1. Introducción

Catalana de Seguretat i Comunicacions, S.L., en adelante **CSC**, es una empresa de base tecnológica con sede en Sant Feliu de Llobregat (Barcelona) y con más de veinticinco años de trayectoria en el diseño, instalación y mantenimiento de sistemas de protección contra incendios, seguridad y comunicaciones. A través de su delegación en la zona centro, que opera bajo la marca **In Genis**, extiende su actividad al resto del territorio nacional.

La naturaleza de lo que hacemos nos obliga a manejar, a diario, información muy sensible: configuraciones de sistemas de seguridad en instalaciones de terceros, imágenes procedentes de cámaras de videovigilancia, planos técnicos detallados de edificios e infraestructuras, datos personales de empleados y de contactos de clientes, y documentación contractual que en muchos casos tiene carácter reservado. A eso hay que sumar que nuestros técnicos acceden físicamente a instalaciones de clientes —muchas de ellas de titularidad pública o con un alto nivel de criticidad— con regularidad.

Por todo ello, la protección de la información no es para **CSC** una cuestión de cumplimiento formal, sino que es algo que forma parte directa de cómo trabajamos y de la confianza que depositamos y que nos depositan. Un incidente que comprometiera la confidencialidad de una instalación de seguridad o la disponibilidad de nuestros sistemas de gestión tendría consecuencias directas sobre nuestros clientes, sobre nuestra reputación y, en algunos casos, sobre la seguridad de personas.

Esta Política nace de esa realidad y recoge cómo **CSC** entiende y gestiona la seguridad de su información, qué compromisos asume y qué se espera de todas las personas que forman parte de la organización o que trabajan con nosotros.

2. Misión de la organización

La misión de **CSC** es ofrecer soluciones tecnológicas de alto nivel en el ámbito de la protección contra incendios, la seguridad patrimonial y las comunicaciones, acompañando a nuestros clientes desde la primera consulta hasta el mantenimiento a largo plazo de los sistemas instalados. Trabajamos con la convicción de que un servicio bien hecho es aquel en el que el cliente no tiene que preocuparse de nada una vez que se ha firmado el contrato.

En línea con esa misión, **CSC** define esta Política de Seguridad de la Información como documento de carácter obligatorio para empleados, colaboradores y proveedores. Su finalidad es garantizar que la información que manejamos —la nuestra y la de nuestros clientes— esté protegida en todo momento, y

que la prestación de nuestros servicios no se vea comprometida por incidentes que podrían haberse evitado.

Esta Política establece las bases para que el acceso, uso, custodia y salvaguarda de los activos de información y de los dispositivos de seguridad se realicen con garantías de seguridad en sus dimensiones:

- Disponibilidad: asegurar que las entidades o procesos autorizados puedan acceder a los activos y servicios cuando lo requieran, asegurando su continuidad y minimizando interrupciones.
- Integridad: garantizar que los activos de información y las configuraciones de los dispositivos no se alteren de manera no autorizada.
- Confidencialidad: impedir que la información se ponga a disposición o sea revelada a individuos o entidades no autorizadas, especialmente aquella vinculada a clientes, instalaciones y datos captados por los sistemas de seguridad, restringiendo el acceso únicamente a personal autorizados y aplicando mecanismos de protección adecuados.
- Autenticidad: garantizar la identidad de las entidades y la procedencia fiable de los datos.
- Trazabilidad: asegurar que las actuaciones puedan imputarse a las entidades responsables.

Objetivos específicos de la Seguridad de la Información en **CSC**:

- Velar por la seguridad de la información y por la protección de los datos captados y gestionados por los sistemas de seguridad.
- Gestionar formalmente la seguridad mediante procesos de análisis y tratamiento de riesgos.
- Elaborar, mantener y probar planes de contingencia y continuidad para los servicios críticos (instalación, monitorización y mantenimiento).
- Prevenir y mitigar incidentes de seguridad en la medida técnica y económicamente viable.
- Cumplir con todos los requisitos legales, normativos y contractuales aplicables, incluyendo la legislación sobre protección de datos personales según el RGPD y LOPDGDD, la normativa sobre seguridad privada y cualquier otra disposición obligatoria.
- Promover la concienciación y la formación continua de todo el personal en materia de seguridad y ciberseguridad.
- Fomentar la mejora continua del sistema de gestión de seguridad de la información (SGSI), adaptándolo a las nuevas amenazas, avances tecnológicos y necesidades del negocio.
- Proporcionar los niveles de seguridad acordados con clientes y terceros cuando se compartan o cedan activos de información.

