POLÍTICA ENS DE SEGURIDAD DE LA INFORMACIÓN

Fecha:	27/10/2022
Aprobado por:	Dirección
Nivel de confidencialidad:	Público

Tabla de contenido

1. APROBACIÓN Y ENTRADA EN VIGOR

El texto ha sido aprobado por la Dirección de EVERYCODE en la fecha que figura en la portada de este documento. Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

EVERYCODE depende de los sistemas TI (Tecnologías de Información) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando de forma rápida y eficiente frente a los incidentes.

Los sistemas TI deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad 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 inversión deben ser identificados e incluidos en la planificación y en la solicitud de ofertas.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad según se indica en el Artículo 7 del ENS.

2.1 PREVENCIÓN

Los departamentos de la organización deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos de EVERYCODE deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TI como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

El alcance del SGSI de EVERYCODE se define para los sistemas de información que dan soporte a las actividades de desarrollo, implantación y operación de plataformas software y plataformas de accesibilidad digital, de acuerdo con la declaración de aplicabilidad en su versión vigente.

La dirección del centro de trabajo dentro del alcance se localiza en la Calle Doctor Vicente Zaragozá, 1, oficina 2, Valencia.

4. MISIÓN

EVERYCODE desarrolla e implanta tecnologías de accesibilidad para el mercado y usuarios con el objetivo de conseguir que las páginas web sean accesibles y sencillas de usar para cualquier persona, independientemente de sus capacidades y preferencias.

5. MARCO NORMATIVO

EVERYCODE se encuentra sujeta a la normativa que viene descrita en detalle en el "Procedimiento de Cumplimiento Normativo" del SGSI.

El marco de referencia que da cobertura legal a este documento se establece en las siguientes secciones del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica:

- ENS. Artículo 12. Organización e implantación del proceso de seguridad

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el Anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

- ENS. Anexo II
    - Medidas de Seguridad Marco organizativo [org]
    - Política de seguridad [org.1]

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información coordina la seguridad de la información en EVERYCODE y estará formado por los siguientes miembros:

- Responsable de la Información.
- Responsable del Servicio.
- Responsable de Seguridad.
- Responsable del Sistema de Gestión.
- Administrador de la Seguridad del Sistema.

El Comité estará presidido por el Responsable de la Información. El Secretario del Comité de Seguridad de la Información será el Responsable de Seguridad y tendrá como funciones:

- Convocar las reuniones del Comité de Seguridad de la Información.
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- Ser responsable de la ejecución directa o delegada de las decisiones del Comité.

Las Funciones y Responsabilidades atribuidas al Comité serán:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información en EVERYCODE.
- Elaborar la estrategia de evolución de EVERYCODE en lo que respecta a la seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por EVERYCODE y recomendar posibles actuaciones respecto de ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas de seguridad que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de EVERYCODE.
- Priorizar 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 TIC desde su especificación inicial hasta su puesta en operación.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

Los diferentes roles junto con sus respectivas funciones y responsabilidades se describen a continuación:

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.
- Promover que el tratamiento de los datos personales efectuados por EVERYCODE, se efectúe de forma respetuosa con la normativa.
- Desde el punto de vista de la seguridad y teniendo en cuenta el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables deberá velar por que se garantice una seguridad adecuada de los datos personales y determinar las medidas de seguridad concretas que tendrá que proponer al responsable del tratamiento.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existentes son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Responsable del Sistema de Gestión

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspender el manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Administrador de la Seguridad del Sistema

- Implantar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Gestionar las autorizaciones concedidas a los usuarios del sistema; en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por la Dirección a propuesta del Comité de Gestión de la Seguridad de la Información. El nombramiento se revisará cuando el puesto quede vacante o cuando se considere oportuno por parte de la Dirección.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Gestión de la Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. Esta Política será aprobada por el mismo Comité y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

EVERYCODE trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de EVERYCODE se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

8. GESTIÓN DE RIESGOS

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo autónomo, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en el Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en la normativa vigente en materia de protección de datos de carácter personal.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

El análisis de riesgos también contemplará los requisitos establecidos en la normativa vigente en materia de protección de datos de carácter personal para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por la legislación.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.
Los criterios de evaluación de riesgos detallados se especificarán en el “Procedimiento de Aceptación del Riesgo” con la metodología de evaluación de riesgos.

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información. Estos niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

9. GESTIÓN DOCUMENTAL

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el "Procedimiento para información documentada" y la "Política de Clasificación de la Información".

10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa en las siguientes materias definidas en las políticas, procedimientos y otros documentos del SGSI de EVERYCODE.

De todas ellas, las más relevantes son las siguientes:

- "Planificación y control operacional", que establece los aspectos operativos de la seguridad de la información y el marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.
- "Procedimiento para Puestos y Formación", en el que se determinan los aspectos organizativos en cuanto a requisitos, funciones y formación para los perfiles de puestos de trabajo establecidos en materia de seguridad de la información.
- "Política de Transferencia de Información", que define las pautas a seguir para asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información, así como de las redes.
- "Política de Control de Accesos", que define cómo limitar el acceso a los recursos de tratamiento para prevenir el acceso no autorizado, garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.
- "Procedimiento de Seguridad en la Gestión de Proyectos", para garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida.

- "Procedimiento de Cumplimiento Normativo", para evitar incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.
- "Política de Seguridad de los Proveedores y Compras", para asegurar que los contratistas entiendan sus responsabilidades y sean adecuados para desempeñar sus funciones.
- "Política de Controles criptográficos", para garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.
- "Procedimiento para Gestión de Incidentes", que especifica las actividades a realizar cuando se produce un incidente de seguridad de la información.

La Normativa de Seguridad desarrollada en los procedimientos y políticas anteriores y otras que conforman la información documentada en materia de seguridad de la información estará a disposición de todos los miembros de la organización que necesiten conocerla. En particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

11. OBLIGACIONES DEL PERSONAL

Todos los miembros de EVERYCODE tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad contenida en las políticas y procedimientos definidos en el SGSI de la organización, siendo responsabilidad del Comité de Seguridad de la Información disponer de los medios necesarios para que la información llegue a los usuarios.

Se establecerá un programa de concienciación continua para atender a todos los miembros de EVERYCODE y, en particular, a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TI 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.

12. TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando EVERYCODE utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.