CUESTIONARIO

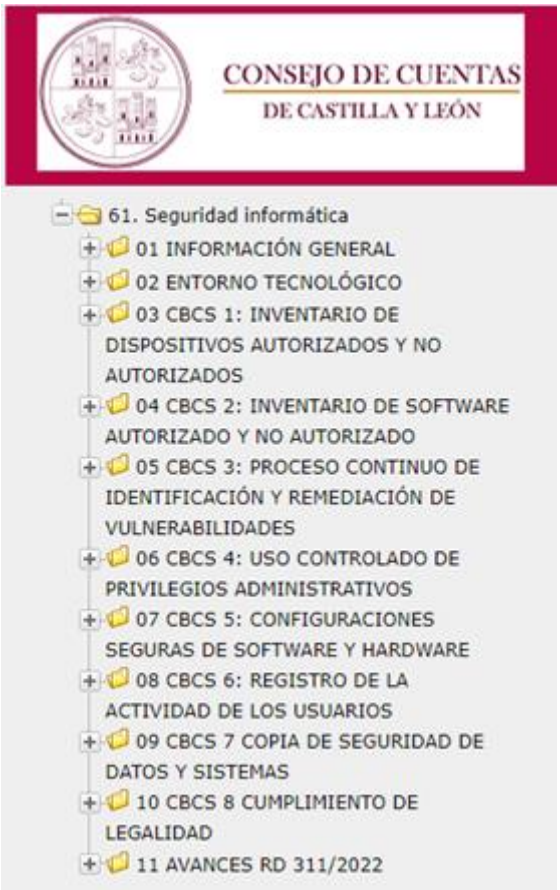
ANÁLISIS DE LA SEGURIDAD INFORMÁTICA EN LAS ENTIDADES LOCALES DE CASTILLA Y LEÓN

INTRODUCCIÓN

A continuación, se expone brevemente el contenido de cada uno de los apartados del formulario que ha de cumplimentar el Ayuntamiento.

Para resolver cualquier duda sobre la información a aportar, puede consultar con el personal del Consejo responsable de realizar la fiscalización a través de las vías de contacto proporcionadas.

El cuestionario se compone de los siguientes 11 bloques:



Los dos primeros corresponden a la información general de la entidad y de su entorno tecnológico. Los 8 siguientes corresponden a cada uno de los 8 controles básicos de ciberseguridad que se van a revisar.

De manera general, para cumplimentar el cuestionario no es necesario que se genere documentación adicional a la ya disponible en el Ayuntamiento. La idea es disponer de la documentación ya existente en la entidad en el momento de inicio del trabajo de campo, con el fin de optimizar el tiempo invertido por ambas partes.

01. INFORMACIÓN GENERAL

Los datos de este apartado han sido cumplimentados previamente, aunque pueden ser modificados al responder al formulario si se considera necesario.

02. ENTORNO TECNOLÓGICO

02.01. Relación de Sistemas de Información utilizados por la entidad como soporte de su actividad

En este apartado se pretende conocer qué Sistemas de Información dan soporte a las actividades que realiza el Ayuntamiento en el marco de sus competencias.

Al tratarse de una auditoría horizontal sobre ciberseguridad se incluirán todos aquellos sistemas de que disponga el Ayuntamiento, ya sean específicos para un determinado proceso (por ejemplo, la gestión de personal) o sistemas que, sin dar soporte específico a los procesos de gestión, son elementos críticos del entorno de TI de cualquier ente.

02.02. Diagrama físico/lógico de los SI identificados

Se detallarán los elementos software (aplicaciones y bases de datos), hardware, y las relaciones entre ellos, así como la existencia de elementos comunes (equipos de usuario, controlador de dominio, equipamiento de red).

En el caso de utilizar SI externalizados o en la nube, total o parcialmente, se indicará en este apartado, así como el modelo de sistema en la nube (SaaS, IaaS o PaaS)

02.03. Mapa de la red de la entidad

En este mapa se reflejará la ubicación de los SI dentro de la red, así como de los principales elementos de seguridad y los equipos de comunicaciones.

02.04. Descripción breve del entorno tecnológico.

Solo en caso de no disponer de la documentación solicitada en los apartados 02.01, 02.02 y 02.03, se describirá aquí brevemente el entorno tecnológico del Ayuntamiento y los principales elementos de los que consta.

03. CBCS 1: INVENTARIO DE DISPOSITIVOS AUTORIZADOS Y NO AUTORIZADOS

03.01. ¿Existe un inventario de hardware?

En caso de disponer de un inventario de los dispositivos físicos que forman los SI, aunque sea parcial o incompleto, debe marcar la casilla para responder afirmativamente.

En ese caso se responderá a las siguientes cuestiones, teniendo en cuenta que si el inventario contiene la información solicitada, aunque sea parcialmente, debe marcarse la casilla para contestar afirmativamente.

03.01.01. ¿Contiene identificación del activo: fabricante, modelo, número de serie?