Esta Política será aprobada por la Dirección de **CSC**.

Es de aplicación obligatoria para todo el personal, así como colaboradores, proveedores y subcontratistas, que accedan a información o sistemas bajo la responsabilidad de **CSC**.

La política se revisa al menos una vez al año o cuando se produzcan cambios significativos.

Se comunica a todos los empleados y colaboradores, y está disponible para clientes y otras partes interesadas.

3. Alcance

Esta Política se aplicará a los sistemas de información, dispositivos y servicios gestionados por **CSC** que entren dentro del ámbito de aplicación del Esquema Nacional de Seguridad (ENS) y/o resulten críticos para la prestación de los servicios objeto de su actividad. En particular, se entenderá por sistema de información a:

- Las redes de comunicaciones que utilice **CSC** del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.
- Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.
- Los datos digitales e información almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los puntos anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

Así, el alcance queda definido de la siguiente manera.

Los sistemas de información necesarios para la prestación de los servicios de:

Diseño, instalación, mantenimiento y comercialización de:

- Sistemas de protección contra incendios (sistemas de detección y extinción manual y automática de incendios, sistemas de ventilación y extracción de humos)
- Sistemas de protección patrimonial (sistemas de seguridad anti-intrusión, sistemas de circuito cerrado de televisión CCTV, sistemas de control de acceso)
- Sistemas de comunicaciones (sistemas de cableado estructurado, sistemas electrónicos de comunicación, sistemas de megafonía e interfonía, sistemas de control de aforo, sistemas audiovisuales, sistemas de TV-FM)
- Proyectos de infraestructuras comunes de telecomunicaciones
- Integración digital, monitorización y centralización de distintos sistemas de comunicaciones

4. El marco regulatorio en el que se desarrollarán las actividades

El marco regulatorio aplicable a **CSC** y desarrollado en el Anexo I de esta Política.

CSC cumple con la legislación vigente y es consciente del especial cuidado que requiere gestionar datos personales, acatando las leyes europeas y nacionales.

5. Cumplimiento de los requisitos de seguridad

Para dar cumplimiento al Real Decreto 311/2022 y a los requisitos del ENS, **CSC** implementará medidas de seguridad proporcionadas a la naturaleza de la información y a la categoría de los sistemas y servicios a proteger. La seguridad se entenderá como un proceso integral que incluye elementos técnicos, humanos, organizativos y legales.

Se prestará especial atención a la concienciación y formación del personal y se exigirá la adopción de medidas que eviten que la falta de organización, formación o procedimientos inadecuados constituyan fuentes de riesgo.

Los sistemas y dispositivos se diseñarán con el principio de mínimos privilegios y con configuración segura para eliminar funciones innecesarias. En particular:

a) Los sistemas y dispositivos proporcionarán la funcionalidad imprescindible para que **CSC** alcance sus objetivos contractuales y operativos.
b) Las funciones de operación, administración y registro serán las mínimas necesarias y estarán restringidas a personal y ubicaciones autorizadas; podrán definirse restricciones de horario y puntos de acceso.
c) En los entornos de explotación se desactivarán funciones no necesarias mediante control de configuración. El uso cotidiano de los sistemas deberá ser sencillo y seguro; un uso inseguro deberá requerir una acción consciente por parte del usuario.
d) Se aplicarán guías de configuración segura adaptadas a la categorización de los sistemas y tecnologías empleadas.

6. Modelo de gobernanza

Para garantizar el cumplimiento del ENS y organizar la seguridad de la información en **CSC** se designarán los roles de seguridad mínimos y se constituirá un Comité de Seguridad de la Información. Los roles incluyen, como mínimo:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de Seguridad
- Responsable del Sistema

Además, **CSC** cuenta con el Responsable de los Servicios que es la persona con conocimientos en Protección de Datos.

