MINISTERIO
DE ECONOMÍA, COMERCIO
Y EMPRESA

Instituto de Contabilidad y Auditoria de Cuentas

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL INSTITUTO DE CONTABILIDAD Y AUDITORÍA DE CUENTAS

C/ HUERTAS, 26
28014 MADRID
TEL.: 91 389 56 00

www.icac.gob.es

Tabla de contenido

1. Alcance

Este documento contiene la Política General de Seguridad de la Información (en adelante, PGS) del Instituto de Contabilidad y Auditoría de Cuentas (en adelante, ICAC).

El objetivo fundamental de esta Política se centra en definir las estructuras organizativas, roles, responsabilidades, criterios e iniciativas del ICAC respecto a la Seguridad de la Información que almacena y gestiona, así como el cumplimiento de los diferentes marcos normativos que la regulan.

Esta política aplica y será de obligado cumplimiento para todas las subdirecciones del ICAC, así como para terceras partes con las que este instituto comparta información o reciba algún servicio que implique el acceso a la misma.

Para facilitar su conocimiento y cumplimiento, estará disponible en el sitio web del ICAC, así como en la intranet corporativa.

2. Marco normativo y misión

El ICAC es un Organismo Autónomo creado por la Ley 19/1988, adscrito al Ministerio de Economía, Comercio y Empresa, que rige su actuación por las leyes y disposiciones generales que le sean de aplicación y, especialmente, por lo que para dicho tipo de Organismos públicos dispone la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como por lo establecido específicamente en la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en su Reglamento de desarrollo, aprobado por el Real Decreto 2/2021, y en su Estatuto, aprobado por Real Decreto 302/1989.

La base regulatoria que afecta al desarrollo de las actividades del ICAC, y que implica la implementación explícita de medidas de seguridad en los sistemas de información, está constituida por la legislación del procedimiento administrativo y régimen jurídico del sector público, por el reglamento de protección de datos personales, por las normativas e instrucciones técnicas en materia de seguridad en el ámbito de la administración electrónica y otras normativas sectoriales que resulten de aplicación.

Las normas que integran el dicho marco se recogen en un registro a tales efectos, el cual se mantiene actualizado.

La misión del ICAC consiste en generar confianza y seguridad en la economía, proporcionando un marco normativo adecuado para garantizar la fiabilidad de la información corporativa, desde el punto de vista de su formulación (contabilidad y sostenibilidad), y desde el punto de vista de su verificación o auditoría, actuando como el principal elemento dinamizador de la calidad de la auditoría.

Atendiendo a la regulación anteriormente mencionada, al Instituto de Contabilidad y Auditoría de Cuentas le corresponden dos grandes bloques de funciones, por una parte, las que se refieren a la normalización de información corporativa y por otra parte las que corresponden a la auditoría de cuentas. Para obtener más información sobre la estructura y competencias de este organismo puede acceder a la página web.

Adicionalmente, el ICAC actúa en el tratamiento de datos personales conforme a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), así como en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que desarrolla y adapta el citado Reglamento al ordenamiento jurídico español, estableciendo las garantías necesarias para el ejercicio de los derechos de las personas y las obligaciones aplicables a las administraciones públicas en esta materia.

Asimismo, la seguridad de la información y de los sistemas que la soportan en el ámbito del ICAC se rige por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que establece los principios básicos y los requisitos mínimos necesarios para garantizar una protección adecuada de la información tratada y de los servicios prestados por medios electrónicos en el sector público, asegurando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

3. Ámbito objetivo de la PGSI[1]

La PGSI abarca todos los medios, automatizados o no, que el ICAC utiliza para el desarrollo de sus competencias y actividades, así como todos los medios por los cuales interopera con otras Entidades, públicas y/o privadas. Las actividades incluyen:

- Las relaciones de carácter jurídico-económico-administrativo entre los interlocutores sociales y el ICAC.
- La realización de las funciones de negocio/servicio por parte del ICAC, tanto los desarrollados por medios electrónicos como los manuales.
- El tratamiento de la información gestionada por el ICAC en el ejercicio de sus competencias, especialmente aquélla relacionada con datos personales.
- Las relaciones del ICAC con las Administraciones Públicas.

4. Principios básicos

4.1. Introducción

La Política de Seguridad de la Información es el instrumento en que se apoya el ICAC para alcanzar sus objetivos utilizando de forma segura los sistemas de información y las comunicaciones (STIC).

Estos sistemas se convierten en pilares básicos para su funcionamiento, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos definidos en el RD 311/2022 Esquema Nacional de Seguridad (En adelante, ENS).

La Política de Seguridad de la Información, que se plasma en este documento, recoge la forma en que el ICAC gestiona y protege la información y los servicios. En concreto, aquellos que hace uso el ciudadano por medios electrónicos para el ejercicio de derechos y el cumplimiento de deberes en su relación con este organismo.

