

1. Introducción
2. Los Controles Básicos de Ciberseguridad
3. Revisión de cumplimiento de la legalidad
4. Objetivos de la auditoría de los CBCS
5. Alcance del trabajo de revisión
6. Procedimientos de auditoría y programa de trabajo
7. Evaluación de las deficiencias detectadas
8. Bibliografía
Anexo 1 Por qué son importantes los controles básicos de ciberseguridad
Anexo 2 Cuestionario básico de Ciberseguridad
Anexo 3 Programa de auditoría (fichas de revisión)
Anexo 4 Niveles de madurez
Anexo 5 Tipos de ciberincidentes

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 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.

También se mencionan 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:

- Realizar una auditoría de ciberseguridad consistente en un análisis a fondo de la cuestión en un determinado ente.

Podría ser similar a una auditoría de seguridad de las requeridas por el ENS¹ o una auditoría siguiendo la metodología de ISACA². Un trabajo de este tipo entraña una intensa dedicación de personal especializado tanto para el auditor como para el ente auditado.

- La revisión de aspectos directamente relacionados con las áreas significativas en una auditoría financiera. Consistirá en la revisión de los Controles Generales de Tecnologías de la Información (CGTI) relacionados únicamente con las áreas significativas para los fines de la auditoría financiera del ente auditado. Una parte significativa de dichos controles está formada por controles de ciberseguridad. Este es el objeto de la GPF-OCEX 5330.

- La revisión de una serie de controles básicos de ciberseguridad.

Los controles básicos de ciberseguridad son un subconjunto reducido de los controles de ciberseguridad. Su revisión permitirá 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. Será por tanto un trabajo más viable en entes que no dispongan de muchos recursos técnicos o humanos.

Un enfoque de este tipo es el que motiva el desarrollo de la presente guía.

¹ Siguiendo por ejemplo las guías CCN-STIC-802, 808 y 804.

² En la bibliografía final se citan dos guías de ISACA que podrían utilizarse para este propósito.

2. Los Controles Básicos de Ciberseguridad (CBCS)

En el desarrollo de esta GPF-OCEX 5313, cuyo contenido está fundamentalmente relacionado con la auditoría de la seguridad de la información, se ha tenido especial cuidado en mantener la máxima coherencia con los postulados del ENS puesto que es de obligado cumplimiento para todos los entes públicos y esta alineación facilita la realización de las auditorías de ciberseguridad y coadyuvan a la implantación del ENS. No obstante, dada su amplitud, se han seleccionado, por las razones señaladas en el apartado anterior, una serie limitada de controles para su revisión. Con objeto de seleccionar los más relevantes se ha atendido al marco conceptual establecido por el Center for Internet Security³ (CIS) que prioriza y clasifica los controles según su importancia para hacer frente a las ciberamenazas.⁴

Tal como se señala en el anexo 4 de la GPF-OCEX 5311, los controles de seguridad críticos del CIS son un conjunto conciso y **priorizado** de acciones de ciberdefensa, orientados a mitigar los ataques más comunes y dañinos con la intención de automatizarlos lo máximo posible. Incluyen 20 controles de seguridad de la información alineados con la publicación NIST⁵ 800-53. En agosto de 2016 se publicó la versión 6.1, y en 2018 se han actualizado a la versión 7 y se ha cambiado su denominación a **Controles CIS**. Estos controles están pensados para organizaciones de cualquier tipo.

Según el CIS⁶, con carácter general, las organizaciones que apliquen sólo los cinco primeros controles pueden reducir su riesgo ante ciberataques alrededor del 85%. Si se implementan los 20 controles el riesgo se puede reducir un 94%. La nueva versión 7 clasifica los 6 primeros controles como **Básicos** y son los que se han utilizado como referencia en esta guía para establecer los controles básicos de ciberseguridad (CBCS) de los OCEX.

Además de los seis controles CIS básicos se ha incluido en los CBCS el control “Copias de seguridad de datos y sistemas” (control CIS número 10) ya que es un elemento fundamental para mantener un grado razonable de ciber-resiliencia⁷. Si todos los controles preventivos fallan y un ciberataque traspasa todas las líneas de defensa y tiene éxito, el último recurso de la entidad atacada es restaurar sus sistemas y datos en un plazo predeterminado para poder continuar prestando sus servicios.

³ Organización de reconocido prestigio internacional.

⁴ No es el único marco de ciberseguridad que establece una priorización de controles, pero sí es uno de los más reconocidos internacionalmente. Son varios los países que han establecido listas priorizadas de medidas de ciberseguridad, por ejemplo, la Australian National Audit Office en su reciente informe [Cyber Resilience](#) establece como criterio de auditoría las estrategias de mitigación de las ciberamenazas denominadas Essential Eight, que deben aplicar las entidades públicas de ese país.

⁵ U.S. National Institute of Standards and Technology.

⁶ Guide to the First 5 CIS Controls (v6.1).

⁷ Ciber-resiliencia es la capacidad para continuar prestando servicios mientras se previenen y responden los ciberataques. También reduce la probabilidad de que los ciberataques tengan éxito. Para ser ciber-resiliente, una entidad pública debe tener implementado un sólido sistema de CGTI, cuya función es proporcionar un entorno TI fiable sobre el que otros procesos y controles TI pueden apoyarse y funcionar.