03.01.02. ¿Contiene configuración del activo: perfil, política, software instalado?

03.01.03. ¿Contiene información sobre software instalado: fabricante, producto, versión y parches aplicados?

03.01.04. ¿Contiene información sobre la configuración de la red: MAC, IP asignada (o rango)?

03.01.05. ¿Contiene la ubicación del activo?

03.01.06. ¿Contiene información sobre la persona responsable del mismo?

03.01.07. Indicar la fecha de última actualización.

03.01.08 Si existe, indicar herramienta para actualización continua del inventario (nombre de la herramienta, fabricante y versión)

03.01.09. Si no se dispone de herramienta, indicar cómo se lleva a cabo la actualización del inventario. Si dispone de un procedimiento donde se describa cómo se realiza esta actualización, no es preciso que lo introduzca aquí, indique el nombre del procedimiento y apórtelo en el apartado 3.05

03.02 ¿Dispone de un procedimiento de autorización de los elementos hardware antes de su entrada en producción?

El procedimiento debe indicar quién puede solicitar la instalación de nuevo hardware, cómo debe hacerlo y quién lo autoriza. En caso de disponer de un procedimiento, aunque no esté aprobado formalmente, responda afirmativamente a la pregunta igualmente, y aporte la documentación de que disponga en el apartado 03.05

03.02.01. Descripción del procedimiento de autorización ¿Está aprobado? ¿Quién lo ha aprobado?

03.03. ¿Dispone de mecanismos para controlar (detectar y restringir) el acceso de dispositivos físicos no autorizados?

Si tiene implementado un mecanismo integral para realizar este control, como puede ser 802.1x, debe responder afirmativamente a la pregunta, aunque el mecanismo no aplique a todos los sistemas (un caso habitual es que se implemente únicamente para el acceso mediante WiFi).

03.04. ¿Cómo controla, a falta de mecanismo como 802.1x, y aunque sea de manera limitada, que no se conectan dispositivos no autorizados?

En este apartado entrarían medidas como la restricción de MACs por puerto, no cablear tomas de red vacías, deshabilitar los puertos de los equipos de acceso a la LAN por defecto, etc. En definitiva, medidas que aun no constituyendo un mecanismo integral, aporten cierto grado de control.

03.05. Aportar documentación:

Debe aportarse, si existe, copia de la documentación que se detalla a continuación. En el caso de los procedimientos, si no se dispone de un procedimiento formalizado, pero sí de guías o de manuales prácticos, utilizados por el personal TIC aunque no se trate de documentos formales, inclúyalos igualmente.

- Copia del procedimiento de mantenimiento y gestión del inventario de hardware.
- Copia del inventario de hardware.
- Copia del procedimiento de autorización de hardware.
- Copia del procedimiento donde se describan los controles para detectar o restringir el acceso de dispositivos físicos no autorizados.

04. CBCS 2: INVENTARIO DE SOFTWARE AUTORIZADO Y NO AUTORIZADO

04.01. ¿Existe una lista actualizada de software autorizado?

Si tiene un listado de software (o "*whitelist*") que ha pasado por el proceso de autorización y que se utiliza para decidir que software puede ser instalado, marque la casilla para responder afirmativamente

04.02. ¿Existe un inventario de software instalado en los dispositivos de la entidad?

En este caso se trata del inventario de software realmente instalado en los equipos de su entidad. En caso de tener este inventario, aunque sea parcial o incompleto, responda afirmativamente a la pregunta marcando la casilla.

En ese caso se responderá a las siguientes cuestiones, teniendo en cuenta que si el inventario contiene la información solicitada, aunque sea parcialmente, debe marcarse la casilla para contestar afirmativamente.

04.02.01. Indicar la fecha de la última actualización.

04.02.02. ¿Contiene identificación del software: fabricante, versión y parches aplicados?

04.02.03. ¿Contiene información del hardware en que está instalado dicho software?

04.02.04. ¿Contiene información sobre la persona responsable del mismo?

04.03 ¿Dispone de una herramienta automatizada para la gestión del inventario de software?

04.04. ¿Existe un procedimiento de autorización de software?

El procedimiento debe indicar quién puede solicitar la instalación de nuevo software, cómo debe hacerlo, y quién debe aprobarlo.

04.05. ¿Dispone de un plan de mantenimiento del software, de acuerdo con las especificaciones de los fabricantes?

El procedimiento debe indicar las tareas a realizar, el responsable de realizarlas, etc. Si dispone de este plan, aunque se trate de un procedimiento informal, o disperso en varios documentos, responda afirmativamente y aporte la documentación correspondiente en el apartado 04.09.

En caso de haber respondido afirmativamente:

04.05.01. El plan de mantenimiento anterior, ¿incluye el control de las fechas de fin de soporte del SW por parte de los fabricantes?

04.06. ¿Existe software fuera de soporte por parte del fabricante?

