CÁMARA
DE CUENTAS DE
ARAGÓN

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CÁMARA DE CUENTAS DE ARAGÓN

ÍNDICE

1. INTRODUCCIÓN

1.1. Misión y valores de la organización

Misión. Es misión de la Cámara de Cuentas de Aragón (CCA en adelante) fiscalizar la actividad económico-financiera del sector público aragonés para promover el uso adecuado y eficiente de los recursos y fortalecer la confianza de la sociedad en la gestión pública.

El propósito de la CCA es ser útil a la sociedad aragonesa y que se le reconozca como un referente independiente y profesional en el control del gasto y en la revisión de la eficacia de las políticas públicas, para lo que se compromete a que sus informes y actuaciones tengan un impacto real, sean relevantes y oportunos, exactos y claros, cortos en su extensión y precisos en sus conclusiones y a que se aprueben en un plazo razonable.

Valores. Los valores de la CCA son la independencia, profesionalidad, trabajo en equipo, transparencia y servicio público.

En la prestación de estos servicios, nuestros valores en materia de seguridad son: 1.- profesionalidad 2.- protección de las instalaciones 3.- seguridad por defecto 4.- protección de la información 5.- prevención 6.- mejora continua 7.- confidencialidad 8.- concienciación y formación 9.- integridad y calidad de la información 10.- disponibilidad de los sistemas de información y continuidad de los servicios ante contingencias 11.- gestión del riesgo 12.- proporcionalidad en coste.

1.2. Funciones y servicios prestados

La CCA es el órgano técnico al que corresponde la fiscalización externa de la gestión económico-financiera, contable y operativa del sector público de Aragón. Las funciones y competencias de la CCA son las establecidas en los artículos 3 y 4 de la Ley 11/2009, de 30 de diciembre, de la Cámara de Cuentas de Aragón.

Desde la CCA se prestan los siguientes servicios en la sede electrónica con sus diferentes trámites:

- Mi carpeta electrónica para consultar expedientes y notificaciones.
- Factura electrónica, que conecta con el Punto General de Entrada de Facturas de la Administración General del Estado (FACe).
- Perfil del contratante, que conecta con la plataforma de contratación del sector público.
- Portal de transparencia con información pública.
- Validación de documentos firmados electrónicamente en la plataforma de administración electrónica de la CCA.
- Trámites para ciudadanos, empresas y otras administraciones.
- Órganos colegiados.
- Trámites de empleados y cargos públicos.

Salvo los 2 últimos, que son exclusivos para los miembros del consejo de la CCA y sus trabajadores, el resto están disponibles tanto para los empleados de la CCA como para el público en general.

En la página web de la CCA se ofrece, para el público en general, información institucional, financiera y económica de la CCA, así como de los servicios prestados por ella, destacando los informes de fiscalización realizados y el estado de la rendición de cuentas de las entidades del sector público local Aragonés. Por su parte, en la intranet, solo accesible a los empleados de la CCA, se encuentra todo tipo de documentación y noticias relevantes para los empleados de la CCA.

Para la consecución de su misión se utilizan servicios internos que permiten la gestión y almacenamiento papeles de trabajo de auditoría y la gestión de la rendición cuentas sector público aragonés, además de servicios externos que permiten la interacción e intercambio de información de manera segura con las entidades fiscalizadas por la CCA.

Por último, hay que reseñar que se incluyen dentro del ámbito del ENS servicios internos y horizontales de la CCA que permiten su buen funcionamiento y el normal desarrollo de sus actividades, como la gestión contable, administrativa y de recursos humanos.

2. JUSTIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1. Necesidad de seguridad en los sistemas

Para el cumplimiento de su misión, la prestación de los servicios identificados y el cumplimiento de sus objetivos, la CCA, depende de las tecnologías de la información y la comunicación (TIC en adelante).

Las herramientas y sistemas TIC deben ser administrados con diligencia, adoptando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada o de 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 con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad, 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.

Es por ello por lo que el ENS en su artículo 12.2 establece que, “Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente”.