Los siete controles básicos de ciberseguridad debidamente referenciados con el ENS son:

Control		Objetivo de control	Medidas de seguridad del ENS
CBCS 1	Inventario y control de dispositivos físicos	Gestionar activamente todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.	op.exp.1
CBCS 2	Inventario y control de software autorizado y no autorizado	Gestionar activamente todo el software en los sistemas, de forma que sólo se pueda instalar y ejecutar software autorizado.	op.exp.1 op.exp.2
CBCS 3	Proceso continuo de identificación y remediación de vulnerabilidades	Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remedarlas y reducir la ventana de oportunidad a los atacantes.	mp.sw.2 op.exp.4
CBCS 4	Uso controlado de privilegios administrativos	Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.	op.acc.4 op.acc.5
CBCS 5	Configuraciones seguras del software y hardware de dispositivos móviles, portátiles, equipos de sobremesa y servidores	Implementar la configuración de seguridad de dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarla activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir que los atacantes exploten servicios y configuraciones vulnerables.	op.exp.2 op.exp.3
CBCS 6	Registro de la actividad de los usuarios	Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.	op.exp.8 op.exp.10
CBCS 7	Copias de seguridad de datos y sistemas	Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.	mp.info.9

Figura 1

Sin duda una auditoría de los 20 controles CIS o una auditoría siguiendo el ENS⁸, 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 y puesto que los CBCS están priorizados, de más efectivos a menos, una alternativa con mejor relación coste/beneficio consiste en diseñar un plan de trabajo basado en los siete controles básicos de ciberseguridad más los controles de legalidad del siguiente apartado, criterio que recoge esta guía⁹.

⁸ De acuerdo con la *Guía de auditoría del ENS CCN-STIC-802*.

⁹ Los Controles CIS ya se han usado como criterios de auditoría de referencia en auditorías de ciberseguridad realizadas por auditores públicos de prestigio reconocido. Véase como ejemplo el informe del Auditor General of British Columbia de Octubre 2017, [An Independent Audit of the Regional Transportation Management Centre's Cybersecurity Controls](#).

3. Revisión de cumplimiento de la legalidad

Además de los CBCS vistos en el apartado anterior, en este tipo de revisión se incluirá la verificación del cumplimiento de diversas normas relacionadas con la seguridad de la información:

Control de legalidad		Objetivo de cumplimiento	Medidas de seguridad del ENS
CBCS 8	Cumplimiento del ENS	<ul style="list-style-type: none"> Política de seguridad y responsabilidades Declaración de aplicabilidad Informe de Auditoría (nivel medio o alto) Informe del estado de la seguridad Publicación de la declaración de conformidad y los distintivos de seguridad en la sede electrónica 	Org1 Art 27.4 Art.34 Art.35 Art.41
	Cumplimiento de la LOPD/RGPD	<ul style="list-style-type: none"> Nombramiento del DPD Registro de actividades de tratamiento Análisis de riesgos y evaluación del impacto de las operaciones de tratamiento (<i>para los de riesgo alto</i>) Informe de auditoría de cumplimiento (<i>cuando el responsable del tratamiento haya decidido realizarla</i>) 	--
	Cumplimiento de la Ley 25/2013, de 27 de diciembre (<i>Impulso de la factura electrónica y creación del registro contable de facturas</i>)	<ul style="list-style-type: none"> Informe de auditoría de sistemas anual¹⁰ del Registro Contable de Facturas 	--

Figura 2

4. Objetivos de la auditoría de los CBCS

El objetivo de la auditoría es proporcionar una evaluación sobre el diseño y la eficacia operativa de los controles básicos de ciberseguridad mediante:

- La identificación de deficiencias de control interno 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 sistema auditado en relación con el nivel de ciberseguridad implantado. No obstante, la auditoría proporcionará información relevante sobre el grado de ciberseguridad y ciber-resiliencia de la entidad y sobre posibles acciones de mejora aconsejables.

¹⁰ De acuerdo a lo exigido en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público (*Artículo 12 apartado 3*). La "Guía para las auditorías de los Registros Contables de Facturas" de la IGAE, establece como uno de los objetivos de dichas auditorías la "Revisión de la gestión de la seguridad en aspectos relacionados con la confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad de los datos y servicios de gestión."

5. Alcance del trabajo de revisión

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

La revisión de los 8 CBCS debería incluirse como **procedimiento mínimo obligatorio** en todas las fiscalizaciones de regularidad de los OCEX, ya que los riesgos de ciberseguridad deben tener una especial consideración en todas las auditorías financieras.

b) En el marco de una auditoría de un proceso específico o una auditoría operativa:

- Los sistemas directamente relacionados con la actividad de la entidad, (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 sobre ciberseguridad se seleccionarán:

- Los sistemas que se espere que tengan todos los entes a revisar, con objeto de poder realizar análisis comparativos.
- 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, 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 integren la aplicación de gestión (ej. servidor web, servidor de aplicación, servidor 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.)

Recordemos que la estructura simplificada de un sistema de información puede representarse así:

