabilidad de la Cámara/Sindicatura de Cuentas es concluir sobre la situación a 31 de diciembre de 20XX de los controles básicos de ciberseguridad que la entidad tiene implantados y formular las recomendaciones contribuyan a la mejora de los procedimientos de control. Les comunicaremos cualquier deficiencia significativa en el control interno o incumplimientos legales relevantes para la auditoría que, en su caso, identifiquemos durante la realización de la auditoría.

Nuestras conclusiones estarán basadas en el trabajo de auditoría a realizar, que es de alcance limitado.

Llevaremos a cabo nuestro trabajo de conformidad con los Principios fundamentales de fiscalización de los órganos de control externo y las Normas Internacionales de Auditoría adaptadas al Sector Público Español (NIA-ES-SP). Dicha normativa exige que cumplamos los requerimientos de ética aplicables a los auditores públicos; así como que planifiquemos y ejecutemos el trabajo con el fin de obtener una seguridad razonable de que las cuentas analizadas están libres de incorrección material, debida a fraude o error, y que las actividades revisadas y la

información reflejada en los estados financieros/contables resulten, en todos sus aspectos significativos, conformes a la normativa aplicable.

La fiscalización se realizará siguiendo las líneas establecidas en la nueva versión de la guía GPF-OCEX 5313, "Revisión de los controles básicos de ciberseguridad", que se resumen en el anexo 2.

Debido a las limitaciones inherentes a la auditoría, junto con las limitaciones propias del control interno, existe un riesgo inevitable de que no puedan detectarse algunas deficiencias de control, aun cuando la auditoría se planifique y ejecute adecuadamente de conformidad con las normas técnicas de auditoría.

4. Responsabilidades de los órganos de gobierno y dirección de la entidad

Realizaremos la fiscalización partiendo de la premisa que los órganos de gobierno y dirección reconocen y comprenden que son responsables de:

- a) Actuar de acuerdo con los principios de eficacia, economía y eficiencia, y vigilar la consecución del interés general y el cumplimiento de los objetivos de la entidad.
- b) Diseñar, aplicar y mantener el sistema de control interno que consideran oportuno para asegurar adecuadamente el cumplimiento de los principios financieros, de legalidad, de eficacia, de economía y de transparencia, exigibles al sector público.
- c) Elaborar, aprobar y aplicar las políticas de seguridad de la información de la entidad.
- d) El sistema de gestión de la seguridad de la información requerida por la normativa y/o que consideran necesaria para permitir un funcionamiento adecuado de los sistemas de información y de los procesos de gestión que estos sistemas soportan, así como para prevenir y corregir posibles deficiencias en su funcionamiento.
- e) Proporcionarnos:
 - acceso a toda la información de la que tenga conocimiento y que sea relevante para la auditoría, como por ejemplo registros, documentación en papel o electrónica, y otro material;
 - acceso a las aplicaciones y bases de datos relevantes para la auditoría;
 - información adicional que podamos solicitar para los fines de la auditoría, y
 - acceso ilimitado a las personas de la entidad de las cuales consideramos necesario obtener evidencia de auditoría. Una vez nos comunican la persona de la entidad interlocutora con el equipo de auditoría el auditor se pondrá en contacto con ella para programar los trabajos.
- f) Tomar las medidas oportunas para enmendar las deficiencias que pueda poner de manifiesto la **Cámara/Sindicatura**.

5. Informes de la auditoría

Con carácter general y como resultado del trabajo realizado se emitirán tres documentos:

- Borrador previo para discusión*: primer borrador del informe, que se comenta y discute con la dirección del ente fiscalizado. Borrador para alegaciones: el aprobado por el órgano competente del OCEX para su envío a trámite de alegaciones.
- Borrador para alegaciones*: el aprobado por el órgano competente del OCEX para su envío a trámite de alegaciones
- Informe final o definitivo*: el definitivamente aprobado por el órgano competente del OCEX y publicado.

Cualquier cambio en las cuentas anuales auditadas realizado con fecha posterior al informe emitido deberá ser necesariamente comunicado al auditor para que proceda a valorar esta circunstancia de acuerdo con lo establecido en las normas de auditoría en los términos indicados.

6. Equipo de auditoría y desarrollo de esta

La auditoría la llevará a cabo un equipo de auditoría de sistemas de información de la **Cámara/Sindicatura**, dirigido por el auditor **XXXX** y formado por los auditores de sistemas de información:

- **xxx <xxx@xxx>**

- **xxx <xxx@xxx>**

Le solicito que dé las instrucciones oportunas para que se preste la colaboración necesaria al equipo de auditoría.

Las reuniones que sea necesario realizar durante el trabajo de fiscalización se realizarán bien manteniendo reuniones presenciales o bien mediante herramientas de trabajo en remoto, serán comunicadas con antelación incluyendo los puntos a revisar en cada una.

El trabajo de campo está previsto que se lleve a cabo durante los meses de **xxx** a **xxx**, con el objetivo de disponer de un borrador previo para discusión con la entidad el mes de **xxx**.

7. Confidencialidad

Toda la información recabada sobre la entidad será tratada de forma confidencial y segura, de acuerdo con la política de seguridad de la información aprobada por la **Cámara/Sindicatura de Cuentas** y con la normativa de protección de datos personales.

Dado que la información utilizada en la auditoría tiene un carácter sensible, los resultados preliminares de nuestra fiscalización o hallazgos de auditoría se comunicarán con carácter confidencial a los responsables de la entidad para que puedan realizar sus comentarios y analicen la razonabilidad de las conclusiones alcanzadas.

8. Solicitud

8.1 Para poder realizar nuestro trabajo de la forma más eficiente posible, precisamos que:

- devuelva el acuse de recibo de este documento debidamente firmado (se acompaña modelo en el anexo 1);
- indique el interlocutor designado por la entidad con el que mantendrá en contacto el auditor para realizar la fiscalización, y
- se remitan al equipo de auditoría los anexos 3 y 4 debidamente cumplimentados y firmados por el interlocutor designado. Para facilitar su cumplimentación, las tablas serán remitidas en formato editable una vez se nos comunique el interlocutor.