2.2. Requisitos de seguridad en la organización

Toda la organización debe aplicar las medidas mínimas de seguridad exigidas por el 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.

Todos los miembros de la institución 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.

El comité de seguridad de la información de la CCA velará por el cumplimiento de esta política y de las medidas de seguridad que derivan de ella dentro de la organización y por terceros que presten servicios a la CCA.

Todos los usuarios de los sistemas de información deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el artículo 8 del ENS.

3. MARCO NORMATIVO

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Real Decreto 4/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Interoperabilidad** en el ámbito de la administración electrónica, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.
- 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 y por el que se deroga la Directiva 95/46/CE (RGPD en adelante).
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales (LOPDGDD en adelante).
- Instrucciones técnicas de seguridad de la Secretaría de Estado de Administraciones Públicas:
  - Resolución de 7 de octubre de 2016, por la que se aprueba la instrucción técnica de seguridad de informe del estado de la seguridad.
  - Resolución de 13 de octubre de 2016, por la que se aprueba la instrucción técnica de seguridad de conformidad con el ENS.
  - Resolución de 13 de octubre de 2016, por la que se aprueba la instrucción técnica de seguridad de conformidad con el ENS.
- Ley 39/2015 de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 5/2021, de 29 de junio, de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón.

4. PRINCIPIOS DE PROTECCIÓN

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes, de acuerdo con el artículo 5 del ENS:

A. **Existencia de líneas de defensa:** El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad. La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de la organización para conformar un todo coherente y eficaz.

B. **Responsabilidad diferenciada**: Tal cual se indica en el artículo 11 del ENS, *en los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema*. Esto implica que *la* responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.
   En el caso de la CCA, las competencias de los responsables de la información y del servicio serán asumidas por el comité de seguridad de la información, determinando este comité los requisitos de la información tratada y los requisitos de los servicios prestados. Por otra parte, el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

C. **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

D. **Gestión de riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

E. **Prevención, detección, respuesta y conservación:** El establecimiento de medidas de protección, prevención, detección, respuesta, conservación y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

F. **Reevaluación periódica y vigilancia continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

G. **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la política de seguridad y del ENS. Se establecen los siguientes:

a. Organización e implantación del proceso de seguridad. Este principio recoge la estructura organizativa establecida en el ENS cuyo objetivo es facilitar una futura convergencia entre la seguridad física y la ciberseguridad.
b. Análisis y gestión de los riesgos. Se empleará la metodología reconocida internacionalmente. Las medidas adoptadas mitigarán o suprimirán los riesgos, siendo justificadas y proporcionadas.
c. Gestión de personal. Todo el personal de la CCA relacionado con la información y los sistemas, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.
d. Profesionalidad. 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. La CCA determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.
e. Autorización y control de los accesos. El acceso a los sistemas de información y a los activos de la CCA o de otras organizaciones, deberá ser controlado y limitado a los usuarios debidamente autorizados, restringiendo el acceso a las funciones permitidas.
f. Protección de las instalaciones. Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Las salas estarán cerradas y dispondrán de un control de llaves.
g. Adquisición de productos de seguridad y contratación de servicios de seguridad. La CCA adquirirá productos de seguridad de las tecnologías de la información y comunicaciones que se vayan a utilizar de forma proporcionada a la categoría de los sistemas y su nivel de seguridad.
h. Mínimo privilegio. Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.
i. Integridad y actualización del sistema. La CCA deberá conocer el estado de seguridad de los sistemas: especificaciones, vulnerabilidades y actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.
j. Protección de la información almacenada y en tránsito. La CCA dispondrá de procedimientos que aseguren la recuperación y conservación de los documentos electrónicos y la información en soporte no electrónico. Esta información deberá estar protegida en función del grado de seguridad definido.

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. Definición de roles

Tal como indica el artículo 13 del ENS, la seguridad afecta y es responsabilidad de todos los miembros de la institución.

La política de seguridad, según detalla el anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la CCA.