El Comité de Seguridad de la Información estará constituido por las funciones citadas, siendo presidido por Gerencia.

El rol de Responsable de Seguridad está externalizado en una persona de la empresa DM Sistemas.

6.1 Los roles o funciones de seguridad

Al Responsable de la Información se le atribuyen, entre otras, las siguientes funciones:

- Determinar los requisitos de la información tratada y la clasificación de activos.
- Establecer y aprobar los requisitos de seguridad aplicables a la información en el marco del ENS, la normativa de protección de datos y las guías técnicas aplicables.
- Aceptar los niveles de riesgo residual que afecten a la información de su responsabilidad (propietario del riesgo).

Esta función no es delegable en lo relativo a la aceptación final del riesgo sobre la información.

Al Responsable del Servicio le corresponderán, entre otras:

- Determinar los requisitos de los servicios prestados y su nivel de disponibilidad y continuidad.
- Establecer y aprobar los requisitos de seguridad aplicables al servicio según el marco ENS y las guías técnicas.
- Aceptar los riesgos residuales que afecten al servicio bajo su responsabilidad.

Esta función no es delegable en lo relativo a la aceptación final del riesgo sobre el servicio.

El Responsable de Seguridad desempeñará las siguientes funciones:

- Definir las decisiones y controles necesarios para satisfacer los requisitos de seguridad de la información y de los servicios.
- Mantener y verificar el nivel adecuado de seguridad de la información y de los servicios prestados por **CSC**.
- Promover la formación y concienciación en materia de seguridad.
- Coordinar la ejecución de análisis de riesgos, declarar aplicabilidad de controles e identificar medidas de seguridad.
- Asesorar en la determinación de la categoría de los sistemas y en la elaboración de planes de mejora y continuidad.
- Gestionar revisiones, auditorías y procesos de certificación.

- Actuar como punto de contacto con las autoridades competentes en materia de seguridad de redes y sistemas, cuando proceda.
- Elevan a la Dirección las propuestas de cambios relevantes en materia de seguridad.
- Proponer indicadores e informes de riesgos.

El Responsable del Sistema realizará, entre otras, las siguientes funciones:

- Suspender o restringir accesos a la información o la prestación de servicio si conoce deficiencias graves de seguridad.
- Desarrollar, operar y mantener los sistemas y dispositivos durante todo su ciclo de vida.
- Elaborar los procedimientos operativos necesarios para la gestión técnica.
- Definir topologías, configuraciones y criterios de uso y gestión del sistema.
- Integrar las medidas específicas de seguridad en la operación.
- Actuar como administrador técnico: gestión de configuración, actualizaciones, autorizaciones y monitorización técnica.
- Aprobar cambios en configuraciones que afecten al sistema y asegurar que los controles técnicos son cumplidos.

La persona responsable de Protección de Datos desempeñará las funciones descritas en su job description y de acuerdo con la normativa vigente en materia de protección de datos personales.

Funciones del Comité de Seguridad de la Información:

- Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.
- Asesorar en materia de Seguridad de la Información.
- Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
  - Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

Estas funciones podrán ser delegadas, en otros órganos de la organización.

El Responsable del Sistema actuará como secretario del Comité:

- Convoca las reuniones del Comité de Seguridad de la Información.
- Prepara los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elabora el acta de las reuniones.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité

6.2 Procedimientos de designación y renovación

La asignación de roles y funciones de seguridad será realizada por la Dirección del Comité de Seguridad. Los roles de seguridad se revisarán periódicamente (se recomienda revisión al menos cada cuatro años) y en caso de vacante deberá cubrirse en un plazo definido inferior a un mes, siguiendo el procedimiento interno de selección y nombramiento. La designación será comunicada formalmente a las personas afectadas.

6.3 Resolución de conflictos

Cualquier conflicto entre responsables o sobre la titularidad de riesgos será resuelto por el Comité de Seguridad de la Información, que actuará como órgano de arbitraje técnico-organizativo.