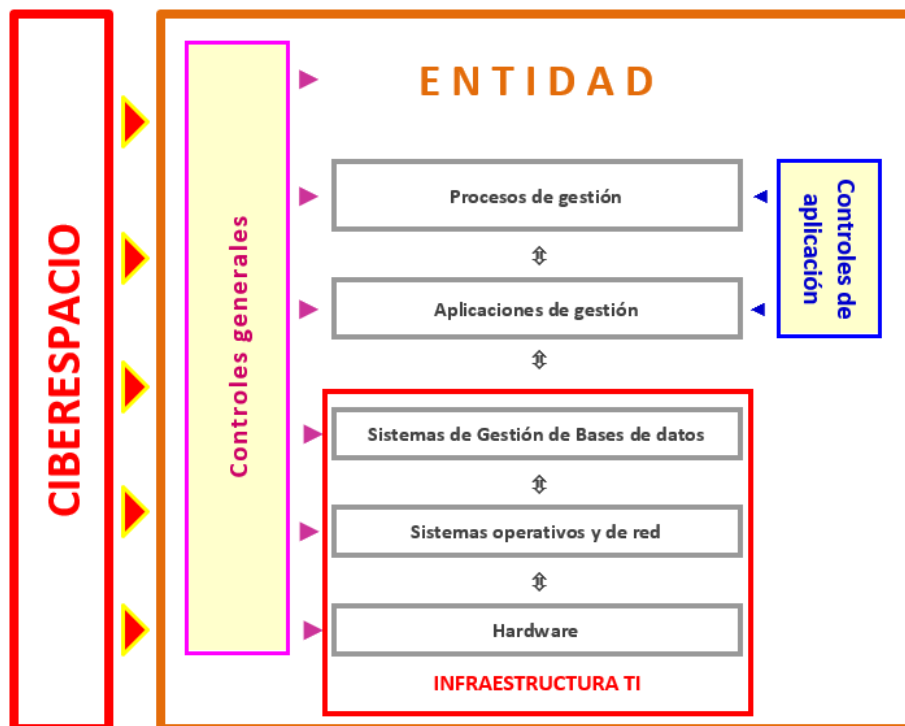


Figura 3

Por último, señalar que los sistemas seleccionados siempre deberán estar incluidos en el ámbito de aplicación del ENS¹¹, y estar clasificados en las categorías media y alta según el ENS.

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 tanto en los papeles de trabajo y reflejado en el informe resultado del mismo.**

6. Procedimientos de auditoría y programa de trabajo

Se deberá mantener una reunión con los responsables de la entidad para explicar el trabajo que se va a realizar, en la cual se entregará el cuestionario del Anexo 4 para que sea cumplimentado por el responsable de seguridad de la entidad auditada, quien deberá estar presente en la reunión.

Posteriormente, tras analizar el cuestionario, se cumplimentará el **programa de trabajo del Anexo 3**, para lo cual en general, los auditores deberán mantener otras reuniones con los distintos responsables y se obtendrán las evidencias precisas.

Estos procedimientos deberán ser llevados a cabo por personal especializado, idóneamente por auditores de sistemas de información o por informáticos que presten apoyo a los auditores. De no disponer de personal especializado en los OCEX, se deberá contar con especialistas externos.

Determinadas comprobaciones podrán darse por cumplidas si la entidad presenta las legalmente obligatorias auditorías de seguridad (ENS).

Confianza en las auditorías del ENS.

Dado que los CBCS están alineados con el ENS, cuando su revisión se realice en entidades que hayan pasado la auditoría de seguridad obligatoria establecida en el artículo 34 del RD 3/2010 por el que se aprueba el ENS, la revisión podrá basarse, en la medida de lo posible, en los resultados de dicha auditoría.

¹¹ Véase la guía GCN-STIC-830





A los efectos de la presente guía, para depositar confianza en dichas auditorías deberán cumplir con los requisitos legalmente establecidos¹², entre otros, las entidades certificadoras deberán estar acreditadas y constar en la sección [Entidades de certificación acreditadas](#) de la página web del CCN.

Si depositamos confianza en estas auditorías deberá señalarse expresamente en el informe.

7. Evaluación de los hallazgos de auditoría

Los resultados del trabajo se analizarán y evaluarán a dos niveles:

- a) Cada uno de los CBCS señalados en las Figuras 1 y 2 está compuesto por una serie de subcontroles o controles detallados, que están relacionados en las fichas de revisión del Anexo 3. En estas fichas se debe documentar el trabajo realizado y concluir para cada subcontrol, en base a las evidencias obtenidas sobre su eficacia, pudiendo encontrarse cada uno de ellos en alguna de las siguientes situaciones:

	Control efectivo
	Control bastante efectivo
	Control poco efectivo
	Control no efectivo o no implantado

- b) Los CBCS son controles globales (compuestos por subcontroles) y se evaluará cada uno de ellos utilizando el modelo de nivel de madurez (ver Anexo 4). Para evaluar su nivel de madurez se tendrá en cuenta los resultados obtenidos en los subcontroles que lo forman y la importancia relativa de estos para el cumplimiento del objetivo de control del CBCS.

Se seguirán los criterios de evaluación establecidos en el apartado 8. *Evaluación de las deficiencias de control interno detectadas*, de la GPF-OCEX 5330.

En todo caso, los resultados de la revisión de los controles básicos de ciberseguridad se comunicarán de forma detallada al responsable de seguridad de la Entidad.

Si los resultados obtenidos de acuerdo con el modelo de nivel de madurez no alcanzan el nivel mínimo de exigencia requerido¹³, se valorará la realización de una auditoría de ciberseguridad de mayor amplitud.

¹² Véanse la Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información, y la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

¹³ Según el Informe nacional del estado de seguridad de los sistemas de las tecnologías de la información y la comunicación, de 2018, apartado 3.1, en los diferentes perfiles se evalúan los controles mediante un nivel de exigencia, también conocido como nivel de madurez, en la aplicación de las diferentes medidas de seguridad, y el nivel mínimo de exigencia requerido será:

CATEGORÍA DEL SISTEMA	NIVEL MÍNIMO DE EXIGENCIA REQUERIDO
BÁSICA	L2 – Reproducible, pero intuitivo (50%)
MEDIA	L3 – Proceso definido (80%)
ALTA	L4 – Gestionado y medible (90%)

