# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Aprobado por: Comité de Seguridad

# ÍNDICE

# 1 Introducción

La Cámara de Comptos de Navarra, como ente fiscalizador del sector público navarro, establece entre sus valores la competencia profesional, entendida como la adquisición y actualización de los conocimientos requeridos para el desempeño de actividades profesionales y la eficacia, que permite la mejor asignación y empleo de los recursos.

Para el cumplimiento de estos objetivos, la Cámara de Comptos de Navarra depende de los sistemas TIC (Tecnología de Información y Comunicaciones). En consecuencia, 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.

La Cámara de Comptos siempre ha asumido el compromiso de garantizar que las TIC se utilizan de una forma segura. Mediante resolución del Presidente de la Cámara de Comptos de 23 de diciembre de 2008 se aprobó el documento de seguridad que contiene las medidas de índole técnica y organizativa de obligado cumplimiento para el personal con acceso a los sistemas de información que contienen datos de carácter personal y que se encuentran bajo la responsabilidad de la Cámara de Comptos de Navarra. Este documento fue actualizado en septiembre de 2014.

Aunque las políticas de seguridad aprobadas en 2014 estaban alineadas con los principios de la seguridad de la información vigentes, el transcurso del tiempo y la revisión de diversas normas jurídicas, entre ellas el Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, por el que se aprueba el Esquema Nacional de Seguridad (ENS), hacen necesario adaptar las políticas de seguridad a la evolución tecnológica y normativa.

Mediante resolución de la Presidencia de la Cámara, de 5 de octubre de 2015, se crea y regula la sede electrónica de la Cámara de Comptos de Navarra para facilitar a los ciudadanos y a las administraciones públicas comunicarse con la Cámara de Comptos a través de medios electrónicos. Los contenidos publicados en la sede electrónica de la Cámara responden a los criterios de seguridad e interoperabilidad establecidos en el ENS y en el Esquema Nacional de interoperabilidad.

El ENS, de acuerdo con lo previsto en la Ley 40/2015, tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada. El ámbito de aplicación del ENS es el Sector Público y su aplicación en la Cámara de Comptos, se hace con la finalidad de implantar medidas organizativas y técnicas de seguridad que protejan la información manejada y los servicios prestados, garantizando la seguridad y confidencialidad de los datos tratados por los Sistemas de Información de esta institución.

Esta política se actualiza con la entrada en vigor del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El objetivo de la seguridad de la información es garantizar la calidad y seguridad de la información (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) y la

prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

La presente política plasma la voluntad de la Cámara de Comptos de Navarra de desarrollar los sistemas de gestión que sean necesarios para la mejora de la seguridad de su propia información y servicios y el cumplimiento de la legislación anteriormente indicada.

Dado el carácter de mejora continua definido en los marcos anteriormente mencionados e inherentes a todo sistema de seguridad, se debe de 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 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 TIC.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

## 1.1 Prevención

La Cámara de Comptos de Navarra 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 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, la organización a través de los responsables designados debe:

- Autorizar los sistemas TIC antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.

## 1.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada 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 deben establecer mecanismos de detección, análisis y reporte que lleguen a las o los responsables regularmente y en el momento en que se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

## 1.3 Respuesta

La Cámara de Comptos de Navarra debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar el punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la Cámara de Comptos de Navarra.
- 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) reconocidos a nivel nacional: Iris-CERT, CCN-CERT, etc.

# 2 Alcance

## 2.1 Alcance de ámbito personal

La presente política es de obligado cumplimiento para todo el personal de la Cámara de Comptos de Navarra y todas aquellas personas con acceso a los sistemas de información (SI) de la institución.

## 2.2 Alcance de ámbito objetivo

La presente política se aplica sobre el total de los sistemas TIC que conforman el sistema de información y todos los recursos implicados en los sistemas de información de la Cámara de Comptos de Navarra.

# 3 Misión y objetivos

La Cámara de Comptos de Navarra es el órgano técnico dependiente del Parlamento o Cortes de Navarra, fiscalizador de la gestión económica y financiera del sector público de la Comunidad Foral, así como de aquellos fondos que tengan la consideración de públicos, de acuerdo con la Ley Foral 19/1984, de 20 de diciembre, de la Cámara de Comptos de Navarra.