8.2. Documentación que se solicita

A continuación, detallamos la documentación necesaria para iniciar los trabajos de auditoría. Esta relación es inicial y la completaremos durante el desarrollo del trabajo.

Deben remitirnos, debidamente cumplimentada y firmada por el interlocutor designado:

- La tabla/cuestionario sobre los CBCS (anexo 3).
- La tabla para documentar el conocimiento de la entidad (anexo 4)

Cuando nos comuniquen el interlocutor designado le enviaremos esas tablas en formato editable para facilitar su cumplimentación.

8.3 Procedimiento de remisión de la información

La documentación puede remitirse en formato electrónico de forma segura a través de procedimiento habilitado a tal efecto en la sede electrónica de la **Cámara/Sindicatura de Cuentas**.

ANEXO 1 - MODELO DE CONTESTACIÓN A CUMPLIMENTAR POR EL XXXX DE XXXX O PERSONA EN QUIEN DELEGUE

Con fecha _____, he recibido el documento de inicio de la auditoría (DIA) que va a realizar la **Cámara/Sindicatura de Cuentas**.

Hemos leído y comprendido el DIA en su totalidad.

Asimismo, adjunto se remite la siguiente documentación solicitada en el DIA:

-
-

(Se deberá detallar cada uno de los documentos que se adjunten)

La persona que actuará como interlocutor con el equipo de auditoría de la **Cámara/Sindicatura** será _____ (nombre y cargo), su teléfono de contacto es _____ y su correo electrónico es _____.

Fecha: __/__/20__

Firmado:

_____ (nombre y cargo)

ANEXO 2 – LOS CONTROLES BÁSICOS DE CIBERSEGURIDAD

1. Metodología de trabajo

Los CBCS son un subconjunto priorizado de subcontroles CGTI, por lo que su revisión y la metodología y los procedimientos a utilizar se encuentran ampliamente detallados en la GPF-OCEX 5330 y siguientes.

Para revisar los CBCS se utilizarán las fichas de revisión incluidas en las GPF-OCEX 5333 a 5335 y en la GPF-OCEX 5314, tal como se indica a continuación:

- GPF-OCEX 533, "Revisión de los CGTI del área C. Operaciones de los sistemas de información".

Aplicable para los **CBCS 1, 2 y 4**.

En el caso del CBCS 4 se utilizará la ficha de revisión adicional, la C.9.5: "Centro de operaciones de ciberseguridad", incluida en esta guía. Este subcontrol no se encuentra incluido en la guía GPF-OCEX 5330, pero será incorporado al aprobarse la próxima actualización de la guía.

- GPF-OCEX 5334, "Revisión de los CGTI del área D. Controles de acceso a datos y programas". Aplicable para el **CBCS 3**.
- GPF-OCEX 5335, "Revisión de los CGTI del área E. Continuidad del servicio". Aplicable para el **CBCS 5**.
- GPF-OCEX 5314, "Gobernanza de la ciberseguridad y su auditoría". Aplicable para el **CBCS 6**.

En general la metodología de trabajo será la establecida en la GPF-OCEX 5330. En particular, los apartados

10. Evaluación del diseño e implementación (D+I) de los CGTI relevantes
11. Revisión de la eficacia operativa de los CGTI relevantes
16. Evaluación de las deficiencias de control interno detectadas
17. Importancia relativa de las deficiencias de control a efectos de la auditoría
18. Recomendaciones

Tabla 1. Estructura de los controles básicos de ciberseguridad (2026)

Control		Objetivo de control	Ref.	Subcontroles de los CBCS/CGTI
CBCS 1	Inventario y control de activos	Gestionar activamente todos los activos <i>hardware</i> y <i>software</i> en la entidad, posibilitando la aplicación de controles posteriores a dichos activos.	5333	C.1.1: Inventario de activos físicos autorizados C.1.2: Inventario de activos SW C.1.3: Control de HW no autorizados C.1.4: Control de SW no autorizados
CBCS 2	Seguridad de los activos	Gestionar activamente la configuración, el estado de la seguridad y las medidas aplicadas a los activos de la entidad.	5333	C.2.1: Gestión de vulnerabilidades C.2.2: Parcheo C.2.3: SW soportado por el fabricante C.3.1: Configuración de seguridad C.3.2: Gestión y mantenimiento de la configuración de seguridad
CBCS 3	Gestión de usuarios y privilegios de administración	Disponer de un proceso de gestión de usuarios de la entidad, su identificación, autenticación y la asignación de derechos de acceso, particularmente para los administradores de los sistemas.	5334	D.1.1: Inventario y control de cuentas de administración D.1.2: Uso dedicado de cuentas de administración D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos D.2.1: Procedimiento de gestión de usuarios D.2.2: Identificación D.2.5: Gestión de derechos de acceso
CBCS 4	Monitorización y respuesta	Disponer de procesos y herramientas que permitan la monitorización activa de eventos de seguridad y la gestión de la respuesta en caso de materialización de las amenazas.	5333	C.4.4: Centralización y revisión de <i>logs</i> C.9.3: Vigilancia C.9.4: Monitorización y correlación C.9.5: Centro de operaciones de ciberseguridad C.8.1: Procedimiento, notificación, detección y respuesta de incidentes
CBCS 5	Continuidad y resiliencia	Disponer del conjunto de planes, procedimientos y herramientas que, en caso de incidente de seguridad, permitan la recuperación de los sistemas en tiempo y forma adecuados para limitar el impacto en el servicio hasta un nivel aceptable.	5335	E.1.1: Realización de copias de seguridad E.1.2: Realización de pruebas de recuperación E.1.3: Protección de las copias de seguridad E.2.1: Identificación de elementos críticos del negocio E.2.2: Plan de recuperación de desastres (DRP). Pruebas. E.2.3: Plan de continuidad. Pruebas.
CBCS 6	Gobernanza de la ciberseguridad	Disponer de un conjunto de responsabilidades y actividades que tienen como finalidad proporcionar una dirección estratégica en materia de seguridad y garanticen la consecución de los objetivos establecidos.	5314	A.2: Cumplimiento normativo A.3: Gobernanza de la ciberseguridad

2. Por qué son importantes los controles básicos de ciberseguridad (CBCS)

CBCS 1	Inventario y control de activos
Objetivo de control:	Gestionar activamente todos los dispositivos <i>hardware</i> y <i>software</i> en la entidad, posibilitando la aplicación de controles posteriores a dichos activos.