8. Bibliografía

- [Centro Criptológico Nacional:](#)
 - Guía CCN-STIC-802, Guía de auditoría del ENS, 2017.
 - Guía CCN-STIC 804, Guía de Implantación del ENS, 2017.
 - Guía CCN-STIC-808, Verificación del cumplimiento de las medidas en el ENS, 2017.
 - Informe nacional del estado de seguridad de los sistemas de las tecnologías de la información y la comunicación, 2018.
- [Ciberseguridad. Una guía de supervisión](#), Instituto de Auditores Internos de España, 2016.
- [Código de Derecho de la Ciberseguridad](#), BOE, julio 2018.
- [Cybersecurity Risk Considerations in a Financial Statement Audit](#), Institute of Singapore Chartered Accountants, junio 2018.
- [Esquema Nacional de Seguridad](#).
- [GPF-OCEX 5311 Ciberseguridad, seguridad de la información y auditoría externa](#), 27/11/2017.
- ISACA:
 - [CIS Controls Audit/Assurance Program](#), 2017.
 - [IS Audit/Assurance Program. Cybersecurity: Based on the NIST Cybersecurity Framework](#), 2016.
- [The Center for Internet Security:](#)
 - The Critical Security Controls for Effective Cyber Defense, Version 7, 19/3/2018.
 - CIS Controls Measures and Metrics for Version 7, 2018.
 - Guide to the First 5 CIS Controls (v6.1), 2017.
- [Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información](#).
- SANS Institute, Back to Basics: Focus on the First Six CIS Critical Security Controls, enero 2017.

Anexo 1. Por qué son importantes los controles básicos de ciberseguridad (CBCS)¹⁴

CBCS 1 Inventario y control de dispositivos físicos

Objetivo de control: Gestionar activamente (inventariar, revisar y corregir) todos los dispositivos hardware en la red, de forma que sólo los dispositivos autorizados tengan acceso a la red.

Este control ayuda a las organizaciones a definir la base de lo que hay que 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.

En cualquier caso, el objetivo inicial del control es conocer lo que está en la red para que pueda ser defendido y, posteriormente, impedir que dispositivos no autorizados se unan a la red.

¿Por qué es importante este control?

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. 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.

Otros dispositivos que se conectan a la red corporativa (p.e. sistemas para demostraciones, redes para invitados, etc.) deben ser gestionados con cuidado o aislados para prevenir accesos no autorizados que comprometan la seguridad.

Los dispositivos personales de los empleados (portátiles, tabletas, móviles) que se conecten a la red corporativa también pueden verse comprometidos y ser usados para infectar los recursos internos.

El adecuado control de todos los dispositivos también juega un papel crítico en la planificación y ejecución de las copias de seguridad del sistema y en su recuperación.

¿Qué dice el ENS?

“Artículo 20. Integridad y actualización del sistema

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.”

Medidas de seguridad:

“4.3.1 Inventario de activos (op.exp.1)

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.”

Guía CCN-STIC 804: 4.3.1 [OP.EXP.1] INVENTARIO DE ACTIVOS

“183. El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema de información, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.

- Identificación del activo: fabricante, modelo, número de serie
- Configuración del activo: perfil, política, software instalado
- Software instalado: fabricante, producto, versión y parches aplicados
- Equipamiento de red: MAC, IP asignada (o rango)

¹⁴ Fuente: *The Critical Security Controls for Effective Cyber Defense, Esquema Nacional de Seguridad* y elaboración propia.

- Ubicación del activo: ¿dónde está?
- Propiedad del activo: persona responsable del mismo.”

CBCS 2 Inventario y control de software autorizado y no autorizado

Objetivo de control: Gestionar activamente (inventariar, revisar y corregir) todo el software en la red, de forma que sólo se pueda instalar y ejecutar software autorizado y que el no autorizado sea detectado y se evite su instalación y ejecución.

La finalidad de este control es asegurar que sólo está permitido ejecutar software autorizado en los sistemas de la organización impidiendo la ejecución de software potencialmente vulnerable.

Mantener un inventario de software es importante, y disponer de una lista blanca de aplicaciones autorizadas es un factor crucial de este proceso, ya que limita la capacidad de ejecutar aplicaciones únicamente a aquellas que están expresamente autorizadas.

Aunque no es una solución mágica para la defensa, este control a menudo se considera uno de los más eficaces para la prevención y detección de ciberataques.

La implementación del control a menudo requiere que las organizaciones reconsideren sus políticas y su cultura, los usuarios ya no podrán instalar el software que deseen. Pero este control está implementado con éxito por numerosas organizaciones, y probablemente ayudará a prevenir y detectar ciberataques.

¿Por qué es importante este control?

Los atacantes escanean continuamente las organizaciones objetivo buscando versiones vulnerables de software que puedan explotarse remotamente. Algunos atacantes también distribuyen páginas web hostiles, archivos de documentos, archivos multimedia y otros contenidos a través de sus propias páginas web o sitios de terceros de confianza. Cuando las víctimas desprevenidas acceden a este contenido con un navegador vulnerable u otro programa, los atacantes comprometen sus máquinas, a menudo instalando programas ocultos y bots¹⁵ que le dan al atacante un control a largo plazo del sistema. Sin el conocimiento o el control apropiados del software desplegado en una organización, los defensores no pueden asegurar adecuadamente sus activos.

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 ha 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.

Las organizaciones que no tienen inventarios completos de software no pueden encontrar software vulnerable o malicioso para mitigar problemas o eliminar a los atacantes.

El control de todo el software también desempeña un papel fundamental en la planificación y ejecución de copias de seguridad y en la recuperación del sistema.

Las listas blancas protegen los sistemas de información de que aplicaciones no autorizadas se ejecuten en ellos, protegiéndolos de aplicaciones dañinas. Son aplicables a servidores, equipos de sobremesa y portátiles.