La responsabilidad del éxito de una organización recae, en última instancia, en su dirección. La dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad de la CCA, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad y jerarquía en el proceso de decisiones de la CCA la componen:

Rol	Funciones	Cargo
Dirección	Decide la misión y los objetivos de la organización.	Presidente de la Cámara de Cuentas de Aragón
Comité de seguridad de la información	Toma decisiones que concretan cómo alcanzar los objetivos de seguridad y protección de la privacidad marcados por la dirección	Secretaria general Director de tecnologías y sistemas de información Delegado de protección de datos (DPD)
Responsable de la información	Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la organización.	Comité de seguridad de la información
Responsable de servicio	Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la institución.	Comité de seguridad de la información
Responsable de seguridad de la información	Funciona como supervisor de la operación del sistema y vehículo de reporte al comité de seguridad de la información.	Director de tecnologías y sistemas de información
Responsable del sistema	Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día	Técnico auditoría de sistemas Analista TIC
Administrador de seguridad del sistema	Es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.	Técnico auditoría de sistemas Analista TIC
Responsable de gestión de personal	Implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de seguridad de la información, e informará a éste de su grado de implantación, eficacia e incidentes	Secretaria general
Delegado de protección de datos	Figura obligatoria para administraciones públicas, es el encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales. Su nombramiento se produce por otra vía ya que sus cometidos no se ciñen únicamente a aspectos de seguridad.	Externo

5.1.1. Dirección

Las funciones de la Dirección son aprobar la política de seguridad y realizar la designación de quienes integran el comité de seguridad de la información

5.1.2. Comité de seguridad de la información

El comité de seguridad de la información estará compuesto por los siguientes miembros:

- Secretaria general.
- Director de tecnologías y sistemas de información, que actuará como secretario del comité.
- DPD.

Se podrá convocar a las reuniones del comité a cualquier usuario de los sistemas de información cuando lo temas a tratar estén relacionados con su ámbito o cuya intervención sea precisa por ser afectados por el ENS y por el RGPD.

El comité asume las funciones de responsables del servicio y de la información, si bien, se tendrán en cuenta las valoraciones efectuadas por los usuarios en su participación en el comité.

Funciones del secretario. Será el responsable de seguridad de la información, correspondiéndole las siguientes 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.
- La responsabilidad de la ejecución directa o delegada de las decisiones del comité.

Funciones del comité. Corresponde al comité de seguridad de la información:

Función	Detalle
Informar	• Atender las inquietudes de la dirección y de los diferentes usuarios de los sistemas de información. • Informar regularmente del estado de la seguridad de la información a la dirección.
Promover	• Promover la mejora continua del sistema de gestión de la seguridad de la información. • Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
Coordinar	• 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. • Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes usuarios de los sistemas de información, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
Elaborar	• Elaborar (y revisar regularmente) la política de seguridad de la información para que sea aprobada por la dirección. • Elaborar la estrategia de evolución de la organización en lo que respecta a la seguridad de la información.

Aprobar	• Aprobar la normativa de seguridad de la información. • Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores (si los hubiera) y usuarios desde el punto de vista de seguridad de la información • Aprobar planes de mejora de la seguridad de la información de la organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse por diferentes usuarios.
Controlar	• Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. • Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC 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.

5.1.3. Responsable de la información

Las funciones de responsable de la información son asumidas por el comité de seguridad de la información.

Función	Detalle
Establecer requisitos de seguridad sobre la información	Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
Determinar niveles de seguridad en cada dimensión	Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el anexo I del ENS. Aunque la aprobación formal de los niveles corresponda al responsable de la Información, podrá recabar una propuesta del responsable de la seguridad y conviene que escuche la opinión del responsable del sistema.
Adoptar medidas sobre los datos personales	Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
Responder del uso	Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

5.1.4. Responsable del servicio

Las funciones del responsable del servicio son asumidas por el comité de seguridad de la información.

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al responsable del servicio, se puede recabar una propuesta al responsable de la seguridad y conviene que se escuche la opinión del responsable del sistema.
Riesgos	Aprobar el riesgo residual (el resultante una vez aplicado los controles de seguridad).