En caso de tener en producción software fuera de soporte, marque afirmativamente la casilla y aporte la siguiente información:

04.06.01. Indicar producto, fabricante y versión.

04.07. ¿Se dispone de guías de instalación y bastionado de los sistemas, previo a su entrada en operación, que garantice que no se instala software innecesario?

Dentro del procedimiento más amplio de bastionado/fortificación o instalación del software, responder si en algún punto se indica que solo se instale el software estrictamente necesario, sin instalar otras funcionalidades o herramientas que puedan incorporarse como accesorias al software principal.

En ese caso, responder a la siguiente cuestión:

04.07.01. ¿Especifica el procedimiento que debe dejarse constancia de quién lo realiza, fecha y versión del procedimiento utilizado?

04.08. ¿Dispone de alguna herramienta para controlar e impedir la instalación de software no autorizado?

Por ejemplo, AppLocker o directivas de restricción de software (SRP). En el caso de que las herramientas utilizadas no apliquen a todos los dispositivos, responda de manera afirmativa igualmente y aporte la siguiente información:

04.08.01. Indicar nombre de la herramienta, fabricante y versión.

04.08.02. ¿La herramienta detecta automáticamente el software instalado en cada sistema?

04.08.03. ¿Actualiza de forma automática el inventario de software?

Y en caso de no disponer de ninguna herramienta:

04.08.04 ¿Existe un procedimiento para la revisión del software instalado en los equipos de la entidad?

04.08.04.01 Descripción en caso de detectar software no autorizado en estas revisiones (eliminación, comunicación, etc.)

04.09. Aportar documentación

Debe aportarse, si existe, copia de la documentación que se detalla a continuación:

- Copia del procedimiento de mantenimiento y gestión del inventario de software.
- Copia del inventario de software.
- Copia del procedimiento de autorización de software.
- Copia del procedimiento/guías de configuración que indique los criterios para la instalación de software según el perfil de sistema y/o usuario.
- Copia del procedimiento de revisión del software instalado en los sistemas de la entidad.

05. CBCS 3: PROCESO CONTINUO DE IDENTIFICACIÓN Y REMEDIACIÓN DE VULNERABILIDADES

05.01. ¿Se dispone de una herramienta para la identificación de las vulnerabilidades de seguridad que puedan afectar a los productos y tecnologías de sistemas de información existentes en la entidad?

05.01.01 Indicar nombre de la herramienta, fabricante y versión.

05.02. ¿Se efectúa un seguimiento continuo de los anuncios de defectos realizados por los fabricantes?

En caso afirmativo, marque la casilla y responda a las siguientes cuestiones, o en caso de disponer de un procedimiento documentado, indíquelo:

05.02.01. ¿Cómo? (Ejemplo: contratación de un servicio específico a fabricantes, suscripción a listas públicas de publicación de defectos, etc.)

05.02.02. ¿Quién es el responsable de realizarlo?

05.03. Tras la puesta en servicio de un sistema, ¿se realizan análisis de vulnerabilidades periódicos?

Dentro del procedimiento más amplio de bastionado/fortificación o instalación de los nuevos sistemas, responder si en algún punto se indica que se realice un análisis de vulnerabilidades.

05.04. ¿Dispone de un procedimiento para analizar y priorizar la resolución de las vulnerabilidades y defectos de seguridad identificados, basado en la gestión de riesgos?

En caso de que sí que exista, aunque se trate de un procedimiento no aprobado formalmente, responda afirmativamente y conteste a:

05.04.01. ¿El procedimiento anterior define plazos máximos de resolución de las vulnerabilidades en función del riesgo asociado?

05.05. ¿Se dispone de un procedimiento para realizar el seguimiento y la corrección de las vulnerabilidades identificadas que, de acuerdo con la gestión de riesgos, se ha decidido resolver?

En caso de disponer de algún tipo de procedimiento, ya sea aprobado formalmente o no, o basado o no en la gestión de riesgos, responda afirmativamente a la pregunta.

05.06. ¿Se dispone de un procedimiento para la instalación de parches en sistemas/tecnologías (sistemas operativos, bases de datos, aplicaciones…)?

Si dispone de un procedimiento, aunque no esté aprobado formalmente o sea parcial, o aplique solo a determinados sistemas, marque la casilla para responder afirmativamente.

05.07. ¿Se dispone de una/s herramienta/s para la gestión e instalación de parches y actualizaciones de seguridad?

En caso afirmativo:

05.07.01. Indicar el nombre de la herramienta, fabricante y versión. En caso de utilizar herramientas diferentes en función de la tecnología, detallar de forma separada cada una de ellas.

05.08. ¿Ha tenido algún incidente de seguridad informática en su organización en el último año?

Tipología de incidentes de seguridad:

- Infecciones por código malicioso de sistemas, equipos de trabajo o dispositivos móviles.
- Intrusiones o intentos de intrusión provocadas por explotación de vulnerabilidades, ataques mediante exploits y vulneración de credenciales, lo que

conlleva el compromiso de cuentas con o sin privilegios de administrador y el compromiso de aplicaciones o servicios.