7. Desarrollo de la política de seguridad de la información

La presente Política se desarrollará mediante normativa interna, estándares y procedimientos que aborden los requisitos y controles exigidos por el ENS y por la normativa de protección de datos, estando esta documentación a disposición de las personas y entidades interesadas.

La revisión anual corresponderá al Comité de Seguridad, que propondrá mejoras para su aprobación. Toda la normativa de seguridad estará publicada internamente en el subdirectorio: **Z:\07 CALIDAD\ENS**

En las decisiones de seguridad se tendrán en cuenta los siguientes principios básicos:

7.1 Organización e implantación del proceso de seguridad

CSC implanta una estrategia de protección basada en múltiples capas (medidas organizativas, físicas y lógicas) de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

La organización de la seguridad queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en materia de gestión de la seguridad de los sistemas y la implantación de una estructura que las soporte.

Con carácter general, todos y cada uno de los/as usuarios/as de los sistemas de información de **CSC** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos.
Para una mejor respuesta a incidentes de seguridad, **CSC** mantendrá relaciones de cooperación en materia de seguridad con las autoridades competentes, proveedores de servicios informáticos o de comunicación, así como organismos públicos o privados dedicados a promover la seguridad de los sistemas de información.

En particular, la gestión de la seguridad de la información es responsabilidad específica de un conjunto de personas y comités con funciones concretas, definidas y documentadas en el punto 6 de esta política.

7.2 Análisis y gestión de los riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.
- Cuando cambien los servicios/productos prestados.
- Cuando cambie algún sistema de información.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La gestión de riesgos quedará documentada en los informes de Análisis y Gestión de riesgos.

7.3 Gestión de personal

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

Todos los miembros de **CSC** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todas las políticas y procedimientos en materia de seguridad deberán ser comunicadas regularmente a todos los trabajadores y usuarios terceros si procede.

Todos los miembros de **CSC** recibirán concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Todos los empleados requerirán de un acuerdo de confidencialidad para evitar la divulgación de información confidencial. En los casos de proyectos que así lo requieran, se firmarán acuerdos de confidencialidad específicos para ello.

Cuando se termine la relación laboral o contractual con empleados o personal externo, se les retirarán los permisos de acceso a las instalaciones y la información y se les pedirá que devuelvan cualquier tipo de información o equipos que se les haya entregado para la realización de los trabajos.

7.4 Profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información de **CSC**, dentro del ámbito del ENS, será formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la Dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Además, se establece una planificación de formación para la concienciación en temas de seguridad de la información de forma periódica para todos los puestos de trabajo.

7.5 Autorización y control de los accesos

El control de acceso digital se describe en el Manual ENS.

CSC ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

El control de acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de **CSC** y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se trabaja en remoto.

7.6 Protección de las instalaciones

Sólo las personas autorizadas tendrán acceso a las instalaciones.

CSC ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

CSC cuenta con las medidas de protección necesarias para:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de **CSC**.
- Proteger las infraestructuras de **CSC**, diseñando áreas protegidas con un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de los mismos en caso de traslado y/o permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento de los equipos que albergan la información de **CSC**.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de **CSC**: Instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de **CSC** a las áreas restringidas bajo su responsabilidad.

Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de **CSC** cuando lo consideren apropiado.

Todo el personal de **CSC** es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas y los espacios designados fuera de ella.

7.7 Adquisición de productos de seguridad y contratación de servicios de seguridad

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Para adquisición de productos o contratación de servicios de seguridad de la información, **CSC** dará preferencia, siempre que sea proporcionado a la categoría del sistema, a productos y servicios que cuenten con certificación, funcionalidades de seguridad verificadas o referencias técnicas que acrediten su idoneidad.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

La política de adquisición y contratación se complementa con procedimientos internos que regulan la contratación de terceros.

7.8 Mínimo privilegio

Los sistemas se diseñarán y configurarán otorgando mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. 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.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

7.9 Integridad y actualización del sistema

CSC se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por el Responsable de Seguridad con la aprobación del Comité de Seguridad de **CSC** que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con 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 estos.