Consideraciones. El responsable del servicio deberá tener en cuenta las siguientes consideraciones:

- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el anexo I del ENS. Se recomienda que los criterios de valoración estén respaldados por la política de seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de esta, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

5.1.5. Responsable de seguridad de la información

El responsable de seguridad de la información será el titular de la dirección de tecnologías y sistemas de información. Esta es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información y sus funciones serán las siguientes:

Función	Detalle
Política, normativa y procedimientos	• Participará en la elaboración, en el marco del comité de seguridad de la información, de la política y normativa de seguridad de la información, para su aprobación por Dirección. • Elaborará y aprobará los procedimientos operativos de seguridad de la información.
Documento de seguridad	• Coordinará y controlará las medidas definidas en el documento de seguridad y en general se encargará del cumplimiento de las medidas de seguridad que detallan el RGDP y la LOPDGDD. • Coordinará la elaboración de la documentación de seguridad del sistema.
Formación y concienciación	• Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Elaborará los planes de formación y concienciación del personal en seguridad de la información, que deberán ser aprobados por el comité de seguridad de la información

Gestión de la seguridad	• Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la política de seguridad de la organización. • Recopilará los requisitos de seguridad de los responsables de información y servicio y determinará la categoría del sistema. • Realizará el análisis de riesgos. • Facilitará a los responsables de información y a los responsables de servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. • Elaborará una declaración de aplicabilidad a partir de las medidas de seguridad requeridas conforme al anexo II del ENS y del resultado del análisis de riesgos. • Elaborará, junto a los responsables de sistemas, planes de mejora de la seguridad o planes de tratamiento de riesgos, para su aprobación por el comité de seguridad de la información. • Validará los planes de continuidad de sistemas que elabore el responsable de sistemas, que deberán ser aprobados por el comité de seguridad de la información y probados periódicamente por el responsable de sistemas. • Aprobará las directrices propuestas por los responsables de sistemas para considerar la seguridad de la información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios. • Elaborar la memoria anual sobre el estado de la seguridad de la información, con el progreso de los proyectos de los planes de mejora, resumen de las actuaciones en materia de seguridad, de los incidentes relativos a seguridad de la información, del estado de la seguridad del sistema, y en particular del nivel de riesgo residual al que está expuesto el sistema.
Monitorizar	• Monitorizará los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones respecto de ellos. • Monitorizará el desempeño de los procesos de gestión de incidentes de seguridad y recomendará posibles actuaciones respecto de ellos. En particular, velará por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
Asesoramiento	• Asesorará a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo del ámbito de la empresa
Comité de seguridad de la información	• Facilitará periódicamente al comité de seguridad de la información un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de responsable de la seguridad, se podrá designar cuantos responsables de seguridad delegados considere necesarios.

La designación corresponde al responsable de la seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el responsable de la seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el responsable de la seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del responsable de la seguridad, que es a quien reportan.

5.1.6. Responsable del sistema

Las funciones de responsable del sistema recaerán en el personal que cubra las plazas de técnico de auditoría de sistemas y analista TIC, quienes tomarán las decisiones operativas relacionadas con la arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

Compatibilidades. Dadas las dimensiones de la institución, este rol coincide con el de administrador de seguridad del sistema.

Incompatibilidades. Este rol no coincide con el de responsable de información, ni con el de responsable de servicio, ni con el de responsable de seguridad de la información.

Las funciones del responsable del sistema son las siguientes:

Función	Detalle
Gestionar el sistema	• Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la Información afectada, del servicio afectado y con el responsable de la seguridad antes de ser ejecutada.
Establecer directrices y medidas	• Definir la topología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Definir la política de conexión o desconexión de equipos y usuarios nuevos en el sistema. • Decidir las medidas de seguridad que aplicarán los suministradores de componentes del sistema durante las etapas de desarrollo, instalación y prueba de este. • Determinar la configuración autorizada de hardware y software a utilizar en el sistema. • Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del sistema.
Elaborar	• Elaborar procedimientos operativos de seguridad. • Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
Aprobar	• Aprobar los cambios que afecten a la seguridad del modo de operación del sistema. • Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
Monitorizar	• Monitorizar el estado de la seguridad del sistema de información y reportarlo periódicamente o ante incidentes de seguridad relevantes al responsable de seguridad de la información.