¿Qué dice el ENS?

“Artículo 20. Integridad y actualización del sistema

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

¹⁵ Según Wikipedia un bot (aféresis de robot) es un programa informático que efectúa automáticamente tareas repetitivas a través de Internet.

2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.”

Medidas de seguridad:

“4.3.1 Inventario de activos (op.exp.1)

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que es responsable de las decisiones relativas al mismo.”

Guía CCN-STIC 804: 4.3.1 [OP.EXP.1] INVENTARIO DE ACTIVOS

“183. El inventario debe cubrir todo el dominio de seguridad del responsable de la seguridad del sistema de información, hasta alcanzar los puntos de interconexión y los servicios prestados por terceros. La granularidad debe ser suficiente para cubrir las necesidades de reporte de incidentes y para hacer un seguimiento, tanto formal (auditorías) como reactivo en el proceso de gestión de incidentes.

- Identificación del activo: fabricante, modelo, número de serie
- Configuración del activo: perfil, política, software instalado
- **Software instalado: fabricante, producto, versión y parches aplicados**
- Equipamiento de red: MAC, IP asignada (o rango)
- Ubicación del activo: ¿dónde está?
- Propiedad del activo: persona responsable del mismo.”

CBCS 3

Proceso continuo de identificación y remediación de vulnerabilidades

Objetivo de control: Disponer de un proceso continuo para obtener información sobre nuevas vulnerabilidades, identificarlas, remediarlas y reducir la ventana de oportunidad a los atacantes.

El objetivo de este control es 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 punteras implementan sistemas de administración de parches y actualizaciones que cubren vulnerabilidades tanto de sistemas operativos como aplicaciones de terceros.

Esto permite de forma automática, continua y proactiva la instalación de actualizaciones para solucionar vulnerabilidades del software.

Las organizaciones deben implementar herramientas de gestión de vulnerabilidades para dotarse de la capacidad de detectar y remediar debilidades de software explotables.

¿Por qué es importante este control?

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.

¿Qué dice el ENS?

“Artículo 20. Integridad y actualización del sistema

2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.”

Medidas de seguridad:

“5.6.2 Aceptación y puesta en servicio (mp.sw.2)

Categoría BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

a) Se comprobará que:

1.º Se cumplen los criterios de aceptación en materia de seguridad.

2.º No se deteriora la seguridad de otros componentes del servicio.

b) Las pruebas se realizarán en un entorno aislado (preproducción).

c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.

b) Pruebas de penetración.

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de coherencia en la integración en los procesos.

b) Se considerará la oportunidad de realizar una auditoría de código fuente.”

“4.3.3 Gestión de la configuración (op.exp.3)

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).”

“4.3.4 Mantenimiento (op.exp.4)

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

b) Se efectuará un seguimiento continuo de los anuncios por defectos.

c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.”

Guía CCN-STIC 804: “4.3.4 [OP.EXP.4] MANTENIMIENTO

199. Proactivamente se deberá estar informado de los defectos anunciados por parte del fabricante o proveedor (como por ejemplo mediante suscripciones a listas de correo o RSS, consultando noticias en webs de tecnología, seguridad o fabricantes, etc.).

200. Deberá existir un procedimiento para establecer cuándo implantar los cambios y determinar su prioridad y urgencia proporcionada al riesgo que implica su no aplicación (cambios preaprobados, cambios de emergencia, etc.).”

CBCS 4 Uso controlado de privilegios administrativos

Objetivo de control: Desarrollar procesos y utilizar herramientas para identificar, controlar, prevenir y corregir el uso, asignación y configuración de privilegios administrativos en ordenadores, redes y aplicaciones.

Este control garantiza que los privilegios de administración de sistemas estén asignados únicamente a los empleados que los necesitan, en base a las funciones que desempeñan, y que la entidad pueda atribuir las acciones administrativas a usuarios individuales.

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.

¿Por qué es importante este control?

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.

La revisión de este control puede orientarse a verificar la existencia de una política de alta, baja y mantenimiento de usuarios administradores, y la fortaleza de las contraseñas y las tareas que se desarrollan para comprobar su cumplimiento.

Por otro lado, también podemos solicitar el listado de usuarios definidos en los sistemas y los ficheros de contraseñas cifradas asociados, y comprobar que no disponen de las claves por defecto utilizando herramientas automáticas.

¿Qué dice el ENS?

“Artículo 16. Autorización y control de los accesos.

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.”

Medidas de seguridad:

“4.2 Control de acceso (op.acc)

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.

En todo control de acceso se requerirá lo siguiente:

- a) Que todo acceso esté prohibido, salvo concesión expresa.
- b) Que la entidad quede identificada singularmente [op.acc.1].
- c) Que la utilización de los recursos esté protegida [op.acc.2].
- d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
- e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
- f) Que la identidad de la entidad quede suficientemente autenticada [op.acc.5].
- g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).”

“4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:

- a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.
- b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
- c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.”

Guía CCN-STIC 804: “4.2.4 [OP.ACC.4] PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

121. En la estructuración de los derechos de acceso se deben en cuenta las necesidades de cada usuario según su función en la organización y las tareas que tiene encomendadas.

122. La necesidad de acceso debe venir por escrito de parte del responsable de la información o proceso al que va a concedérsele acceso.
123. El reconocimiento de la necesidad de acceso debe ser reasegurado periódicamente, extinguiéndose cuando no se demuestre positivamente que la necesidad perdura.
124. Deberá prestarse una especial atención a las cuentas de administración del sistema (administración de equipos, de aplicaciones, de comunicaciones, de seguridad), estableciendo procedimientos ágiles de cancelación y mecanismos de monitorización del uso que se hace de ellas.”

