Política de Seguridad,

según el Esquema Nacional de Seguridad (ENS)

Marzo 2025

1. OBJETIVOS Y FUNDAMENTOS DE LA POLÍTICA: PRINCIPIOS DE SEGURIDAD

La información debe ser protegida durante todo su ciclo de vida, desde su creación o recepción, durante su procesamiento, comunicación, transporte, almacenamiento, difusión y hasta su eventual borrado o destrucción.

Por ello, se establecen los siguientes principios mínimos:

a) **Seguridad como proceso integral** (art.6)

La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. El tratamiento de la información estará presidido por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y de los responsables jerárquicos, para evitar que la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas constituyan fuentes de riesgo para la seguridad.

b) **Gestión de la seguridad basada en los riesgos** (art. 7).

El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de esos riesgos permitirá el mantenimiento de un entorno controlado, minimizando los mismos 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.

c) **Prevención, detección, respuesta y conservación** (art. 8).

La seguridad del sistema debe contemplar 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, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar Política de Seguridad de la Información (RD 2022) 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, que 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. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, 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.

d) **Existencia de líneas de defensa** (art. 9).

El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea 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.

• Minimizar el impacto final sobre el mismo. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

e) y f) **Vigilancia continua y reevaluación periódica**. (art. 10).

La vigilancia continua 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.

f) **Diferenciación de responsabilidades**. (art. 11).

En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamiento de datos personales, además se identificará el responsable del tratamiento y, en su caso, el encargado del tratamiento.

2. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día de firma de la dirección general.

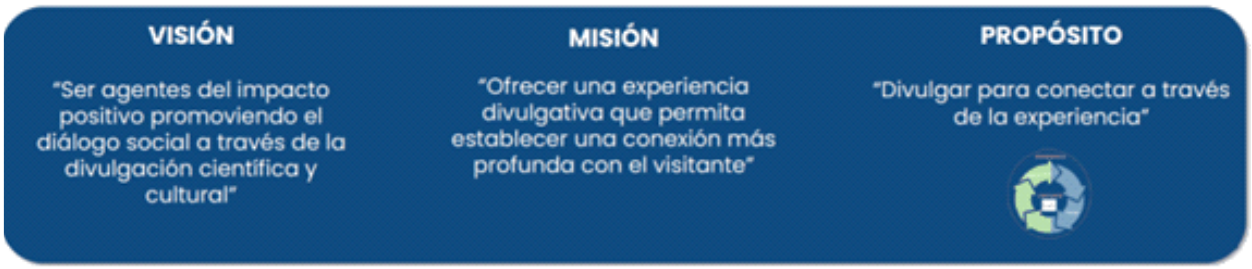
Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

3. ALCANCE

Esta política aplica a los sistemas de Información incluidos en el alcance del Sistema de Seguridad del ENS y a todo el personal de CACSA, sin excepciones.

4. DESCRIPCIÓN

4.1. MISIÓN, VISIÓN Y VALORES (art. 12.1.a)



4.2. MARCO NORMATIVO (art. 12.1.b)

CIUDAD DE LAS ARTES Y LAS CIENCIAS se encuentra sujeto a la siguiente normativa en la provisión de los servicios prestados a sus clientes y ciudadanos:

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (reglamento General de Protección de Datos), de aplicación al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

- Prevención de Riesgos Laborales Ley 31/1995 de 8 de noviembre y Real Decreto 39/1997 de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención.

- El convenio colectivo aplicable, correspondiente a “Oficinas y Despachos”.

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE).

- RD-ley 13/2012 de 30 de marzo, ley de cookies.

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

El marco de referencia que da cobertura legal a este documento se establece en las siguientes secciones del Real Decreto 311/2022 de 22 de mayo,por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS):

- ENS. Artículo 12. Política de Seguridad y requisitos mínimos 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 empresa.

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

4.3. ORGANIZACIÓN DE LA SEGURIDAD. ROLES Y FUNCIONES DE SEGURIDAD (art. 12.1.c y d)

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en los procedimientos del sistema de gestión de documentación de calidad:

Tanto la función del Responsable de la Información, como el Responsable de los Servicios en CACSA está representa por el órgano colegiado Comité de Seguridad.