Los objetivos generales de la institución son:

- Controlar los fondos públicos para aportar fiabilidad sobre las cuentas de los entes públicos y contribuir a la mejora en la prestación de los servicios públicos.
- Dotar de máxima calidad a los trabajos de fiscalización de la Cámara como garantía a los entes fiscalizados y a los ciudadanos sobre la gestión de los fondos públicos.
- Comunicar a la sociedad el trabajo que la Cámara realiza. Es esencial que los ciudadanos conozcan cómo se gestionan los fondos públicos y la importancia de la labor de control de los mismos por su contribución a la mejora de la gestión pública y a la prevención del fraude y la corrupción.

Las TIC constituyen una herramienta necesaria que debe ser utilizada de forma adecuada para minimizar los riesgos, que conlleva su utilización, garantizando razonablemente la seguridad de la información, lo cual incluye:

- Asegurar la disponibilidad de los SI y de los datos almacenados en estos SI (los usuarios autorizados tienen acceso a la información y sus activos asociados cuando lo requieren).
- Asegurar la integridad de la información almacenada en los SI (la información y sus métodos de proceso son exactos y completos).
- Preservar la confidencialidad de los datos sensibles (solo quienes están autorizados pueden acceder a la información).
- Asegurar el cumplimiento de las leyes, regulaciones y estándares aplicables.

La Cámara de Comptos de Navarra enumera los siguientes objetivos de seguridad de la información:

- Contribuir desde la gestión de la seguridad, al cumplimiento de la misión y objetivos estratégicos de la institución.
- Implementar el valor de la seguridad de la información en el conjunto de la organización.
- Contribuir todas y cada una de las personas de la Cámara de Comptos de Navarra a la protección de la información que manejan en su actividad diaria, como base para asegurar una gestión de la seguridad de la información eficaz y conforme con los requisitos de la legislación aplicable.
- Preservar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información, con el objetivo de garantizar que se cumplan los requisitos legales y/o regulatorios, normativos, u otros relativos a seguridad de la información.

- Establecer un plan que integre las actividades de prevención y minimización del riesgo de los incidentes de seguridad en base a los criterios de gestión del riesgo establecidos por la entidad.
- Proporcionar los medios necesarios para poder realizar las actuaciones pertinentes de cara a la gestión de los riesgos identificados.
- Definir como marco de gestión de la seguridad el compromiso de mejora continua utilizando el marco de un sistema de gestión de la seguridad de la información.
- Asumir la responsabilidad en materia de concienciación y formación en materia de seguridad de la información y protección de datos personales como medio para garantizar el cumplimiento de esta política.
- Extender nuestro compromiso con la seguridad de la información al conjunto de partes interesadas.

# 4 Marco normativo

Son de aplicación las leyes y normativas españolas y europeas en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Esta política se sitúa dentro del marco normativo definido por las leyes y Reales Decretos siguientes:

- Ley Orgánica 13/1982, de 10 de agosto, de reintegración y amejoramiento del Régimen Foral de Navarra.
- Ley Foral 19/1984, de 20 de diciembre, de la Cámara de Comptos de Navarra.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 del Régimen Jurídico del Sector Público.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
- Resolución de 13 de octubre de 2016 de la Secretaría de Estado de AAPP.
- Resolución de 27 de marzo de 2018 de la Secretaría de Estado de Función Pública.

# 5 Organización de la seguridad

La responsabilidad sobre la seguridad de la información de los SI recae sobre toda la organización y se reparte en base a las funciones y responsabilidades de cada puesto u órgano.

El máximo responsable de la seguridad de la información en la Cámara de Comptos es la Presidencia de la institución, que de acuerdo con las competencias que tiene atribuidas aprueba las políticas generales contenidas en este documento.

## 5.1Comité de Seguridad de la Información

Este comité es el máximo órgano al que compete la gestión de la seguridad de la información en la Cámara de Comptos. Debe reunirse semestralmente con carácter ordinario y podrá reunirse con carácter extraordinario en alguno de los siguientes supuestos, bajo decisión del Responsable de Seguridad:

- Cuando aparezcan incidencias de seguridad graves que puedan afectar a la seguridad de la información o protección de datos personales.
- Surjan nuevas necesidades de seguridad que requieran la participación de los componentes del Comité de Seguridad de la Información.