- Fallos de disponibilidad a través de ataques DoS (denegación de servicio) que pueden afectar a diferentes recursos de la organización (redes, servidores, equipos de trabajo, etc.) e imposibilitar el normal funcionamiento de los mismos.
- Compromiso de la información como resultado del acceso no autorizado a la misma o de su modificación (por ejemplo, mediante cifrado por ransomware).
- Fraude provocado principalmente a través de la suplantación de entidades legítimas, con el objetivo de engañar a los usuarios para obtener un beneficio económico, o por ataques de phishing, para la obtención de credenciales privadas de acceso a medios de pago.

05.08.01 Detallar brevemente los principales tipos de incidentes y las medidas adoptadas. Por otro lado, marque otras medidas adicionales, que se hayan aplicado, con carácter preventivo.

05.09. Aportar documentación:

Aporte la siguiente documentación:

- Copia del procedimiento de identificación de vulnerabilidades.
- Copia del procedimiento de análisis y priorización de vulnerabilidades.
- Copia del procedimiento de seguimiento de la resolución de vulnerabilidades.
- Copia del procedimiento de parcheo de sistemas/tecnologías (o de modificación de la configuración del sistema si está incluido allí).

06.CBCS 4: USO CONTROLADO DE PRIVILEGIOS ADMINISTRATIVOS

06.01. ¿Existe un procedimiento de gestión de privilegios que contemple la limitación de los privilegios de cada usuario al mínimo estrictamente necesario para acceder a la información requerida y para cumplir sus obligaciones?

Responda afirmativamente si al menos se distingue entre usuarios administradores y no administradores.

06.01.01. ¿El procedimiento garantiza que se restringen los permisos de administración a los casos en que sea necesario y que solo se utilicen las cuentas de administrador cuando sea necesario?

06.02. ¿Se dispone de un inventario de las cuentas de administración que permita su adecuada gestión y control?

06.03. ¿Dispone de un servidor de autenticación centralizado (Radius, TACACS+, etc.)?

06.04. ¿Los usuarios que no realizan funciones técnicas son administradores de sus equipos?

Aunque puedan existir diversas casuísticas según el sistema de información en concreto/ departamentos/ etc., responda afirmativamente si es lo más habitual.

06.05. Antes de la puesta en producción de un sistema, ¿se eliminan/renombran las cuentas de administración estándar y se les cambia la contraseña por defecto?

06.06. ¿Los usuarios que disponen de cuentas con privilegios administrativos utilizan una cuenta nominativa sin privilegios de administrador para las tareas habituales y accesos a Internet o correo electrónico?

06.07. Las cuentas de administración, ¿son nominativas? (es decir, cada usuario tiene la suya propia, no permitiendo el uso compartido de cuentas genéricas) siempre que sea posible.

Si las cuentas son nominativas en todos aquellos sistemas en los que sea posible, y solo se permiten compartidas en aquellos en que no se pueda definir más de un usuario de administración, responda afirmativamente.

Siempre que existan cuentas de administración compartidas, con independencia de si se realiza por procedimiento o porque el sistema no lo permite, responda a las siguientes preguntas:

06.07.01. En caso contrario, si no existen cuentas de administración nominativas o hay sistemas donde no es posible crear cuentas nominativas, indicar las cuentas de administración de uso compartido en caso de existir.

06.07.02. Si existen cuentas de administración compartidas, ¿Cómo se controla su uso? ¿Cómo se gestiona la contraseña (distribución, cambio periódico, cambio tras cese de una de las personas que la conocían, etc.)?

06.08. Para cada uno de los sistemas/tecnologías existentes en la entidad, indicar el mecanismo de autenticación de las cuentas de administración. Si se utilizan contraseñas, indicar las principales características de la política de autenticación (longitud mínima, vigencia máxima, vigencia mínima, requerimientos de complejidad como el uso de mayúsculas, minúsculas, números y caracteres especiales, histórico de contraseñas recordadas).

Adjunte, si dispone de los datos, una tabla con la siguiente información:

Sistema / Tecnología	Mecanismo de autenticación	Características principales
Ej: SGBD Oracle 11.2	Contraseña	….
Ej: Aplicación XXXXX	Certificado + contraseña	….
Dominio Windows (servidores y equipos de usuario)	Certificado + contraseña	….

06.09. ¿Se dispone de un procedimiento para regular la gestión de las cuentas de administración? (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.)

Si existe un procedimiento, aunque no esté aprobado, responda afirmativamente a la pregunta y responda a la siguiente cuestión:

06.09.01. El procedimiento anterior ¿contempla el que se retiren/deshabiliten/eliminen las cuentas de administración cuando la persona termina su relación con la entidad?