“4.2.5 Mecanismo de autenticación [op.acc.5].

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens).
- "algo que se es": elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema se denominarán **credenciales**.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Nivel BAJO

- a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.
- b) En el caso de utilizarse como factor "algo que se sabe", se aplicarán reglas básicas de calidad de la misma.
- c) Se atenderá a la seguridad de las credenciales de forma que:
 1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
 2. Las credenciales estarán bajo el control exclusivo del usuario.
 3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
 4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
 5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

- a) Se exigirá el uso de al menos dos factores de autenticación.
- b) En el caso de utilización de "algo que se sabe" como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.

- c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:
1. Presencial.
 2. Telemático usando certificado electrónico cualificado.
 3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

- a) Las credenciales se suspenderán tras un periodo definido de no utilización.
- b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
- c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma."

"4.3.8 Registro de la actividad de los usuarios (op.exp.8) #SOLO ADMINISTRADORES DE SISTEMAS#

Se registrarán las actividades de los usuarios en el sistema, de forma que:

- a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
- b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
- c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
- d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel MEDIO (dimensión trazabilidad)

Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO (dimensión trazabilidad)

Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada."

CBCS 5 Configuraciones seguras del hardware y software de dispositivos móviles, portátiles, equipos de sobremesa y servidores

Objetivo de control: Establecer una configuración base segura para dispositivos móviles, portátiles, equipos de sobremesa y servidores, y gestionarlas activamente utilizando un proceso de gestión de cambios y configuraciones riguroso, para prevenir a los atacantes explotar servicios y configuraciones vulnerables.

Por defecto, la mayoría de los sistemas están configurados para la facilitar su uso y no necesariamente pensando en la seguridad. Para implantar este control, las organizaciones necesitan reconfigurar los sistemas de acuerdo con estándares de seguridad.

¿Por qué es importante este control?

Tal como lo entregan los fabricantes y vendedores, las configuraciones predeterminadas para los sistemas operativos y las aplicaciones están normalmente orientadas a la facilidad de implementación 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.

¿Qué dice el ENS?

“Artículo 19. Seguridad por defecto.

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

- a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.
- c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.
- d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.”

Medidas de seguridad:

“4.3.2 Configuración de seguridad (op.exp.2)

Se configurarán los equipos previamente a su entrada en operación, de forma que:

- a) Se retiren cuentas y contraseñas estándar.
- b) Se aplicará la regla de «mínima funcionalidad»:
 - 1.º El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,
 - 2.º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
 - 3.º Se eliminará o desactivará mediante el control de la configuración aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.
- c) Se aplicará la regla de «seguridad por defecto»:
 - 1.º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
 - 2.º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
 - 3.º El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.”

Guía CCN-STIC 804: “4.3.2 [OP.EXP.2] CONFIGURACIÓN DE SEGURIDAD

187. Todos los sistemas deben ser configurados de forma sistemática antes de entrar en producción. El organismo debe elaborar unos pocos perfiles de configuración para las diferentes actividades a que pueden ser dedicados, siendo típicos los siguientes:

- usuarios normales (uso administrativo)
- atención a clientes
- gestión de proveedores (incluidos bancos)
- desarrollo
- operadores y administradores (técnicos de sistemas)
- responsable de seguridad (consola de configuración)
- auditoría

188. La medida se instrumenta por medio de una lista de verificación (checklists) que se debe aplicar sistemáticamente a cada equipo antes de entrar en producción.
189. En todos los perfiles de usuario, excepto en los de administrador, se debe bloquear la opción de que éste pueda cambiar la configuración del sistema o pueda instalar nuevos programas o nuevos periféricos (drivers).
190. La configuración de seguridad debe incluir un perfil básico de auditoría de uso del equipo.”

“4.3.3 Gestión de la configuración (op.exp.3)

(Categoría Media)

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

- a) Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
- b) Se mantenga en todo momento la regla de "seguridad por defecto" ([op.exp.2]).
- c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).
- d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).
- e) El sistema reaccione a incidentes (ver [op.exp.7]).”

CBCS 6

**Registro de la actividad de los usuarios
(Mantenimiento, monitorización y análisis de los LOG de auditoría)**

Objetivo de control: Recoger, gestionar y analizar logs de eventos que pueden ayudar a detectar, entender o recuperarse de un ataque.

Implica que todos los sistemas y aplicaciones deberían tener habilitadas las trazas de auditoría, incluyendo respuestas a desde dónde, quién, qué y cuándo, así como tener definidas acciones de alerta.

Debería existir una política asociada, un formato de log corporativo y una tarea de análisis de logs. En organizaciones con presupuesto y personal suficiente se suele disponer de un SIEM (Security Information and Event Management), sistema que permite disponer en tiempo real de alertas de seguridad.

La mayoría de los sistemas operativos, servicios de red y firewall, tanto libres como comerciales, ofrecen capacidades de log, pero tales registros deben ser activados. Firewalls, proxies y sistemas de acceso remoto (VPN, telefónico, etc.) deben ser configurados para el registro detallado y almacenar toda la información disponible para el caso de una investigación. Además, los sistemas operativos, especialmente los de servidores, deben estar configurados para crear registros de control de acceso cuando un usuario intenta acceder a recursos sin los privilegios adecuados. Para evaluar si tal registro está operativo, la organización debe escanear periódicamente sus logs y compararlos con el inventario de activos instalado como parte del Control 1 para asegurar que cada elemento conectado a la red está generando periódicamente logs.