MO-SI-01 MANUAL DE FUNCIONES Y RESPONSABILIDADES DEL ESQUEMA NACIONAL DE SEGURIDAD

MO-SGP-01 MANUAL DE ROLES Y RESPONSABILIDADES RGPD

4.3.4. Los ROLES DE SEGURIDAD: Funciones y Responsabilidades

Los diferentes roles junto con sus respectivas funciones y responsabilidades están reflejados en los procedimientos del sistema de gestión de documentación de calidad:

Tanto la función del Responsable de la Información, como el Responsable de los Servicios en CACSA está representa por el órgano colegiado Comité de Seguridad.

MO-SI-01 MANUAL DE FUNCIONES Y RESPONSABILIDADES DEL ESQUEMA NACIONAL DE SEGURIDAD

MO-SGP-01 MANUAL DE ROLES Y RESPONSABILIDADES RGPD

4.3.5. Procedimientos de Nombramiento

La Dirección General de CACSA nombrará al Responsable de la Seguridad, que debe reportar directamente a la Dirección general de CACSA, y al Responsable del Sistema, que, en materia de seguridad, reportará al Responsable de la Seguridad.

Se formalizará el nombramiento con la aprobación por parte de la Dirección general del MO-SI-01 MANUAL DE FUNCIONES Y RESPONSABILIDADES DEL ESQUEMA NACIONAL DE SEGURIDAD (ENS).

El nombramiento se revisará cada 4 años o cuando el puesto quede vacante.

4.3.6. Concienciación y Formación

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

Todos los trabajadores de CACSA asistirán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, 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.

4.4. DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA (art. 12.1.e)

CACSA tiene un sistema de gestión documental mediante el cual se editan, revisan y aprueban los documentos, y se publican a los usuarios correspondientes según la naturaleza y alcance del documento.

La documentación está estructurada de la siguiente manera, con la siguiente estructura de documentación: Política, Procedimientos, Instrucciones, Manuales Operativos, Normativas.

Las directrices para la estructuración de la documentación del sistema, su gestión y acceso se encuentran documentadas en el procedimiento PC-PLC-01 CONTROL DE LA DOCUMENTACIÓN.

4.5. GESTIÓN DE RIESGOS (art. 12.1.f)

Todos los sistemas sujetos a esta Política formarán parte de 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 prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la valoración del análisis de riesgos, el Comité de Gestión de la Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Gestión de la Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

4.6. DATOS DE CARÁCTER PERSONAL

CIUDAD DE LAS ARTES Y LAS CIENCIAS 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 CIUDAD DE LAS ARTES Y LAS CIENCIAS 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.

4.7. TERCERAS PARTES

Cuando preste servicios a otros organismos o maneje información de otras empresas, 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 CIUDAD DE LAS ARTES Y LAS CIENCIAS utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad relacionada con 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 está 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.

4.7. PREVENCIÓN, DETECCIÓN, RESPUESTA Y RECUPERACIÓN

CACSA debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

4.7.1 Prevención

CAC debe 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 se debe 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 del Área de Sistemas 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.

4.7.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple degradación 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 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.7.3. Respuesta

Los distintos departamentos del Área de Sistemas 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).

4.7.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, el Área de Sistemas debe desarrollar planes de continuidad de los sistemas TIC como parte del plan general de continuidad de negocio y actividades de recuperación.

4.8. PROCESO DE REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información la elaboración de esta Política de Seguridad de la Información, según art. 12 y control org.1), su revisión anual y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por Dirección general de CACSA, una vez aprobada por el Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

Firmado digitalmente por: ANA MARIA ORTELLS MIRALLES (R: A46483095)
CIUDAD DE LAS ARTES Y DE LAS CIENCIAS, S.A.U.

Fecha y hora: 31.03.2025 10:41:54

Directora General

Ana María Ortells Miralles

Ciudad de las Artes y las Ciencias

v_02 (marzo 2025)