06.10. ¿Se dispone de un registro de actividad de las acciones realizadas con cuentas y sobre cuentas de administración para todos los sistemas (sistemas operativos, bases de datos, aplicaciones, etc.) de la entidad?

En el caso de que los registros de actividad no abarquen todos los elementos, marque la casilla de manera afirmativa igualmente, y sobre los registros que existan, conteste a las siguientes cuestiones:

06.10.01. ¿Contempla el registro tanto acciones exitosas como fallidas?

06.10.02. ¿Existe algún sistema en el que el registro anterior no esté habilitado?

06.10.03. ¿Existen alertas automáticas cuando se asignan/desasignan privilegios de administración?, y en ese caso 06.10.03.01. ¿Quién recibe y aprueba las alertas?

06.10.04. ¿Existen alertas automáticas cuando se supera un umbral de intentos de acceso fallidos mediante una cuenta con privilegios de administración?

06.10.05. ¿Qué mecanismos se utilizan para evitar que los propios administradores de los sistemas modifiquen los registros de auditoría de las acciones realizadas con cuentas de administración?

06.11. Aportar documentación:

- Copia del procedimiento de gestión de privilegios (en particular, privilegios de administración).
- Copia del procedimiento de inventariado de cuentas de administración.
- Copia del inventario de cuentas de administración.
- Copia del procedimiento de instalación/bastionado de sistemas, o aquél que contemple el control de renombrado/eliminación de cuentas estándar con privilegios de administración y las correspondientes contraseñas.
- Copia del procedimiento de gestión de cuentas de administración (ej. construcción del identificador de usuario, distribución de la contraseña/credencial, etc.).
- Copia del procedimiento para el registro de las acciones realizadas con cuentas de administración.

07.CBCS 5: CONFIGURACIONES SEGURAS DE SOFTWARE Y HARDWARE EN DISPOSITIVOS MÓVILES, PORTÁTILES, EQUIPOS DE SOBREMESA Y SERVIDORES

07.01. ¿Dispone de un procedimiento de fortificación o bastionado (configuración segura) de los sistemas previo a su entrada en operación?

Si dispone de un procedimiento, ya sea aprobado formalmente o no, o de guías de instalación que contemplen medidas para el bastionado del sistema responda afirmativamente y conteste a la siguiente cuestión:

07.01.01 ¿Qué tipo de dispositivos cubre? Por ejemplo, servidores, equipos de sobremesa, portátiles, móviles y tabletas, etc.

07.02. ¿Se utilizan imágenes o plantillas para aplicar la configuración de seguridad de todos los sistemas, de acuerdo con estándares aprobados por la organización?

07.03. Tras la puesta en producción de los sistemas, ¿se realizan comprobaciones periódicas para verificar que la configuración actual no ha sido modificada de forma no autorizada respecto de la configuración de seguridad original?

07.04. ¿Se dispone de alguna herramienta para realizar la tarea anterior?

En caso de disponer de una herramienta, marcar la casilla para responder afirmativamente y responder:

07.04.01. Indicar nombre de la herramienta, fabricante y versión.

07.05. ¿Se utilizan herramientas de configuración de los sistemas que impiden la modificación de la configuración de seguridad?

En caso de disponer de una herramienta, marcar la casilla para responder afirmativamente y responder:

07.05.01. Indicar nombre de la herramienta, fabricante y versión.

07.06. ¿Se utiliza un sistema de supervisión de configuración para "monitorizar" en tiempo real la configuración de seguridad de todos sistemas de producción de la entidad?

En caso de disponer de este tipo de herramienta, aunque no abarque todos los sistemas de la entidad, marque la casilla para responder afirmativamente y conteste a las siguientes cuestiones:

07.06.01. Indicar nombre de la herramienta, fabricante y versión.

07.06.02. ¿Permite definir alertas cuando se realizan cambios sobre dicha configuración?

En caso de no disponer de una herramienta:

07.06.03. ¿Se dispone de otros mecanismos que impidan o monitoricen la realización de cambios no autorizados en la configuración de seguridad de los sistemas?

07.07. Aportar documentación:

- Copia del procedimiento de pruebas de seguridad previas al pase a producción (en el que se detalle el alcance, es decir qué sistemas deben pasar estas pruebas, responsables de definir las pruebas, ejecutarlas, aprobarlas, herramientas para realizarlas, etc.).

- Ejemplo del plan de pruebas de seguridad y resultado de su ejecución para un cambio realizado durante el año.
- Copia del procedimiento que regule la realización de análisis de vulnerabilidades, pruebas de penetración y/o inspección de código fuente en su caso, previo al pase a producción.
- Ejemplo del resultado de un análisis de vulnerabilidades, una prueba de penetración y una inspección de código fuente en su caso, realizados durante el ejercicio.
- Copia del procedimiento de gestión de la configuración (o aquél que indique cómo garantizar que las configuraciones de seguridad no son modificadas de forma no autorizada tras la puesta en producción de un sistema.