Los atacantes, que pueden estar ubicados en cualquier parte del mundo, están escaneando continuamente las redes de las organizaciones objetivo, esperando que nuevos y desprotegidos sistemas se incorporen a esas redes, buscando versiones vulnerables de *hardware* y *software* que puedan explotarse remotamente.

Buscan dispositivos, como los portátiles, que se conectan y desconectan de las redes corporativas, y es más probable que no dispongan de los últimos parches y actualizaciones de seguridad, aprovechando el lapso transcurrido hasta su actualización.

Es más probable que las máquinas mal controladas estén ejecutando *software* que no sea necesario para los fines de la entidad (introduciendo posibles fallos de seguridad), o ejecutando *malware* introducido por un atacante después de que un sistema haya sido comprometido.

Una vez que una máquina ha sido comprometida, los atacantes la utilizan a menudo como punto para recoger información sensible del sistema en el que está integrada y de otros sistemas conectados a él. Además, las máquinas comprometidas se utilizan como punto de lanzamiento para el movimiento a través de la red y de las redes conectadas. De esta manera, los atacantes pueden rápidamente convertir una máquina comprometida en muchas.

Este control permite a las organizaciones definir la base de activos que es necesario defender. Sin conocer qué dispositivos están conectados, no pueden ser defendidos.

El inventario debe ser tan completo como sea posible: en organizaciones con un nivel de madurez básico el inventario puede ser realizado y mantenido con procedimientos manuales y, en otras más maduras, utilizando herramientas de escaneo (tanto activos como pasivos) que detecten los dispositivos conectados a la red corporativa y agentes que permitan la detección del *software* instalado en los activos *hardware*.

El conocimiento de los activos existentes en la red permite, mediante la comparación con el listado de activos autorizados, identificar aquellos que no forman parte de la organización, incluyendo tanto los activos *hardware* como los activos *software*. Una vez identificados los activos no autorizados es posible aplicar controles y medidas que impidan su acceso a la red corporativa, en el caso de los activos *hardware*, y la ejecución únicamente de aplicaciones contenidas en la lista blanca, en el caso de los activos *software*. Limitar el acceso o la ejecución únicamente a aquellos activos que se encuentran controlados permite asegurar que todos los activos individuales disponen de las medidas de seguridad y de las configuraciones necesarias, limitando la superficie de exposición.

Además, disponer de un inventario actualizado de activos permite aplicar sobre todos ellos controles posteriores que posibilitan alcanzar el nivel de seguridad individual requerido.

Referencias

GPF-OCEX 5333, "Revisión de los CGTI del área C. Operaciones de los sistemas de información"

- C.1.1: Inventario de activos físicos autorizados
- C.1.2: Inventario de activos SW
- C.1.3: Control de HW no autorizados
- C.1.4: Control de SW no autorizados

CBCS 2**Seguridad de los activos**

Objetivo de control: Gestionar activamente la configuración, el estado de la seguridad y las medidas aplicadas a los activos de la entidad.

Los ciberdefensores deben operar en un flujo constante de información nueva: actualizaciones de *software*, parches, avisos de seguridad, boletines de amenazas, etc. La comprensión y gestión de las vulnerabilidades se ha convertido en una actividad continua, que requiere tiempo, atención y recursos significativos.

Los atacantes tienen acceso a la misma información y pueden aprovechar las brechas entre la aparición de nuevos conocimientos y la remediación. Por ejemplo, cuando los investigadores reportan nuevas vulnerabilidades, comienza una carrera entre todas las partes, incluyendo: atacantes (para "armarse", desplegar un ataque, y explotarlo); proveedores (para desarrollar, implementar parches o firmas y actualizaciones), y defensores (para evaluar riesgos, parches de prueba, e instalarlos).

Las organizaciones que no escanean las vulnerabilidades y abordan de forma proactiva los defectos encontrados se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos. Los defensores se enfrentan a desafíos particulares en cuanto a escalar el remedio en toda una entidad, y priorizar las acciones con conflictos de prioridades y, a veces, efectos secundarios inciertos.

Además, la seguridad de los activos se complementa con una configuración adecuada, que minimice o elimine posibles vulnerabilidades. Sin embargo, fabricantes y vendedores entregan sus productos sin esta consideración. Las configuraciones predeterminadas para los sistemas operativos y las aplicaciones están normalmente orientadas a la facilidad de operación y a la facilidad de uso, no a la seguridad. Cuando se entrega un *software* es habitual encontrarse con controles poco robustos, servicios y puertos abiertos, cuentas o contraseñas predeterminadas, protocolos antiguos (vulnerables), preinstalación de *software* innecesario; todos estos aspectos son vulnerables en su estado predeterminado.

El desarrollo de opciones de configuración con buenas propiedades de seguridad es una tarea compleja más allá de la capacidad de los usuarios individuales, requiriendo análisis a veces complejos para tomar buenas decisiones.

Incluso si se desarrolla e instala una configuración inicial fuerte, debe ser revisada y actualizada continuamente para evitar el deterioro de la seguridad, en particular cuando el *software* es actualizado o parcheado, se divulgan las nuevas vulnerabilidades de la seguridad, o las configuraciones se "ajustan" para permitir la instalación de nuevo *software* o para dar soporte a nuevos requerimientos operacionales. Si no se revisa y actualiza de forma continua, los atacantes encontrarán oportunidades para explotar tanto los servicios accesibles a la red como el *software* cliente.