Los programas analíticos para revisar registros pueden ser valiosos, pero los medios empleados para analizar los logs de auditoría son bastante diversos, incluso un rápido examen realizado por una persona es importante para esa finalidad. Las herramientas de correlación pueden hacer mucho más útiles los registros de auditoría para una posterior inspección manual. Tales herramientas pueden ser muy útiles en la identificación de ataques sutiles. Sin embargo, estas herramientas no son una panacea ni un reemplazo para los administradores de sistemas y personal experimentado de seguridad de la información. Incluso con herramientas de análisis de registro automatizado, se requiere la intuición y experiencia humana para identificar y comprender los ataques.

¿Por qué es importante este control?

Deficiencias en el registro de seguridad y en su análisis permiten a los atacantes ocultar su ubicación, el software malicioso introducido y las actividades ilícitas que realizan en las máquinas víctimas. Incluso si las víctimas saben que sus sistemas han sido comprometidos, sin registros de logs completos y protegidos, permanecen ciegos a los detalles del ataque y a las posteriores acciones de los atacantes.

Sin unos logs de auditoría sólidos, 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.

¿Qué dice el ENS?

“Artículo 23. Registro de actividad

Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.”

Medidas de seguridad:

“4.3.8 Registro de la actividad de los usuarios (op.exp.8)

Se registrarán las actividades de los usuarios en el sistema, de forma que:

- a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.
- b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.
- c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.
- d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel MEDIO (dimensión trazabilidad)

Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO (dimensión trazabilidad)

Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada.”

Guía CCN-STIC 804: “4.3.8 [OP.EXP.8] REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

225. Se realiza una inspección regular de los registros para identificar anomalías en el uso de los sistemas (uso irregular o no previsto)

226. Se utilizan herramientas automáticas para recoger y analizar los registros en busca de actividades fuera de lo normal (por ejemplo: consola de seguridad centralizada, SIEM).”

“4.3.10 Protección de los registros de actividad [op.exp.10].

Nivel ALTO

Se protegerán los registros del sistema, de forma que:

- a) Se determinará el periodo de retención de los registros.
- b) Se asegurará la fecha y hora. Ver [mp.info.5].
- c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.
- d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.”

Guía CCN-STIC 804: “4.3.10 [OP.EXP.10] PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

236. Se deberán retener los registros de manera adecuada:

- existe una declaración formal de los periodos de retención habituales
- existe un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención

- existe un procedimiento formal para la retención de evidencias tras un incidente
237. Existen mecanismos que garanticen la corrección de la hora a la que se realiza el registro, en prevención de manipulaciones de los relojes.
238. Únicamente el personal autorizado podrá modificar o eliminar los registros:
- existen mecanismos para prevenir el acceso a los registros de personas no autorizadas
 - existen mecanismos para prevenir el acceso de personas no autorizadas a la configuración del sistema para el registro automático de actividades
 - existe un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad
239. Los registros están contemplados en los procesos de copias de seguridad, garantizando las seguridades antes mencionadas.”

CBCS 7 Copias de seguridad de datos y sistemas

Objetivo de control: Utilizar procesos y herramientas para realizar la copia de seguridad de la información crítica con una metodología probada que permita la recuperación de la información en tiempo oportuno.

¿Por qué es importante este control?

Cuando los atacantes comprometen los sistemas, a menudo realizan cambios significativos de las configuraciones y el software. En ocasiones, los atacantes también realizan alteraciones sutiles de los datos almacenados en los sistemas comprometidos, lo que puede poner en peligro la eficacia de la organización con información contaminada.

Cuando se descubre a los atacantes, puede ser extremadamente difícil para las organizaciones sin una capacidad confiable de recuperación de datos eliminar todos los aspectos de la presencia del atacante en los sistemas.

Otras consideraciones

Periódicamente, por ejemplo, trimestralmente, y cada vez que se compra un nuevo sistema para la realización de copias de seguridad, un equipo de pruebas debe evaluar una muestra aleatoria de las copias de seguridad realizadas intentando restaurarlas en un entorno pruebas. Las **pruebas de recuperación** de los sistemas restaurados deben incluir la verificación no sólo del proceso de recuperación, sino también de su contenido, es decir, que el sistema operativo, la aplicación y los datos de la copia de seguridad estén intactos y sean funcionales.

Los ciberataques mediante ransomware 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 los backups. 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 la de cifrado y seguridad física.

¿Qué dice el ENS?

“Artículo 7. Prevención, reacción y recuperación.

4. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.”

“Artículo 21. Protección de información almacenada y en tránsito

2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.”

“Artículo 25. Continuidad de la actividad.

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.”

Medidas de seguridad:

“5.7.7 Copias de seguridad (mp.info.9)

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

- a) Información de trabajo de la organización.
- b) Aplicaciones en explotación, incluyendo los sistemas operativos.
- c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
- d) Claves utilizadas para preservar la confidencialidad de la información.”

Guía CCN-STIC 804: “5.7.7 [MP.INFO.9] COPIAS DE SEGURIDAD (BACKUP)

596. Se deben realizar copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad a determinar por la organización.

597. Las copias de respaldo poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, debe considerarse la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad (en cuyo caso se estará a lo dispuesto en [op.exp.11]).

598. Se recomienda establecer un proceso de autorización para la recuperación de información de las copias de respaldo.

599. Se recomienda conservar las copias de respaldo en lugar(es) suficientemente independiente(s) de la ubicación normal de la información en explotación como para que los incidentes previstos en el análisis de riesgos no se den simultáneamente en ambos lugares, por ejemplo, si se conservan en la misma sala utilizar un armario ignífugo.