Delegación de funciones

Se podrán externalizar servicios en terceros que estén debidamente certificados en el ENS

5.1.7. Administrador de seguridad del sistema

Las funciones de administrador de seguridad recaerán en el personal que cubra las plazas de técnico de auditoría de sistemas y analista TIC, quienes se encargarán de ejecutar las acciones

diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos. Se podrán externalizar servicios en terceros que estén debidamente certificados en el ENS.

Las funciones del administrador de seguridad del sistema son las siguientes:

Función	Detalle
Implementar, gestionar y mantener la seguridad	• La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información. • Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • 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.
Gestión, configuración y actualización	• La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información. • Aprobar los cambios en la configuración vigente del 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.
Gestión de las autorizaciones	• La gestión de 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	• La aplicación de los procedimientos operativos de seguridad. • Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	• 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.

5.1.8. Responsable de gestión del personal

La responsable de gestión de personal será la secretaria general, a la que le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el responsable de seguridad de la información, e informará a éste de su grado de implantación, eficacia e incidentes.

5.1.9. Delegado de protección de datos (DPD)

La CCA tiene contratado externamente el servicio de DPD.

Las funciones del DPD serán las indicadas en el RGPD y demás disposiciones reguladoras de la materia.

5.2. Jerarquía en el proceso de decisiones y mecanismos de coordinación

Las decisiones en materia de seguridad serán adoptadas por el comité de seguridad de la información, que dará instrucciones al responsable de seguridad de la información para la puesta en marcha de estas.

El responsable de seguridad de la información es el encargado de supervisar la ejecución de las acciones llevadas a cabo por el administrador y, en su caso, los operadores del sistema de información para implementar las medidas aprobadas.

El responsable de la seguridad de la información:

- Informa al comité de seguridad de la información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informa al comité de seguridad de la información de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al comité de seguridad de la información, como secretario:
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
- Da cuenta a la dirección, según lo acordado en el comité de seguridad de la información.
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

El responsable del sistema:

- Informa al comité de seguridad de la información de las incidencias funcionales relativas a cualquier información o servicio.
- Reporta lo siguiente al responsable de la seguridad de la información:
  - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
  - Resumen consolidado de los incidentes de seguridad.
  - Medidas de la eficacia de las medidas de protección que se deben implantar.

5.3. Datos de carácter personal

En el ejercicio de sus funciones, la CCA trata datos de carácter personal. La CCA dispone de un análisis de riesgos de seguridad con controles y medidas que reducen o eliminan los riesgos detectados y, para los tratamientos de alto riesgo, se elaborará una evaluación de impacto en

protección de datos, que, entre otros aspectos, identifique los riesgos en materia de seguridad y recoge medidas y controles para que el riesgo residual sea aceptable.

5.4. Categorización del sistema

La categorización de los sistemas de información es aprobada por el responsable de seguridad, en base a la valoración efectuada de la información y de los servicios en sus correspondientes dimensiones de seguridad (integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad) por los responsables de la información y los servicios. Para la valoración mencionada se seguirán las directrices del anexo I del ENS y, en concreto, la guía de seguridad de las TIC *CCN-STIC 803 - ENS Valoración de los sistemas*.

5.5. Gestión de riesgos

5.5.1. Justificación

Todos los sistemas sujetos a esta política deberán realizar un **análisis de riesgos**, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el ENS, según lo previsto en su artículo.

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 comité de seguridad de la información a través de un plan de adecuación al ENS.

Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del ENS y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación de este elaboradas por el CCN, así como todo lo referente al análisis de riesgos y de impacto en la protección de datos especificado en el RGPD.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el artículo 10 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 crítico de seguridad.
- Cuando se reporten vulnerabilidades críticas.

El análisis de riesgos también contemplará los requisitos establecidos por el artículo 32 del RGPD para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento.

5.5.2. Criterios de evaluación de riesgos

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 la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

5.5.3. Acciones para el tratamiento del riesgo

El comité de seguridad de la información trasladará al presidente de la CCA las necesidades económicas para atender a las necesidades de seguridad de los diferentes sistemas.