La finalidad de este control es asegurar que todos los activos autorizados de la entidad, incluyendo activos *hardware* y activos *software*, dispongan de manera individual de un nivel de seguridad adecuado, minimizando la superficie de exposición de las organizaciones y limitando la probabilidad de materialización de las amenazas.

La seguridad de activos depende principalmente de dos aspectos: la gestión del mantenimiento, las vulnerabilidades y el parcheo, por una parte, y la configuración segura por otra.

La gestión de vulnerabilidades tiene como objeto conocer y eliminar debilidades técnicas que existen en los sistemas de información de la organización, reduciendo la probabilidad de que los sistemas sigan siendo vulnerables. Las organizaciones implementan procesos de gestión y utilizan

sistemas de administración de parches y actualizaciones que cubren vulnerabilidades tanto de sistemas operativos como aplicaciones de terceros.

En cuanto a la configuración de los sistemas, la mayoría de los sistemas están configurados por defecto para facilitar su uso y no necesariamente considerando criterios de seguridad. Para implantar este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad que minimicen la probabilidad de sufrir ataques mediante la explotación de configuraciones vulnerables.

Las organizaciones que no gestionan activamente las vulnerabilidades y configuraciones de los sistemas y abordan de forma proactiva los defectos encontrados, no minimizan la superficie de exposición frente a las amenazas externas y se enfrentan a una alta probabilidad de que sus sistemas informáticos sean comprometidos.

Referencias

GPF-OCEX 5333 Revisión de los CGTI del área C. Operaciones de los sistemas de información

- C.2.1: Gestión de vulnerabilidades
- C.2.2: Parcheo
- C.2.3: SW soportado por el fabricante
- C.3.1: Configuración de seguridad
- C.3.2: Gestión y mantenimiento de la configuración de seguridad

CBCS 3**Gestión de usuarios y privilegios (de administración)**

Objetivo de control: Disponer de un proceso de gestión de usuarios de la entidad, su identificación, autenticación y la asignación de derechos de acceso, particularmente para los administradores de los sistemas.

El uso inadecuado de privilegios administrativos es un método primario para que los atacantes se propaguen dentro de una entidad objetivo. Dos técnicas de ataque muy comunes aprovechan los privilegios administrativos incontrolados.

En la primera, un usuario que opera como administrador de su equipo, abre un adjunto de correo electrónico malicioso, descarga y abre un archivo de un sitio web malicioso, o simplemente navega en un sitio web que aloja contenido del atacante que puede explotar automáticamente navegadores. El archivo o *exploit* contiene código ejecutable que se ejecuta en el equipo de la víctima ya sea automáticamente o engañando al usuario para que ejecute el contenido del atacante. Si la cuenta del usuario de la víctima tiene privilegios administrativos, el atacante puede apoderarse completamente de la máquina de la víctima e instalar los registradores de teclas, los *sniffers* y el *software* de control remoto para encontrar contraseñas administrativas y otros datos sensibles. Ataques similares ocurren con el correo electrónico. Un administrador abre inadvertidamente un correo electrónico que contiene un archivo adjunto infectado y se utiliza para obtener un punto de pivote dentro de la red que se utiliza para atacar otros sistemas.

La segunda técnica común utilizada por los atacantes es la elevación de privilegios al adivinar o romper una contraseña de un usuario administrativo para conseguir el acceso a un equipo de destino. Si los privilegios administrativos se distribuyen de forma holgada y amplia, o son idénticos a las contraseñas utilizadas en sistemas menos críticos, al atacante le cuesta mucho menos tomar el control total de los sistemas, porque hay muchas más cuentas que pueden actuar como vías para el atacante para comprometer privilegios administrativos.

Este control tiene como objeto garantizar que existe un proceso para gestionar los usuarios de la entidad, incluyendo su identificación, que los mecanismos de autenticación implantados son adecuados y seguros y que los privilegios de las aplicaciones y sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan.

Además, el control debe ser particularmente estricto sobre los usuarios que desempeñan tareas relacionadas con la administración de los sistemas, dado que los privilegios de los que disponen dan acceso a funciones que tienen un impacto muy significativo en la seguridad.

Desafortunadamente, para facilitar la agilidad y la comodidad, muchas organizaciones permiten que su personal tenga derechos de administrador tanto a nivel de la aplicación de gestión como en los sistemas que le dan soporte (sistema operativo, base de datos, etc.) así como en sus equipos.

La situación anterior deriva en la existencia del riesgo de acceso y cambios no autorizados a los sistemas, que puede materializarse desde dos puntos diferentes:

- Desde el punto de vista externo, cuya puerta de entrada es el usuario, y en el que se aprovechan los privilegios de administración de los usuarios en sus equipos, para acceder desde fuera a la red interna de la entidad.
- Desde el punto de vista interno, es decir, desde dentro de la red de la entidad (bien por parte de un empleado con acceso autorizado o bien como consecuencia de un ciberataque que se ha iniciado externamente aprovechando la debilidad descrita en el párrafo anterior). En este caso, la gestión inadecuada de los privilegios de administración en los sistemas operativos, base de datos, etc. da a los atacantes la oportunidad de acceder y realizar cambios no autorizados en los sistemas corporativos que sustentan los procesos de gestión.

Este control nos lleva a que las cuentas de usuarios administradores de aplicaciones, bases de datos, sistemas operativos y equipos de usuario deben estar identificadas, su uso auditado, eliminando las que no se utilizan y cambiando las que están definidas por defecto. Adicionalmente, deben cumplir con la política de fortaleza de contraseñas.

Referencias

GPF-OCEX 5334, "Revisión de los CGTI del área D. Operaciones de los sistemas de información"

- D.1.1: Inventario y control de cuentas de administración
- D.1.2: Uso dedicado de cuentas de administración
- D.1.3: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización
- D.1.4: Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos
- D.2.1: Procedimiento de gestión de usuarios
- D.2.2: Identificación
- D.2.5: Gestión de derechos de acceso

CBCS 4**Monitorización y respuesta**

Objetivo de control: Disponer de procesos y herramientas que permitan la monitorización activa de eventos de seguridad y la gestión de la respuesta en caso de materialización de las amenazas.