Para la válida constitución del Comité de Seguridad de la Información, a efectos de toma de acuerdos, se requiere de la mitad más uno de sus miembros, debiendo estar entre ellos el Responsable de Seguridad. El Comité de Seguridad adopta sus acuerdos por mayoría simple de los miembros presentes con derecho a voto.

El Comité de Seguridad de la Información depende de la Presidencia de la Cámara de Comptos de Navarra. Está formado por los siguientes miembros con derecho a voto:

- Responsable de Seguridad.
- Responsable del Sistema.
- Un representante de cada una de las siguientes áreas de la Cámara de Comptos de Navarra:
  - Auditoría.
  - Informática.
  - Asesoría jurídica.
  - Administración.
  - Comunicación.
- Administrador de la Seguridad.

El responsable de cada área establece quién es la persona que la representa en el Comité. En su caso, podrá establecerse una única persona que asuma varios roles en el Comité.

El Responsable de Seguridad, bajo su criterio, podrá convocar a otro personal de la Cámara de Comptos de Navarra no incluido en la lista anterior y que pueda ser relevante en el desarrollo del Comité.

En el ámbito del Comité de Seguridad de la Información, el Responsable de Seguridad ejerce como secretario. Tiene 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.
- Es responsable de la ejecución directa o delegada de las decisiones del Comité.

El Comité de Seguridad de la Información reporta a la Presidencia de la Cámara. Sus principales funciones incluyen:

- Atender las inquietudes de la Presidencia de la Cámara y de las diferentes áreas de la entidad.
- Informar regularmente del estado de la seguridad de la información a la Presidencia de la Cámara.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información.
- Elaborar la estrategia de evolución de la Cámara de Comptos de Navarra en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para que sea aprobada por la Presidencia.
- Aprobar la normativa relativa a las normas de seguridad TIC de desarrollo de la política de seguridad de la información y, aprobar los procedimientos operativos de Sistemas de Información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Cámara de Comptos de Navarra y recomendar posibles actuaciones respecto de ellos.
- 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.
- Promover la realización de las auditorías periódicas 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 la Cámara de Comptos de Navarra. En particular, velar por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- 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. En particular, velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad en el ámbito de la seguridad de la información que puedan aparecer entre los diferentes responsables o áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información asumirá las funciones de Responsable de la Información y Responsable de Servicio tal y como vienen definidas en el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el ENS, entre otras las siguientes:

- Establecer las necesidades de seguridad de la información que se maneja.
- Efectuar valoraciones del impacto que tendría un incidente que afectara a la seguridad de la información para cada tipo de información.
- Aprobar o modificar el nivel de seguridad requerido para cada tipo de información.
- Determinar los requisitos de seguridad del servicio prestado.
- Efectuar valoraciones del impacto que tendría un incidente que afectara a la seguridad de la información para cada servicio.
- Aprobar o modificar el nivel de seguridad requerido para los servicios prestados.
- Revisión y seguimiento de las incidencias en la seguridad de la información requiriendo para ello los informes que sean necesarios al Responsable del Sistema y/o el Administrador de Seguridad.
- Seguimiento de las medidas adoptadas para implantar controles sobre seguridad de la información.

## 5.2Roles. Funciones y responsabilidades

Los roles, funciones y responsabilidades que se desglosan en esta política son de ámbito general. Se contempla la seguridad como función diferenciada, por medio del nombramiento de los siguientes responsables:

- Responsable de Seguridad.
- Responsable de Sistema.
- Administrador de Seguridad.
- Delegado de Protección de Datos.

### 5.2.1 Responsable de Seguridad de la información

El Responsable de Seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y del servicio.

El Responsable de Seguridad de la información será el secretario general de la Cámara de Comptos.

Las funciones del responsable de seguridad serán las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo con la política de seguridad de la información.
- Supervisar el cumplimiento de la Política de Seguridad de la Información, sus normas, procedimientos y configuración de seguridad de los sistemas.
- Asesorar, en colaboración con el Responsable del Sistema, a los responsables de la información y a los responsables del servicio en la realización de los preceptivos análisis de riesgos, y revisar el proceso de gestión del riesgo, elevando un informe anual al Comité de Seguridad de la Información.
- Firmar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.
- Informar al Comité de Seguridad de la Información de las actuaciones realizadas en materia de seguridad de la información y de los incidentes de seguridad.
- Promover la formación y concienciación en materia de seguridad de la información.
- Aprobar la catalogación de los sistemas de información.