5.5.4. Proceso de aceptación del riesgo residual

Los riesgos residuales serán **determinados** por el responsable de seguridad de la información.

Los niveles de **riesgo residuales** esperados sobre cada **información** tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el anexo II del ENS) deberán ser aceptados previamente por el comité de seguridad de la información

Los niveles de **riesgo residuales** esperados sobre cada **servicio** tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el anexo II del ENS) deberán ser aceptados previamente por el comité de seguridad de la información

Los niveles de riesgo residuales serán presentados por el responsable de seguridad de la información al comité de seguridad de la información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

5.6. Gestión de incidentes de seguridad

5.6.1. Prevención de incidentes

Los usuarios 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. El ENS a través de su artículo 20 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la mínima funcionalidad. De igual forma, el artículo 18 del citado ENS define que los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos.

Para ello los usuarios de los sistemas de información 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 usuarios deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- 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.

5.6.2. Monitorización y detección de incidentes

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 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 produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

5.6.3. Respuesta ante incidentes

El comité de seguridad de la información debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados.
- 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).

5.6.4. Recuperación ante incidentes y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos, el comité de seguridad de la información debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

5.7. Obligaciones del personal

Los **miembros de la CCA** tienen la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad, siendo responsabilidad del comité de seguridad de la información disponer los medios necesarios para que la información llegue a los afectados.

Los miembros de la CCA atenderán a una **sesión de concienciación** en materia de seguridad TIC al menos anualmente. Se establecerá un **programa de concienciación** continua para atender a 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.

El cumplimiento de la presente política de seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

5.8. Terceras partes

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta política de seguridad de la información, se establecerán canales para reporte y coordinación de los respectivos comités de seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen 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.

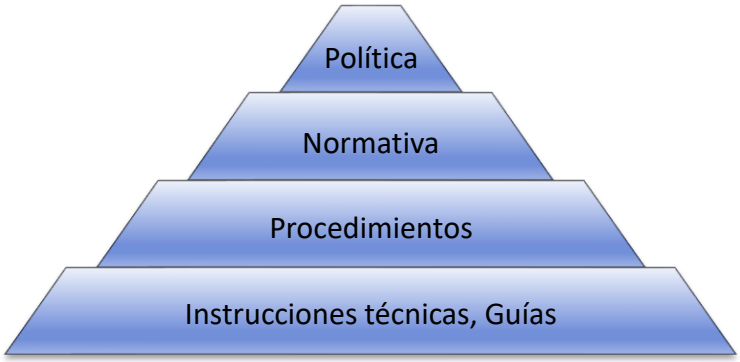
Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política.

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 de la información 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.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por la CCA y deberán formalizar su relación como encargados de tratamientos.

5.9. Estructura normativa y desarrollo de la política de seguridad

La estructura jerárquica de la documentación de seguridad es la siguiente:



Documento	Detalle
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. • Debe ser elaborada por el comité de seguridad de la información y ser aprobada por la dirección.
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el responsable de seguridad de la información y aprobada por el comité de seguridad de la información
Procedimiento	• Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. • Debe ser aprobado por el responsable de seguridad de la información
Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de esta. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el responsable del sistema o administrador del sistema y deben ser aprobados por el responsable de seguridad de la información

Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. • Deben ser aprobadas por el responsable de seguridad de la información.

5.10. Revisión y aprobación de la política de seguridad

La política de seguridad de la información será revisada por el comité de seguridad de la información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la política de seguridad de la información deberán ser aprobados por el presidente de la CCA, de acuerdo con el artículo 12 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

ANEXO. GLOSARIO DE TÉRMINOS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal

Cualquier información concerniente a personas físicas identificadas o identificables.

Gestión de incidentes

Plan de acción para atender a las incidencias que se den. Además de resolverlas, debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad de la información determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información

Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición.

Plaza Santa Cruz, 1 - 50003 Zaragoza - Teléfono: 976912912 - camara@camaracuentasaragon.es