Los sistemas y aplicaciones disponen de mecanismos que permiten el registro de trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo se ejecutan acciones o se producen eventos en los sistemas.

El análisis continuado y centralizado de los registros de actividad de los principales sistemas de las entidades permite monitorizar el estado de la seguridad y detectar en tiempo real, mediante herramientas que disponen de algoritmos que correlacionan el conjunto de todos los registros, posibles situaciones de compromiso de la seguridad.

Incluir en el análisis de los registros de actividad a los activos críticos de la organización resulta clave para la efectividad de los algoritmos de detección, y se deberían incorporar en este análisis, como mínimo, los registros de los equipos de seguridad perimetral, el clúster de servidores que gestiona los servicios de directorio y los sistemas de seguridad de equipos de usuarios y servidores (EDR, EDPR, XDR).

Además, la monitorización del estado de la seguridad puede ser incluido en el conjunto de servicios proporcionados por un centro de operaciones de ciberseguridad (SOC). Un SOC se define como un conjunto de tecnologías, procesos y personas que mediante su interrelación, cooperación y coordinación prestan servicios de ciberseguridad a su comunidad. La explotación de los servicios de SOC mejora significativamente el nivel de seguridad general de las entidades y la efectividad de las medidas de detección de incidentes en particular.

Adicionalmente a la detección de situaciones de compromiso, es necesario, para realizar una adecuada gestión de estos eventos, disponer de un conjunto de procesos, procedimientos y herramientas que permitan articular una respuesta óptima en caso de incidente. La gestión organizada de incidentes resulta crucial y requiere de procedimientos claramente establecidos que detallen todas las fases, incluyendo la valoración, la clasificación, el escalado, el tratamiento, la resolución y la notificación. Y para la correcta articulación de dichos procedimientos se debe disponer de los recursos técnicos y personales necesarios, y establecer formalmente las responsabilidades de los distintos implicados.

Sin una monitorización de los sistemas mediante el análisis continuado de los registros de actividad, un ataque puede pasar desapercibido por tiempo indefinido y los daños infligidos pueden ser irreversibles.

A veces estos registros son la única evidencia de un ataque exitoso. Muchas organizaciones mantienen los registros de auditoría para fines de cumplimiento, pero los atacantes confían en el hecho de que estas organizaciones rara vez analizan los registros de auditoría, por lo que no saben que sus sistemas han sido comprometidos. Debido a deficientes o inexistentes procesos de análisis de registros, los atacantes controlan a veces máquinas víctima durante meses o años sin que nadie se percate en la organización del destino, a pesar de que la evidencia del ataque se ha registrado en dichos registros no examinados.

Cuando el incidente es detectado y los sistemas comprometidos identificados, la reacción posterior es primordial. El tiempo de respuesta juega un papel crucial para minimizar los daños sufridos en un ataque. Para dar una respuesta adecuada, las organizaciones deben articular metódicamente la respuesta. Los pasos tras el incidente deben estar definidos, el personal prevenido, las responsabilidades asignadas y asumidas, y es necesario un entrenamiento del conjunto para asegurar la eficacia de la respuesta.

Las organizaciones que obvian la organización de la respuesta al incidente recaen inevitablemente en la improvisación, lo que conlleva retrasos en las acciones, decisiones erróneas y falta de liderazgo por indefinición de responsabilidades. El resultado de una gestión improvisada implica que el impacto del incidente no se gestiona adecuadamente y los resultados para la organización suelen ser catastróficos.

Referencias

GPF-OCEX 5333, "Revisión de los CGTI del área C. Operaciones de los sistemas de información"

- C.4.4: Centralización y revisión de *logs*
- C.9.3: Vigilancia
- C.9.4: Monitorización y correlación
- C.9.5: Centro de operaciones de ciberseguridad
- C.8.1: Procedimiento, notificación, detección y respuesta de incidentes

CBCS 5**Continuidad y resiliencia**

Objetivo de control: Disponer del conjunto de planes, procedimientos y herramientas que, en caso de incidente de seguridad, permitan la recuperación de los sistemas en tiempo y forma adecuados para limitar el impacto en el servicio hasta un nivel aceptable.

Cuando los mecanismos de monitorización y gestión de incidentes no impiden la materialización de la amenaza y el incidente genera un impacto en los sistemas y servicios de la entidad, es necesario disponer de planes, procedimientos y herramientas que permitan su recuperación.

La gestión de los incidentes de seguridad que han producido un impacto en los sistemas y en la organización necesitan una planificación estricta. El manejo adecuado del impacto de un incidente requiere de respuestas precisas y en un corto espacio de tiempo, lo que impide en general improvisar la respuesta, que debe estar claramente definida con anterioridad al incidente.

La gestión de la respuesta requiere, en primer lugar, identificar los elementos que son críticos para el funcionamiento de la organización. Esto permite, en un contexto de urgencia para limitar los efectos de un incidente, priorizar aquellas acciones que permiten la recuperación de los servicios esenciales de la organización y minimizar las consecuencias, como pérdidas financieras, tiempo de inactividad operativa, daño a la reputación e incumplimiento normativo.

Una vez identificados los elementos críticos de la organización, se debe organizar la respuesta a distintos niveles, el nivel técnico, mediante los planes de recuperación de desastres y el nivel de negocio, mediante los planes de continuidad del negocio. Los planes de recuperación de desastres articulan de manera detallada la respuesta para la recuperación de los sistemas que dan soporte a los servicios esenciales de la organización, y deben de elaborarse tantos planes como sistemas se identifiquen.

En cuanto a los planes de continuidad de negocio, estos articulan la respuesta de la corporación en cuanto a medidas operacionales y organizativas con el objeto de gestionar el mantenimiento de las operaciones y los servicios esenciales, y activan los planes técnicos en caso necesario.