08.CBCS 6: REGISTRO DE LA ACTIVIDAD DE LOS USUARIOS

08.01. ¿Se registran las actividades de los usuarios en el sistema?

En caso de que los logs de auditoría de la actividad de los usuarios estén activados, total o parcialmente, marcar la casilla para responder afirmativamente y contestar a las siguientes cuestiones:

08.01.01. Indicar en qué sistemas (sistema operativo, bases de datos, aplicaciones) se encuentra activado.

08.01.02. ¿El registro de auditoría indica quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario?

08.01.03. ¿Se han habilitado las opciones del registro de auditoría para que incluya información detallada, como direcciones de origen, direcciones de destino y otros datos útiles?

08.01.04. ¿Incluye tanto las actividades realizadas con éxito como los intentos fallidos?

08.02. ¿Dónde quedan almacenados los registros de actividad?

Si dispone de un procedimiento o documento descriptivo en el que se detalle esta información, no es necesario que lo describa aquí, indique el nombre del documento y apórtelo en el apartado 08.15.

08.03. ¿Se dispone de un inventario de los registros de actividad donde además se recoja el personal autorizado a su acceso, modificación o eliminación?

08.04. ¿Qué mecanismos existen para proteger los registros de actividad frente a accesos y modificaciones o eliminación?

Si dispone de un procedimiento o documento descriptivo en el que se detalle esta información, no es necesario que lo describa aquí, indique el nombre del documento y apórtelo en el apartado 08.15.

08.05. ¿Está determinado el periodo de retención de los registros de actividad?

08.06. ¿Se cuenta con un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención?

08.07. ¿Cómo se asegura que la fecha y hora de estos no pueden ser manipuladas?

Si dispone de un procedimiento o documento descriptivo en el que se detalle esta información, no es necesario que lo describa aquí, indique el nombre del documento y apórtelo en el apartado 08.15.

08.08. ¿Se realizan copias de seguridad de los registros de actividad?

08.09. ¿Las copias de seguridad, si existen, se ajustan a los mismos requisitos?

Si las copias de seguridad tienen los mismos requisitos de protección para su acceso, modificación eliminación, periodo de retención, etc. que los originales, marque la casilla afirmativamente.

08.10. ¿Qué mecanismos existen para proteger las copias de seguridad de los registros de actividad frente a accesos y modificaciones o eliminación?

Si dispone de un procedimiento o documento descriptivo en el que se detalle esta información, no es necesario que lo describa aquí, indique el nombre del documento y apórtelo en el apartado 08.15. (O si está incluido en el procedimiento de copias de seguridad general, indíquelo y aporte el procedimiento en el apartado 09.13)

08.11. ¿Se centralizan los logs generados en los diferentes sistemas?

En caso afirmativo,

08.11.01 ¿Como? Por ejemplo, realizando un volcado diario de los logs, reenvío de los logs al sistema central una vez escritos en el sistema original, escritura directa del log del sistema en el equipo centralizador de logs, etc.

08.12. ¿Se revisan los registros de actividad en busca de patrones anormales?

Si se revisan de manera proactiva, no solo como respuesta a un incidente, marque la casilla afirmativamente, y conteste a la siguiente cuestión:

08.12.01 Indicar alcance de las revisiones, responsables de su realización y periodicidad

08.13. ¿Se dispone de alguna herramienta/utilidad que permita alertar, en tiempo real de sucesos anormales a partir del análisis de los logs de auditoría?

En caso de disponer de este tipo de herramientas, marque la casilla para responder afirmativamente y responda a la siguiente cuestión:

08.13.01. Indicar nombre de la herramienta fabricante y versión.

08.14. ¿La entidad dispone de un SIEM (Security Information and Event Management) o una herramienta de analítica de logs para realizar correlación y análisis de logs?

En caso de disponer de este tipo de herramientas, marque la casilla para responder afirmativamente y responda a la siguiente cuestión:

08.14.01. Indicar nombre de la herramienta fabricante y versión.

08.15. Aportar documentación:

- Copia de la política o normativa que establezca las directrices sobre el registro de actividades de los usuarios (qué se debe registrar, con qué detalle, de qué sistemas, periodo de retención, mecanismos de protección de los registros, etc.).
- Copia del inventario de los registros de actividad, donde además se recoja el personal autorizado a su acceso, modificación o eliminación.
- Copia del procedimiento en el que se establezca:
    - El periodo de retención de los registros de actividad y periodo de retención de evidencias tras un incidente.
    - Proceso para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen).

- Copia de la política de copia de seguridad de los registros de actividad (si se sigue una política específica para este tipo de información, no incluida en la política general de copia de seguridad de datos y sistemas en cuyo caso se aportará en el apartado 09.13).
- Copia del procedimiento para la centralización de logs, en el que se indique las fuentes origen a centralizar, cómo se realizará la centralización, periodicidad, etc.
- Copia de una revisión de los registros de auditoría realizada durante el año y/o de los resultados obtenidos.