### 5.2.2 Responsable del Sistema

Se asignan las funciones de Responsable del Sistema al Técnico Superior en Sistemas Informáticos.

Las funciones del Responsable del Sistema comprenden las siguientes:

- Tendrá la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Implantar las medidas necesarias para garantizar la seguridad del sistema durante todo su ciclo de vida, siguiendo las observaciones del responsable de seguridad.
- Informar al Responsable de Seguridad.

- Asimismo, dará cuenta al Comité de Seguridad de la Información de los riesgos e incumplimientos de las políticas que detecte para adoptar las medidas correctoras que correspondan.
- Gestionar las autorizaciones concedidas a los usuarios en los sistemas bajo su responsabilidad, privilegios concedidos, incluyendo la monitorización de la actividad, con la supervisión del responsable de seguridad.
- Monitorizar el estado de seguridad del sistema, bajo la supervisión del Responsable de Seguridad.
- Informar a los Responsables de la Información, del Servicio y de Seguridad de las anomalías detectadas.
- Colaborar en la investigación y resolución de incidentes de seguridad.

El Responsable del Sistema, aunque mantiene la responsabilidad, podrá nombrar delegados que se harán cargo de las funciones delegadas relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

### 5.2.3 Administrador de la Seguridad del sistema

Bajo la dependencia del Responsable del Sistema, se asigna la responsabilidad de Administrador de Seguridad del sistema al Técnico de Grado Medio en Sistemas Informáticos.

Las funciones del Administrador de la Seguridad del sistema comprenden las siguientes:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- 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.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los procedimientos operativos de seguridad.
- Aprobar los cambios en la configuración vigente del sistema de información.
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- 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.
- 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.
- Monitorizar el estado de seguridad del sistema, analizando la información proporcionada por la herramienta de gestión de eventos de seguridad y mecanismos de auditoría técnica instalados en el sistema.
- Supervisar que todo el equipamiento se ajusta a lo autorizado.
- Supervisar las actividades de los administradores del sistema: actuaciones y aplicación de los procedimientos de seguridad establecidos.
- Supervisar que las actividades de los usuarios del sistema son conformes con las autorizaciones concedidas.

### 5.2.4 Delegado de Protección de Datos

El Delegado de Protección de Datos se nombra por resolución de la Presidencia. Las funciones del Delegado de Protección de Datos comprenden las recogidas en el artículo 39 del RGPD, que son entre otras las siguientes:

- Informar y asesorar a la organización y a sus empleados de las obligaciones en materia de legislación de protección de datos.
- Supervisar el cumplimiento de lo establecido en la legislación de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35 del RGPD.
- Cooperar con la autoridad de control y actuar como punto de contacto con la misma.

### 5.2.5 POC

El POC es el punto o persona de contacto que centraliza todas las comunicaciones relacionadas con la seguridad relativa a los servicios externos que presta la organización. Este rol lo asumirá el Responsable de Seguridad. Sus funciones son las siguientes:

- Gestionar las comunicaciones (internas y externas) relevantes en materia de seguridad de la información.
- Canalizar y supervisar, el cumplimiento de los requisitos de seguridad del servicio.

Las incidencias se recibirán a través del correo electrónico respsegccn@comptos.org.

## 5.3 Política de Seguridad de la Información

Será misión del Comité de Seguridad de la Información la revisión anual de esta política y la propuesta de revisión o mantenimiento de la misma. La política será difundida para que la conozcan todas las partes afectadas.

## 5.4 Resolución de conflictos

En caso de que se produzcan conflictos en materia de seguridad de la información, el Comité de Seguridad de la Información será el encargado de su resolución.

En caso de que no tenga suficiente autoridad para decidir, elevará el conflicto a la Presidencia de la Cámara de Comptos de Navarra para su resolución.

# 6 Datos de carácter personal

La Cámara de Comptos de Navarra realiza tratamientos en los que hace uso de datos de carácter personal. El registro de las actividades de tratamiento se recoge en el Documento de Normas de Seguridad de Datos Personales y su inventario está publicado en la página web de la entidad, en la página de protección de datos que figura dentro del área de transparencia.