Entre las medidas que siempre se deben articular para gestionar la continuidad de los servicios y sistemas, se encuentra la utilización de copias de seguridad. Sobre la gestión de las copias que permitan su utilización efectiva en caso de necesidad tras un incidente, resulta de especial relevancia tres aspectos:

- La definición de políticas de copias para sistemas que satisfagan los requisitos de negocio identificados y que se expresan mediante indicadores como el RTO (objetivo de tiempo de recuperación) y el RPO (objetivo de punto de recuperación).
- La realización de pruebas de recuperación periódicas y planificadas, que incluyan todos los tipos de copia realizados, y que permitan asegurar la viabilidad de las recuperaciones y que los indicadores de continuidad de negocio son satisfechos.
- La protección de las copias mediante medidas de seguridad adecuadas, que impidan ataques dirigidos y que tengan como objeto eliminar la capacidad de recuperación mediante copias.

Una de las medidas críticas para la gestión de la recuperación es la realización de copias de seguridad. Estas permiten la recuperación de datos y sistemas que proporcionan los servicios críticos. No obstante, la mera realización de copias no es suficiente, las organizaciones deben asegurar que las copias son correctas y recuperables, y que a su vez se encuentran especialmente protegidas frente a ataques.

Los ciberataques mediante *ransomware*¹ se vuelven inefectivos cuando se dispone de copia de seguridad de los datos secuestrados. Por ello, los ciberdelincuentes han mejorado los programas que utilizan para cifrar, de forma que estos se conectan a todos los repositorios accesibles vía la red de comunicaciones, con el fin de conseguir cifrar también las copias de seguridad. Este tipo de ataques "mejorados" ha sido utilizado con efectos devastadores en las últimas oleadas de *ransomware*. Por ello, el contar con una copia de seguridad que no se encuentre accesible a nivel de red, es decir, se encuentre aislada, es una medida de protección adicional a las de cifrado y seguridad física.

Referencias

GPF-OCEX 5333, "Revisión de los CGTI del área C. Operaciones de los sistemas de información"

- E.2.1: Identificación de elementos críticos del negocio
- E.2.2: Plan de recuperación de desastres (DRP). Pruebas.
- E.2.3: Plan de continuidad. Pruebas.
- E.1.1: Realización de copias de seguridad
- E.1.2: Realización de pruebas de recuperación
- E.1.3: Protección de las copias de seguridad

¹ Un *ransomware* es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de eliminar esta restricción.

CBCS 6**Gobernanza de la ciberseguridad**

Objetivo de control: Disponer de un conjunto de responsabilidades y actividades que tienen como finalidad proporcionar una dirección estratégica en materia de seguridad y garantizar la consecución de los objetivos establecidos.

La gestión de la ciberseguridad, como tarea clave para la prevención proactiva, requiere del establecimiento de un marco de gobernanza en el que se designen a los organismos o unidades responsables de dicha gestión y se definan claramente sus competencias en este ámbito, que deberán ser conocidas por toda la organización.

La existencia de un conjunto eficaz de procesos de gestión de la ciberseguridad y de responsabilidades definidas proporciona a las entidades múltiples ventajas con respecto a las entidades sin un marco de gobernanza adecuadamente definido, independientemente de la existencia de recursos técnicos y de las medidas de seguridad aplicadas.

Algunas de las ventajas que la existencia de un marco efectivo de gobernanza proporciona a las entidades serían:

- Posibilita la alineación de las actividades relativas a la seguridad de la información con los objetivos estratégicos de la entidad.
- Facilita la coordinación entre distintas áreas de la organización y los implicados en materia de seguridad de la información.
- Posibilita que el conjunto de actividades realizadas y medidas de seguridad aplicadas constituyan un Sistema de Gestión de la Seguridad de la Información que trasciende las iniciativas individuales.
- Establece las responsabilidades del personal implicado, necesarias para garantizar que se cumplen los objetivos y se alcanza el nivel de seguridad requerido.
- Ayuda a fomentar una cultura en materia de ciberseguridad en las organizaciones.

Por el contrario, aquellas entidades que no disponen de un marco de gobernanza adecuadamente definido e implantado tienen una alta probabilidad de experimentar las siguientes carencias:

- El principal riesgo consiste en que la entidad sea vulnerable frente a ciberataques por carecer de un sistema de controles coherente y aceptado por toda la organización.
- Probable uso ineficiente de los recursos, dado que, independientemente de la idoneidad de dichos recursos con respecto a las necesidades identificadas, no existen mecanismos que aseguren que estos son utilizados de manera adecuada para responder a necesidades alineadas con los objetivos estratégicos.
- No asegura la existencia de mecanismos de coordinación interna entre las distintas áreas de la organización y los responsables de la seguridad, lo que impide garantizar que las necesidades sean adecuadamente identificadas en tiempo y forma. Además, posibilita que existan áreas que, de manera inadecuada, realicen una gestión no coordinada de la seguridad al margen las políticas y normas de seguridad de la organización.
- No se asegura que el conjunto de medidas y procesos de seguridad implantados constituyan un Sistema de Gestión de la Seguridad de la Información, integrado y coherente, lo que implica un riesgo de que no existan mecanismos de control que velen por la eficacia de dichas medidas y procesos.
- En caso de no haberse definido responsabilidades al nivel directivo adecuado, existe un riesgo de que las necesidades con respecto a la seguridad de la información identificadas por sus responsables no sean debidamente atendidas por la organización.

- No se asegura que existan mecanismos que independicen las medidas y procesos de seguridad de las personas encargadas de gestionarlas, de modo que existe un riesgo de que ante determinadas ausencias, las medidas de seguridad no sean aplicadas.

Por lo tanto, una gobernanza adecuadamente establecida proporciona a las entidades mecanismos que garantizan que la seguridad es entendida como un sistema integrado, continuado y proactivo, con procesos de gestión que velan por la eficacia de las medidas y procesos de seguridad. La inexistencia de este marco de gobernanza, independientemente de los esfuerzos y recursos dedicados a la seguridad, impide asegurar su eficacia e idoneidad.