09. CBCS 7 Copia de seguridad de datos y sistemas

09.01. ¿Se realizan copias de respaldo que permitan recuperar datos perdidos con una antigüedad determinada?

En caso de que se realicen estas copias, aunque no abarquen todos los sistemas, responda afirmativamente a la pregunta marcando la casilla.

09.02. ¿Existe una política de copias de seguridad?

Si dispone de algún tipo de normativa o procedimiento, aunque no se trate de una política formalmente aprobada, responda afirmativamente marcando la casilla y aporte la documentación en el apartado 09.13.

En caso afirmativo,

09.02.01. ¿Incluye datos (información de trabajo) de la entidad?

09.02.02. ¿Algún sistema queda fuera del alcance de la política de copia?

09.02.03. ¿Abarca los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga?

09.02.04. Si se utiliza criptografía para el cifrado de la información, ¿la política de copia incluye el respaldo de las claves criptográficas?

09.03. Indicar tipo de copia y periodicidad (ej. Incremental diaria, completa semanal, etc.).

Si el procedimiento/política/normativa de que dispone ya describe esta información, indíquelo y no es preciso que complete más información.

09.04. ¿Se dispone de herramienta/s para la realización de copias de seguridad?

En caso afirmativo, marque la casilla y responda a la siguiente cuestión:

09.04.01. Indicar el nombre de la herramienta, fabricante y versión.

09.05. ¿En qué soporte se almacenan las copias de seguridad realizadas?

Si el procedimiento/política/normativa de que dispone ya describe esta información, indíquelo y no es preciso que complete más información

09.06. ¿Se externalizan las copias de seguridad?

Aunque se externalice solo una parte, marque la casilla para responder afirmativamente y responda a la siguiente cuestión:

09.06.01. ¿Dónde? (Ejemplo. a un edificio distinto, a una sala distinta dentro del mismo edificio, a las instalaciones de un proveedor, etc.)

09.07. ¿Se utilizan servicios en la nube para el almacenamiento de backups?

Aunque se utilicen servicios en la nube para solo una parte, marque la casilla para responder afirmativamente y responda a la siguiente cuestión:

09.07.01. Indicar qué servicio se utiliza y el proveedor que lo presta.

09.08. ¿Se realizan pruebas de recuperación a partir de las copias de respaldo realizadas?

Aunque solo se realicen pruebas parciales, marque la casilla para responder afirmativamente y responda a las siguientes cuestiones:

09.08.01. Indicar alcance de las pruebas de recuperación y periodicidad.

09.08.02. ¿Se documentan (o queda algún registro) de la realización de dichas pruebas de recuperación y las incidencias identificadas?

Para las dos preguntas anteriores, en el caso de tener un procedimiento o guía descriptiva que contenga esa información, indíquelo en el apartado y aporte la documentación en el apartado 09.13.

09.09. ¿Los backups disfrutan de la misma seguridad que los datos originales, tanto en su acceso, almacenamiento como transporte?

Aunque solo una parte de los backups dispongan de esas medidas, marque la casilla afirmativamente y responda a la siguiente cuestión:

09.09.01. Indicar brevemente los mecanismos utilizados para dicho propósito

En el caso de tener un procedimiento o guía descriptiva que contenga esta información, indíquelo y aporte la documentación en el apartado 09.13

09.10. En cuanto a solicitudes puntuales de recuperación de datos por parte de los usuarios de la organización, ¿se dispone de un procedimiento que establezca cómo debe realizarse (quién puede solicitar, cómo, quién debe autorizar, etc.)?

09.11. ¿Las copias de seguridad están accesibles de forma directa a nivel de red?

Marque la casilla para responder afirmativamente, aunque solo una parte esté accesible.

09.12. ¿Se dispone de una copia de seguridad en un soporte desconectado de la red?

Marque la casilla para responder afirmativamente, aunque solo una parte esté en soporte desconectado de la red, y conteste a la siguiente cuestión:

09.12.01. ¿Cómo y con qué frecuencia se realiza?

En el caso de tener un procedimiento o guía descriptiva que contenga esta información, indíquelo y aporte la documentación en el apartado 09.13

09.13. Aportar documentación:

- Copia del procedimiento de copia de seguridad de datos y sistemas.
- Copia del procedimiento de restauración a partir de las copias de seguridad realizadas.
- Copia de los informes, registros, etc. de las pruebas de recuperación realizadas en el último año.
- Copia del procedimiento para la solicitud de recuperaciones puntuales de información a partir de las copias de seguridad realizadas.

10. CBCS 8 CUMPLIMIENTO DE LEGALIDAD

10.01. ¿Dispone de una política de seguridad escrita?

Conteste afirmativamente, aunque la política no esté aprobada formalmente o no esté actualizada.

10.01.01. ¿Ha sido aprobada por el órgano superior competente (conforme al Art. 12 del RD 311/2022)?