Todos los sistemas de información de la Cámara de Comptos de Navarra se ajustarán a los requisitos de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Normas de Seguridad de Datos Personales.

En caso de conflicto con la normativa de seguridad prevista en estas políticas, prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos personales.

La entidad ha realizado un proceso de adecuación a los requisitos del RGPD y la LOPDyGDD. Asimismo, ha nombrado un delegado de protección de datos, que puede contactarse a través de la siguiente dirección: dpd.camaracomptos@navarra.es .

# 7 Gestión de riesgos

Para todos los sistemas sujetos a esta política debe realizarse 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 armonización de los análisis de riesgos, el Comité de Seguridad de la Información debe establecer una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad de la Información debe dinamizar la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

# 8 Desarrollo de la Política de Seguridad

Esta política se debe desarrollar por medio de normas y procedimientos de seguridad que afronten aspectos específicos. La normativa de seguridad estará a disposición del personal con acceso al sistema de información de la organización que necesite conocerla, en particular para quienes utilicen, operen o administren los sistemas de información y comunicaciones mediante un recurso de la red de datos de la Cámara de Comptos de Navarra.

Se establece un marco normativo en materia de seguridad de la información estructurado en diversos niveles a partir de la presente política:

- Normas de seguridad que definen qué actuaciones deben realizarse para proteger la información y servicios afectados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los activos de información de la organización.
- Procedimientos de seguridad que describen cómo llevar a cabo la protección especificada en las normas de seguridad.
- Instrucciones técnicas, que regulan medidas de carácter técnico a implantar en el ámbito de las TIC.

La siguiente tabla recoge las responsabilidades relacionadas con la documentación:

| **Documento** | **Responsable de desarrollo** | **Personal de soporte** | **Responsable de aprobación** |
|---|---|---|---|
| Normas de seguridad | Responsable de Seguridad | Responsable del Sistema<br>Administrador de la Seguridad<br>Delegado de Protección de Datos | Comité de Seguridad de la Información |
| Procedimientos de seguridad | Responsable del Sistema | Administrador de la Seguridad | Comité de Seguridad de la Información |
| Instrucciones técnicas | Administrador de la Seguridad | - | Responsable del Sistema |

La clasificación de esta documentación está sujeta a los criterios establecidos de forma general para los activos de información de la Cámara de Comptos de Navarra. Con carácter general, esta documentación debe estar accesible al conjunto de la organización.

Esta documentación debe revisarse anualmente (con la cumplementación del informe INES) y actualizarse cuando se produzcan cambios relevantes que puedan afectarle.

# 9 Principios generales de seguridad

Las actuaciones la Cámara de Comptos de Navarra en el ámbito de la seguridad de la información estarán regidas por los siguientes principios básicos, según lo establecido en el art. 5 del ENS:

- Seguridad integral. La seguridad se debe gestionar a través de un sistema de gestión de seguridad de la información que, de manera integral, considere todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema. Para su implantación, se debe llevar a cabo la concienciación necesaria del personal de la entidad de modo que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.
- Gestión de la seguridad basada en riesgos. La seguridad debe basarse en el desarrollo y actualización de un análisis de riesgos que determine las principales amenazas para la seguridad de la información de la Cámara de Comptos de Navarra. Para ello se debe utilizar una metodología reconocida y los criterios establecidos por la propia entidad como actividad previa al análisis y gestión del riesgo.
- Prevención, reacción y recuperación. La seguridad debe contemplar los aspectos necesarios de prevención, detección, respuesta y recuperación, según lo establecido en el capítulo “1 Introducción”. Para ello, la Cámara de Comptos de Navarra debe establecer medidas de seguridad destinadas a evitar o mitigar el riesgo de que se materialicen las amenazas, así como a afrontar debidamente los incidentes de seguridad que puedan producirse.
- Líneas de defensa. La seguridad debe estar basada en múltiples capas de seguridad, integrando medidas de carácter organizativo, físico y lógico.
- Reevaluación periódica. La seguridad se debe basar en el mantenimiento y revisión del sistema de gestión de la seguridad de la información y de las medidas de seguridad que de éste se derivan.
- Función diferenciada. La seguridad se basa en la definición específica de los roles de seguridad, según lo establecido en el punto “5. Organización de la seguridad” de la presente política.