600. El transporte de copias de respaldo desde el lugar donde se producen hasta su lugar de almacenamiento garantiza las mismas seguridades que los controles de acceso a la información original.

601. Las copias de respaldo deben abarcar:

- información de trabajo de la organización
- aplicaciones en explotación, incluyendo los sistemas operativos
- datos de configuración, servicios, aplicaciones, equipos, etc.
- claves utilizadas para preservar la confidencialidad de la información

602. Para los puntos anteriores ver [op.exp] y [mp.info.3].

603. El responsable de la información debe determinar la frecuencia con la que deben realizarse las copias y el periodo de retención durante el que mantenerlas.

604. En caso de disponer de un Plan de Continuidad, las copias de seguridad deberán realizarse con una frecuencia que permita cumplir con el RPO y con un objetivo de tiempo de restauración que permita cumplir el RTO.

605. Se recomienda realizar periódicamente pruebas de restauración de copias de seguridad.

Anexo 2 Cuestionario básico de Ciberseguridad

Anexo 3 Programa de auditoría (fichas de revisión)

Anexo 4. Niveles de madurez de los procesos según la Guía de seguridad CCN-STIC 804

Para evaluar los resultados generales por cada uno de los CBCS se utilizará el modelo de nivel de madurez de los procesos¹⁶ usando una escala entre 0 y 5. Este modelo proporciona una base para comparar resultados entre distintos entes y entre distintos periodos para un ente determinado.

Nivel	Descripción
0 - Inexistente.	Esta medida no está siendo aplicada en este momento.
1 - Inicial / ad hoc	<p>El proceso existe, pero no se gestiona. El enfoque general de gestión no es organizado.</p> <p><i>La organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. En este caso, las organizaciones exceden con frecuencia presupuestos y tiempos de respuesta. El éxito del nivel 1 depende de tener personal de alta calidad.</i></p>
2 - Repetible, pero intuitivo.	<p>Los procesos siguen una pauta regular cuando determinados procedimientos se realizan por distintas personas, sin procedimientos escritos ni actividades formativas.</p> <p><i>La eficacia del proceso depende de la buena suerte y de la buena voluntad de las personas. Existe un mínimo de planificación que proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas. Todavía hay un riesgo significativo de exceder las estimaciones de coste y tiempo.</i></p>
3 - Proceso definido	<p>Los procesos están estandarizados, documentados y comunicados con acciones formativas.</p> <p><i>Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general. Hay normativa establecida y procedimientos para garantizar la reacción profesional ante los incidentes. Se ejerce un mantenimiento regular. Las oportunidades de sobrevivir son altas, aunque siempre queda el factor de lo desconocido (o no planificado). El éxito es algo más que buena suerte: se merece.</i></p> <p><i>Una diferencia importante entre el nivel 2 y el nivel 3 es la coordinación entre departamentos y proyectos, coordinación que no existe en el nivel 2, y que se gestiona en el nivel 3.</i></p>
4 - Gestionado y medible.	<p>La Dirección controla y mide el cumplimiento con los procedimientos y adopta medidas correctoras cuando se requiere.</p> <p><i>Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.</i></p> <p><i>En el nivel 4 de madurez, el funcionamiento de los procesos está bajo control con técnicas estadísticas y cuantitativas. La confianza está cuantificada, mientras que en el nivel 3, la confianza era solamente cualitativa.</i></p>
5 - Optimizado.	<p>Se siguen buenas prácticas en un ciclo de mejora continua.</p> <p><i>El nivel 5 de madurez se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se establecen objetivos cuantitativos de mejora. Y se revisan continuamente para reflejar los cambios en los objetivos de negocio, utilizándose como indicadores en la gestión de la mejora de los procesos.</i></p> <p><i>En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.</i></p>

¹⁶ Basado en la Guía de seguridad CCN-STIC 804.

Anexo 5. Tipos de ciberincidentes

El ENS define incidente de seguridad como: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

En la Guía CCN-STIC 817 se señala que, siguiendo la línea terminológica iniciada por la Estrategia de Ciberseguridad Nacional, a lo largo del citado documento se utilizará el término ciberincidente como sinónimo de incidente de seguridad en el ámbito de los Sistemas de Información y las Comunicaciones.

Clasificación de los ciberincidentes según la Guía de seguridad CCN-STIC 817

Clase de Ciberincidente	Descripción	Tipo de ciberincidente
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus Gusanos Troyanos Spyware Rootkit Ransomware (secuestro informático) Herramienta para Acceso Remoto Remote Access Tools (RAT)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en la productividad y/o la imagen de las instituciones atacadas	Denegación [Distribuida] del Servicio DoS / DDoS Fallo (Hardware/Software) Error humano Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de activos y vulnerabilidades (escaneo) Sniffing Ingeniería social Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	Compromiso de cuenta de usuario Defacement (desfiguración) Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) Falsificación de petición entre sitios cruzados Inyección SQL Spear Phishing Pharming Ataque de fuerza bruta Inyección de Ficheros Remota Explotación de vulnerabilidad software Explotación de vulnerabilidad hardware Acceso no autorizado a red
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Acceso no autorizado a información Modificación y borrado no autorizada de información. Publicación no autorizada de información. Exfiltración de información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Suplantación / Spoofing Uso de recursos no autorizado Uso ilegítimo de credenciales Violaciones de derechos de propiedad intelectual o industrial.

Clase de Ciberincidente	Descripción	Tipo de ciberincidente
Contenido abusivo	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Spam (Correo Basura) Acoso/extorsión/ mensajes ofensivos Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Abuso de privilegios por usuarios Acceso a servicios no autorizados Sistema desactualizado Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	