Referencias

GPF-OCEX 5314 Gobernanza de la ciberseguridad y su auditoría

- A.2: Cumplimiento normativo (Anexo GPF-OCEX 5314, apartado 5. Cumplimiento legal)
- A.3: Gobernanza de la ciberseguridad (Anexo GPF-OCEX 5314, apartados 1 a 4, 6 y 7)

ANEXO 3 – CUESTIONARIO DE REVISIÓN PRELIMINAR DE LOS CBCS

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 1 – Inventario y control de activos				
Inventario de activos HW	GPF-OCEX 5333: C.1.1	Se dispone de un inventario de activos <i>hardware</i> actualizado. Es admisible el concepto de inventario federado, que consiste en la suma de varios inventarios independientes que en su conjunto constituyen el inventario completo.	a) Sí b) Parcial c) No	Indicar herramienta/s utilizada/s.
Inventario de activos SW	GPF-OCEX 5333: C.1.2	Se dispone de un inventario actualizado de todos los activos <i>software</i> del sistema, incluyendo <i>software de endpoint</i> , <i>software</i> de servidores, y <i>software</i> proporcionado por terceros.	a) Sí b) Parcial c) No	Indicar herramienta/s utilizada/s.
Control de HW no autorizados	GPF-OCEX 5333: C.1.3	La entidad dispone de medidas de seguridad para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados.	a) Sí b) Parcial c) No	Describir controles.
Control de SW no autorizados	GPF-OCEX 5333: C.1.4	Se dispone de una lista de <i>software</i> autorizado y de medidas que permitan detectar el uso de <i>software</i> no autorizado.	a) Sí b) Parcial c) No	Describir controles.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 2 - Seguridad de los activos				
Gestión de vulnerabilidades	GPF-OCEX 5333: C.2.1	Se dispone de procesos para identificar, analizar y priorizar la resolución de las vulnerabilidades.	a) Sí b) Parcial c) No	Indicar herramienta/s utilizada/s.
Parcheo	GPF-OCEX 5333: C.2.2	La entidad dispone de procedimientos y herramientas que permiten aplicar los parches de seguridad publicados por los fabricantes en un tiempo razonable.	a) Sí b) Parcial c) No	Indicar herramienta/s utilizada/s.
<i>Software</i> soportado por el fabricante	GPF-OCEX 5333: C.2.3	Se dispone de un plan de mantenimiento del <i>software</i> y se controlan las fechas de fin de soporte del <i>software</i> .	a) Sí b) Parcial c) No	Aportar plan/es de mantenimiento.
Configuración de seguridad	GPF-OCEX 5333: C.3.1	Se realiza una configuración de seguridad (bastionado) a los equipos, previamente a su puesta en producción.	a) Sí b) Parcial c) No	Describir.
Gestión y mantenimiento de la configuración de seguridad	GPF-OCEX 5333: C.3.2	La entidad dispone de mecanismos que le permiten detectar cambios no autorizados o erróneos de la configuración y su corrección (vuelta a la configuración segura) en un periodo de tiempo oportuno.	a) Sí b) Parcial c) No	Describir.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 3 - Gestión de usuarios y privilegios (de administración)				
Inventario y control de cuentas de administración	GPF-OCEX 5334: D.1.1	Está adecuadamente controlada la asignación del privilegio de administración.	a) Sí b) Parcial c) No	Describir.
Uso dedicado de cuentas de administración	GPF-OCEX 5334: D.1.2	Cuando el usuario tiene diferentes roles frente al sistema (por ejemplo, usuario y administrador) se le asignan identificadores singulares para cada perfil.	a) Sí b) Parcial c) No	Describir.
Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios de la organización	GPF-OCEX 5334: D.1.3	Las cuentas de administración utilizadas por personal interno de la entidad están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.	a) Sí b) Parcial c) No	Aportar política de identificación/autenticación de usuarios.
Mecanismos de autenticación de las cuentas de administración utilizadas por usuarios externos	GPF-OCEX 5334: D.1.4	Las cuentas de administración utilizadas por usuarios externos a la entidad están sujetas a mecanismos de autenticación robustos, que impiden el acceso no autorizado mediante dichas cuentas.	a) Sí b) Parcial c) No	Describir.
Procedimiento de gestión de usuarios	GPF-OCEX 5334: D.2.1	La entidad dispone de un proceso formalmente establecido de solicitud y alta de nuevos usuarios en los sistemas. La entidad dispone de un proceso formalmente establecido para la gestión de las bajas de cuentas de usuarios en el sistema que garantice que no existen cuentas no necesarias.	a) Sí b) Parcial c) No	Aportar procedimiento.
Identificación	GPF-OCEX 5334: D.2.2	Cada entidad (usuario o proceso) que accede al sistema cuenta con un identificador singular que permite reconocerlo y asignarle los derechos de acceso que le corresponden.	a) Sí b) Parcial c) No	Aportar política de identificación/autenticación de usuarios.
Gestión de derechos de acceso	GPF-OCEX 5334: D.2.5	Los derechos de acceso de cada recurso TI se establecen según las decisiones de la persona responsable del recurso, ateniéndose a la política y/o normativa de seguridad del sistema. Se gestionan los derechos de acceso en base al principio de mínimo privilegio.	a) Sí b) Parcial c) No	Describir.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 4 - Monitorización y respuesta				
Centralización y revisión de logs	GPF-OCEX 5333: C.4.4	Se realizan revisiones de los logs y se dispone de herramientas para apoyar la revisión.	a) Sí b) Parcial c) No	Aportar procedimiento que describa las acciones realizadas.
Vigilancia	GPF-OCEX 5333: C.9.3	Se dispone de un sistema automático de recolección de eventos de seguridad.	a) Sí b) Parcial c) No	Nombre de la herramienta.
Monitorización y correlación	GPF-OCEX 5333: C.9.4	La entidad dispone de un SIEM (<i>Security Information and Event Management</i>) o una herramienta de analítica de logs para realizar correlación y análisis de logs.	a) Sí b) Parcial c) No	Nombre de la herramienta.
Centro de Operaciones de Ciberseguridad	GPF-OCEX 5333: C.9.5	La entidad dispone de, o está integrada en un Centro de Operaciones de Ciberseguridad (SOC) que dispone de los medios materiales organizativos necesarios y proporciona servicios de prevención, protección, detección, respuesta y gestión de la seguridad.	a) Sí b) Parcial c) No	Describir.
Procedimiento, notificación, detección y respuesta de incidentes	GPF-OCEX 5333: C.8.1	Se dispone de un proceso integral para tratar los incidentes que puedan tener un impacto en la seguridad del sistema.	a) Sí b) Parcial c) No	Describir.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 5 - Continuidad y resiliencia				
Realización de copias de seguridad	GPF-OCEX 5335: E.1.1	Se realizan copias de seguridad que permitan recuperar los datos perdidos accidental o intencionadamente.	a) Sí b) Parcial c) No	Nombre de la herramienta.
Realización de pruebas de recuperación	GPF-OCEX 5335: E.1.2	La organización ha establecido y aprobado procedimientos formales de restauración de datos y sistemas desde las copias de seguridad. Las pruebas de recuperación de copias se realizan regularmente, con una periodicidad dependiente de la criticidad de los datos y del impacto que causaría la falta de disponibilidad.	a) Sí b) Parcial c) No	Aportar registro de pruebas realizadas.
Protección de las copias de seguridad	GPF-OCEX 5335: E.1.3	Las copias de seguridad se preservan de aquellos riesgos que también podrían afectar a la información original. Por ejemplo copias en distintas ubicaciones y copias desconectadas.	a) Sí b) Parcial c) No	Describir.
Identificación de elementos críticos del negocio	GPF-OCEX 5335: E.2.1	Se ha realizado un análisis de impacto (BIA) en los servicios en el ámbito del ENS.	a) Sí b) Parcial c) No	Aportar BIA.
Plan de recuperación de desastres (DRP). Pruebas.	GPF-OCEX 5335: E.2.2	Existen definidos planes de emergencia, contingencia o recuperación, en consonancia con el Plan de Continuidad general.	a) Sí b) Parcial c) No	Aportar plan/es.
Plan de continuidad. Pruebas.	GPF-OCEX 5335: E.2.3	Se dispone de un Plan de Continuidad documentado, coherente con los resultados del BIA.	a) Sí b) Parcial c) No	Aportar plan/es.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
CBCS 6 - Gobernanza de la ciberseguridad				
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un plan estratégico de TI	a) Sí b) Parcial c) No	Aportar plan estratégico
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un comité de gobierno de las TI con un funcionamiento efectivo.	a) Sí b) Parcial c) No	Aportar tres últimas actas
Gobernanza de las TI	GPF-OCEX 5331	Se dispone de un sistema de gestión de riesgos de TI.	a) Sí b) Parcial c) No	Aportar gestión de riesgos
Cumplimiento normativo	GPF-OCEX 5331	Se dispone de la certificación de cumplimiento del ENS o del plan de adecuación correspondiente.	a) Sí b) Parcial c) No	Aportar correspondiente.
Cumplimiento normativo	GPF-OCEX 5331	Se ha nombrado un DPD.	a) Sí b) Parcial c) No	Aportar nombramiento.
Cumplimiento normativo	GPF-OCEX 5331	Se dispone de un plan de adecuación al Esquema Nacional de Interoperabilidad.	a) Sí b) Parcial c) No	Aportar plan/es.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un plan estratégico de ciberseguridad o de seguridad de la información.	a) Sí b) Parcial c) No	Aportar plan/es.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de una Política de Seguridad de la Información (PSI) formalmente aprobada.	a) Sí b) Parcial c) No	Aportar última PSI aprobada.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un comité de seguridad de la información, formalmente aprobado y con un funcionamiento efectivo.	a) Sí b) Parcial c) No	Aportar constitución.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se dispone de un sistema de gestión de riesgos de seguridad de la información.	a) Sí b) Parcial c) No	Describir.