Adicionalmente, se establecen los siguientes principios generales de seguridad:

- La información y los servicios de la Cámara de Comptos de Navarra deben ser adecuadamente protegidos conforme a su valor y criticidad. La determinación de qué medidas de protección son necesarias se basará en la evaluación del riesgo al que dichos activos se encuentran expuestos.
- Debe también asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y de los sistemas de información relacionados con los servicios que ofrece utilizando para ello el marco de gestión establecido en el ENS.
- El acceso de todo usuario a información de la Cámara de Comptos de Navarra debe ser autorizado y la asignación de sus privilegios de seguridad estar determinada por la necesidad de utilización de dicho activo en el desempeño de sus funciones. No se debe

conceder acceso a aquella información a la que no se le asigne (principio de mínimo privilegios).

- El personal de la Cámara de Comptos de Navarra y cualquier otro personal que trabaje bajo contrato para la misma debe acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones y utilizarla exclusivamente para la realización de las distintas funciones operativas que desempeña para la Cámara de Comptos de Navarra. Cualquier acceso o utilización para finalidades distintas a las establecidas se considerará una infracción de la presente política.
- La Cámara de Comptos de Navarra debe cumplir los requisitos de seguridad establecidos por las leyes y reglamentos españoles y europeos en vigor.
- La Cámara de Comptos de Navarra debe concienciar y formar a su personal sobre la importancia que tiene para el desarrollo de sus actividades y servicios el garantizar la seguridad de la información que maneja y procesa.
- La Política de Seguridad de la Información debe ser difundida y estar disponible para todo el personal y partes interesadas que se determine, según sea apropiado en cada caso.
- La seguridad de la información en la Cámara de Comptos de Navarra debe determinarse en función de los siguientes requisitos mínimos, según se establece en el art. 11 del ENS:
  - Organización e implantación del proceso de seguridad, por medio de la mejora continua, la definición de los roles y responsabilidades en el ámbito de la seguridad de la información y el establecimiento de un Comité de Seguridad de la Información.
  - Análisis y gestión de los riesgos, adoptando una metodología reconocida internacionalmente y revisando periódicamente los riesgos y oportunidades a los que se enfrenta la organización.
  - Gestión de personal, definiendo normas de seguridad asociadas a la gestión de los trabajadores de la organización, su selección y el procedimiento sancionador en caso de incumplimientos de la normativa de seguridad, así como haciéndoles conocedores de las normas de uso de los sistemas de información y sus responsabilidades en el ámbito de la seguridad de la información.
  - Profesionalidad, por medio de la formación y concienciación del personal y normas que determinen la selección adecuada de profesionales proveedores.
  - Autorización y control de los accesos, estableciendo normas y medidas de seguridad para el control de acceso y procedimientos para el alta, modificación y baja de usuarios, asegurando que cada uno de ellos tiene un identificador único.
  - Protección de las instalaciones, estableciendo normas de seguridad relativas a la instalación de sistemas de información en centros de procesado de datos con la requerida seguridad física y de equipos.
  - Adquisición de productos, por medio de normas de seguridad relativas a la adquisición de sistemas de información, contemplando en su caso, las certificaciones que sean necesarias.

- Seguridad por defecto, adoptando en las normas de seguridad los principios de mínimos privilegios y seguridad por defecto.
- Integridad y actualización del sistema, por medio de normas de seguridad donde se contemple la necesidad de autorización de puesta en marcha de un nuevo sistema, así como la actualización periódica de los sistemas.
- Protección de la información almacenada y en tránsito, por medio de normas y medidas de seguridad relativas al manejo de dispositivos móviles, portátiles, memorias USB, etc. y estableciendo y adoptando las medidas de seguridad necesarias para proteger la información en soporte papel.
- Prevención ante otros sistemas de información interconectados, mediante la instalación de sistemas de protección perimetral y estableciendo normas de seguridad asociadas.
- Registro de actividad, estableciendo y ejecutando normas relativas a la necesidad de monitorizar la actividad de los usuarios y administradores del sistema de información.
- Incidentes de seguridad, estableciendo un procedimiento de notificación y gestión de incidentes de seguridad y revisándolas periódicamente para el aprendizaje.
- Continuidad de la actividad, mediante el establecimiento de un procedimiento de respuesta ante incidentes de seguridad que pudieran afectar al servicio prestado.
- Mejora continua del proceso de seguridad, por medio de la revisión periódica del sistema y las auditorías de seguridad de la información.
- Deben realizarse las auditorías que sean necesarias para comprobar el cumplimiento de los requisitos de seguridad establecidos en el ENS.