10.01.02. ¿Se han asignado los siguientes roles/responsabilidades?:

- Responsable/s de la información
- Responsable/s del servicio
- Responsable de la seguridad (STIC)
- Responsable del sistema (TIC)

En caso afirmativo indicar nombre y puesto de la persona a quien se le ha asignado.

10.02. ¿Se ha realizado la auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta?

En caso afirmativo

10.02.01. Indicar la empresa encargada de la realización de la auditoría.

10.03. Para los sistemas de categoría Básica, ¿se ha realizado la autoevaluación de cumplimiento exigida en el ENS o bien, de forma opcional, la auditoría de cumplimiento?

10.03.01 Indicar la empresa encargada de la realización de la auditoría (salvo autoevaluación)

10.04 Los resultados de la auditoría y/o de la autoevaluación ¿han sido revisados por el responsable de seguridad y las conclusiones presentadas al responsable del sistema para que adopte las medidas correctoras adecuadas?

10.05 ¿Facilita los datos necesarios para el Informe del Estado de la Seguridad a través de la herramienta INES, cumpliendo así la Instrucción Técnica de Seguridad aprobada por resolución de 7 de octubre de 2016?

10.06. ¿Se ha designado Delegado de Protección de Datos (DPD)?

En caso afirmativo

10.06.01. Indicar nombre y puesto de la persona designada, indicando su posición en el organigrama general de la entidad, o si pertenece a otra administración (como la diputación) indíquelo.

10.06.02. ¿Se ha comunicado su designación a la Agencia Española de Protección de Datos?

10.07. ¿Se dispone de RAT (Registro de Actividades de Tratamiento), de acuerdo con lo establecido en el artículo 30 del RGPD?

10.08. ¿Se han realizado los análisis de riesgo de los tratamientos de datos personales realizados por la entidad y las evaluaciones de impacto para aquellos de riesgo alto?

10.09. ¿Cómo evalúa y verifica la entidad la eficacia de las medidas técnicas y organizativas (ej. mediante auditorías realizadas por empresas externas, autoevaluaciones de cumplimiento, etc.)?

Si dispone de un documento descriptivo en el que coste esta información, indíquelo y no es preciso que cumplimente más información en el apartado. Aporte el documento en el apartado 10.11.

10.10. ¿Se dispone del informe de auditoría anual de sistemas exigido por la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas?

10.11. Aportar documentación:

- Copia de la Política de seguridad requerida por el ENS.
- Copia de los registros (ej. resoluciones, actas, etc.) correspondientes a la designación de los responsables de la información, del servicio, de seguridad y del sistema según el ENS.
- Copia del informe de auditoría de cumplimiento del ENS para los sistemas de categoría Media y Alta.
- Copia de la autoevaluación de cumplimiento para los sistemas de categoría Básica según ENS.

- Copia del documento que recoge los datos de la última declaración en la herramienta INES.
- Copia de la designación del Delegado de Protección de Datos.
- Copia del registro de actividades de tratamiento de datos de carácter personal.
- Copia de los análisis de riesgos y evaluaciones de impacto de los tratamientos de datos personales.
- En los casos en los que aplique, copia del informe de auditoría o de la autoevaluación de la eficacia de las medidas de seguridad aplicadas a los datos personales.
- Copia del informe de auditoría de sistemas exigido en el Art. 12.3. de la Ley 25/2013, de 27 de diciembre de Impulso de la factura electrónica y creación del registro contable de facturas.

11. AVANCES RD 311/2022

Avances en la aplicación del Real Decreto 311/2022

11.01 Plan de Adaptación RD 311/2022

¿Existe un plan de Adaptación al RD 311/2022?

11.02 Designación de roles

¿Se ha efectuado una designación de roles acorde al RD 311/2022?

11.03 Servicios Externalizados (PDC)

¿Se ha designado por parte de los proveedores un POC (Punto o Persona de Contacto) con el fin de analizar y supervisar los requisitos de seguridad del servicio que presta o solución que esté proporcionando?

11.04 Comunicación CCN

¿Se han implementado medidas adicionales de comunicación de incidentes con impacto significativo en la seguridad al CCN?

11.05 Medidas Adicionales de Seguridad

Se han implementado medidas adicionales en lo que respecta a los siguientes controles:

- Aumento del control de los servicios en la nube desde nivel bajo.
- La interconexión de sistemas, mediante la revisión de la prevención ante otros sistemas de información interconectados.
- La protección de la cadena de suministro.

- Vigilancia a nivel de monitorización del sistema desde el nivel bajo. Medidas de detección de intrusos. Mantenimiento de la monitorización de manera constante.
- Otros dispositivos conectados a la red. Existe una hoja de ruta que permita un incremento de sus niveles de madurez en ciberseguridad y la mitigación de los riesgos de seguridad.

11.06 Aportar documentación

- Aportar documentación relacionada.