La vigilancia continua por parte de **CSC** permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

7.10 Protección de la información almacenada y en tránsito

CSC prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección. Y establecerá medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

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

7.11 Prevención ante otros sistemas de información interconectados

CSC establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se seguirá lo dispuesto en el Manual ENS.

7.12 Registro de la actividad y detección de código dañino

CSC registrará las actividades de los usuarios, reteniendo la información mínima necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, **CSC** podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

7.13 Incidentes de seguridad

Los objetivos principales de la gestión de incidentes son los de:

- Establecer un sistema de detección y reacción frente a código dañino.
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.
- Este registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad.
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

CSC notificará al INCIBE-CERT quien lo pondrá inmediatamente en conocimiento del CCN-CERT los incidentes que les afecten a través del Responsable del Sistema.

CSC dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

7.14 Continuidad de la actividad

CSC mantendrá planes de continuidad que permitan la recuperación de actividades esenciales (monitorización, atención a incidencias críticas, restauración de servicios mínimos) en plazos adecuados, proporcionales a la criticidad del servicio.

Además, dispone de planes de contingencia que permiten la recuperación de las actividades al menos a un nivel mínimo en un plazo razonable de tiempo. La gestión de la continuidad del servicio incluirá, por tanto, diversos controles para la identificación y reducción de riesgos y un procedimiento que limite las consecuencias dañinas de los mismos y asegure la reanudación de las actividades esenciales en el menor tiempo posible.

La estrategia de continuidad del servicio está documentada, partiendo de los riesgos detectados y de los controles definidos y estos se revisarán y actualizarán regularmente para comprobar su idoneidad.

CSC fomentará la mejora continua aplicando criterios y metodologías de estándares internacionales como ISO 27001.

8. Terceras partes

Cuando **CSC** preste servicios a otros organismos o maneje información de terceros, se hará partícipe de esta Política y se establecerán canales de reporte y coordinación entre Comités de Seguridad y procedimientos de actuación ante incidentes.

Cuando **CSC** utilice servicios de terceros o ceda información, la tercera parte quedará sujeta a las obligaciones de esta Política y a la normativa de seguridad aplicable. Se exigirá, en los contratos, cláusulas de seguridad, confidencialidad y derechos de auditoría acordes con el riesgo.

Se garantizará que el personal de terceros dispone de nivel de concienciación y formación equivalente a la exigida por **CSC** para tareas que afecten a activos o datos sensibles. Si alguna exigencia no puede ser satisfecha por la tercera parte, el Responsable de Seguridad emitirá un informe de riesgos y las medidas compensatorias necesarias, que deberá ser aprobado por los Responsables de la Información y del Servicio afectados antes de continuar.

9. Los riesgos que se derivan del tratamiento de los datos personales

CSC cumple con la normativa de protección de datos aplicable (RGPD y LOPDGDD) y ha establecido un marco de gobernanza de la privacidad que incluye políticas, procedimientos y medidas técnicas y organizativas proporcionales a los riesgos derivados del tratamiento de datos personales captados por los sistemas de seguridad (imágenes, identificadores, datos de localización, etc.).

CSC asegurará, entre otras acciones:

- La minimización de datos recogidos y su retención conforme a la finalidad y la normativa.
- La transparencia y canalización de consentimientos o legitimaciones legales cuando sea aplicable.
- La aplicación de evaluaciones de impacto sobre la protección de datos (DPIA) para tratamientos de alto riesgo (por ejemplo, videovigilancia en espacios sensibles).
- La firma de contratos y cláusulas de encargado del tratamiento con los proveedores que accedan a datos personales.
- La adopción de medidas de seguridad técnicas (cifrado, control de accesos, segregación de redes) y organizativas (roles, formación, políticas) para proteger los datos personales.
- La cooperación con la autoridad de control en caso de consultas o incidencias relevantes.

CSC documentará su marco de privacidad en políticas específicas y mantendrá procedimientos de gestión y revisión permanente de riesgos asociados al tratamiento de datos personales.

Fecha: 4 de febrero de 2026