La Cámara de Comptos de Navarra debe desarrollar y difundir normas de uso para el acceso a los sistemas de información de la entidad por parte de usuarios y personal externo.

# 10 Obligaciones del personal

Todas las personas que forman parte de la Cámara de Comptos de Navarra tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a las personas o servicios afectados.

Asimismo, los usuarios que tengan acceso a los sistemas de información de la Cámara de Comptos de Navarra deben cumplir lo establecido en las normas de uso de dichos sistemas que a tal efecto debe establecer la organización.

Se debe establecer un programa de acciones de concienciación continua para atender a todos los miembros de la Cámara, en particular a quienes se acaben de incorporar.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC deben recibir formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación debe ser 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.

# 11 Terceras partes

Cuando la Cámara de Comptos de Navarra preste servicios a otros organismos o maneje información de otros organismos, se les debe hacer partícipe de esta Política de Seguridad de la Información, establecer canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y establecer procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Cámara de Comptos de Navarra utilice servicios de terceros o ceda información a terceros, se les debe exigir el cumplimento de esta Política de Seguridad de la Información y de la normativa de seguridad que ataña a dichos servicios o información. Dicha tercera parte debe quedar sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se deben establecer procedimientos específicos de reporte y resolución de incidencias. Cuando algún aspecto de la política no pueda ser satisfecho por una tercera parte según se define en los párrafos anteriores, se requerirá al Responsable de Seguridad un informe 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.

# 12 Anexo. Glosario

A efectos de interpretación de la presente política, se considera el siguiente glosario de términos, el cual puede completarse con lo establecido en el Anexo IV del ENS:

- Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- Análisis de riesgos: estudio sistemático y metodológico de la organización para determinar los riesgos que pueden afectar a la seguridad de la información de sus activos.
- Autenticidad: Propiedad consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Confidencialidad: Característica de la información de ser difundida sólo a personas y entidades autorizadas, con procesos en tiempo y forma autorizados.
- Disponibilidad: Característica de la información y de los sistemas de información de ser accesible y utilizable de forma oportuna y adecuada.
- Incidente de seguridad: Suceso ajeno al funcionamiento normal de un servicio, y que causa o puede causar un detrimento de la seguridad del sistema de información en términos de disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad.
- Información: Se aplica a cualquier almacenamiento, comunicación o recepción de conocimiento, tales como, datos, opiniones, incluyendo cifras, gráficos o narrativos, ya sean orales o soportados en cualquier medio.
- Integridad: Característica de la información por la que ha de ser completa y exacta.
- Medidas de seguridad. Conjunto de controles y mecanismos encaminados a proteger los activos de la organización de los riesgos que pudieran afectar a su seguridad. Puede tratarse de medidas de prevención, disuasión, protección, detección y reacción, o de recuperación.
- Sistema de gestión de la seguridad de la información (SGSI): Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.
- Sistema de información: Término general que engloba elementos de hardware, software, aspectos organizativos o administrativos a tener en cuenta para la protección de los recursos informáticos de la entidad.
- Tecnologías de la Información y la Comunicación (TIC): Conjunto de tecnologías desarrolladas para procesar, almacenar y transmitir información. Incluye un conjunto variado de tecnologías incluyendo ordenadores, teléfonos, dispositivos de comunicaciones, servicios (correo electrónico, Internet), etc.

- Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

# 13 Revisiones

| Edición | Fecha | Modificaciones |
|---|---|---|
| 1.0 | 30/03/2020 | - |
| 1.1 | 24/06/2020 | Aprobación por parte de la Presidencia |
| 1.2 | 06/11/2023 | Adecuación al ENS 2022 y cambio de presidente |
| 1.3 | 06/03/2024 | Inclusión POC |

*(Documento firmado digitalmente por Ignacio Cabeza del Salvador, presidente de la Cámara de Comptos de Navarra, en la fecha indicada al margen)*