Subcontrol	Referencia	Objetivo de control	Respuesta	Observaciones
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Se ha nombrado un responsable de seguridad.	a) Sí b) Parcial c) No	Aportar nombramiento.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	Existe un plan de concienciación y de formación en ciberseguridad.	a) Sí b) Parcial c) No	Aportar planes o describir actividades realizadas.
Gobernanza de la ciberseguridad	GPF-OCEX 5314	El personal y los recursos económicos asignados a las TI y a la seguridad de la información se considera adecuado.	a) Sí b) Parcial c) No	Describir.

ANEXO 4. TABLA PARA DOCUMENTAR EL CONOCIMIENTO DEL ENTORNO TI

ENTORNO TI DE: Entidad

FECHA: xx/xx/2026

Cuentas anuales		Aplicaciones (1)					Bases de datos		Sistemas operativos		Plataforma hardware	Observaciones
Epígrafe	Importe gestionado 2025 (euros)	Proceso	Aplicación utilizada	Tipo de aplicación (2)	Puesto y nombre de los responsables funcional/técnico	Control acceso (SO/aplicación) (3)	Marca y versión	Administrador	Marca y Versión	Puesto y nombre del responsable	Identificación marca. Denominación de los servidores	
Contabilidad												
Personal												
Compras-contratación												
Tributos												
Subvenciones												
<i>Añadir si existen otras aplicaciones relevantes para la gestión económica de la entidad</i>												

(1) Si alguno de estos procesos/aplicaciones es mantenido por un proveedor de servicios externo, indicarlo en el apartado de observaciones, señalando el nombre del proveedor y la fecha del contrato.

(2) Adquirida o de desarrollo propio.

(3) Entorno que ofrece el control en el acceso lógico a la aplicación: delegada en el sistema operativo (SO) u otro sistema o de la propia aplicación.

Nota: En el caso de aplicaciones que soportan procesos que se van a auditar, adjuntar el modelo de datos de la base de datos o la documentación existente sobre el modelo de datos, los manuales de usuario de la aplicación y los informes de auditoría de sistemas de información sobre la aplicación realizados en el último año. Solo se aportará la información que se disponga, no es necesario elaborar documentación ad hoc. Si no se dispone de documentación, señalarlo.