El objetivo de la seguridad de la información es garantizar la calidad de esta y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

[1] PGSI: Política general de la seguridad de la información

Los STIC deben estar protegidos contra amenazas, de rápida evolución, con potencial para incidir en la integridad, disponibilidad, autenticidad, trazabilidad, confidencialidad, 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 continuidad de los servicios prestados.

Esto implica que las subdirecciones en que se articula el ICAC deben cerciorarse de que la seguridad de los STIC es una parte integral de cada etapa de sus actividades y, desde su concepción hasta la retirada de servicio, deben aplicar las medidas mínimas de seguridad exigidas por el ENS para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

Todos los servicios deben estar preparados para cumplir con sus objetivos utilizando sistemas de información, por lo que deben asegurar que se cumplen los principios básicos que se recogen en los apartados siguientes:

4.2. Seguridad integral y mínimo privilegio

La seguridad se concibe como un proceso integral que involucra elementos técnicos, humanos, materiales y organizativos. El ICAC promueve la concienciación y formación del personal, y requiere que quienes participen en la gestión y operación de la seguridad cuenten con la cualificación adecuada. Los sistemas se diseñan y configuran para otorgar únicamente los privilegios mínimos necesarios para el desempeño de funciones.

El ICAC formará e informará a todo su personal acerca de los deberes y obligaciones en materia de seguridad y garantizará que la atención, revisión y auditoría de los sistemas de seguridad se lleven a cabo por personal cualificado, bajo criterios de profesionalidad, exigiendo además que las organizaciones que le presten servicios cuenten con profesionales y técnicos cualificados y con niveles idóneos de calidad y excelencia en la prestación de sus servicios.

Esto incluye la necesidad de reforzar la seguridad de las cadenas de suministro para hacer frente a posibles amenazas que las dependencias estratégicas no deseadas ejercen en las cadenas de suministro, así como la seguridad de los servicios proporcionados por terceros.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

1) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.

2) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

3) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

4) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

4.3. Gestión de la seguridad basada en los riesgos

La gestión del riesgo constituye un componente central de la seguridad. El ICAC evalúa los riesgos que afectan a la información y los servicios, y despliega medidas de seguridad para reducirlos a niveles aceptables, buscando un equilibrio entre la naturaleza de la información, el nivel de exposición y las salvaguardas aplicables.

4.4. Prevención

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

4.5. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, pudiendo incluso provocar su detención, el responsable de Sistema y los Administradores de Seguridad deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia, según lo establecido en el Artículo 9 del ENS y en la norma ISO 27001.

La monitorización es especialmente relevante cuando se establecen líneas de defensa, práctica requerida por las normativas de referencia y en el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

4.6. Respuesta

El ICAC debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros Organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT), autoridades competentes y, en su caso a los afectados. Este precepto está recogido explícitamente en el ENS y en el RGPD - LOPDGDD (en este último caso, cuando el incidente afecte a datos de carácter personal).

4.7. Recuperación

Para garantizar la disponibilidad de los servicios y las informaciones corporativas, el ICAC debe desarrollar y mantener planes de continuidad de los sistemas de información como parte de su plan general de continuidad de servicio, así como actividades de recuperación en caso de caída total o parcial de los mismos. Estas actuaciones afectan tanto al ENS como a RGPD-LOPDGDD.

4.8. Existencia de líneas de defensa

El ICAC cuenta con una estrategia de protección formada por múltiples capas de seguridad que permitan reaccionar ante incidentes inevitables; reducir la probabilidad de que el sistema quede comprometido y minimizar el impacto de un incidente ya producido. En este sentido, será de especial importancia para la seguridad de la información las siguientes actuaciones de este organismo:

- El control y limitación del acceso a los sistemas de información, el registro de las actividades de los usuarios, y la identificación conductas indebidas o no autorizadas.
- La protección física de las instalaciones de las que tengan control, a través de áreas supervisadas y separadas.
- La adquisición de productos de seguridad que cumplan con las garantías de seguridad necesarias en atención a la categoría de los sistemas y nivel de seguridad de la información afectada.
- La protección de la información almacenada o en tránsito a través de entornos inseguros, como los equipos portátiles, periféricos, soportes de información y comunicaciones.
- La protección de la información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica.
- La protección del perímetro y el análisis de los riesgos derivados de la interconexión del sistema con otros sistemas a través de redes.

4.9. Reevaluación periódica y vigilancia continua

El ICAC implementará mecanismos para la detección de actividades o comportamientos anómalos y su oportuna respuesta.

Del mismo modo, se incluirán el proceso de seguridad en un ciclo de actualización y mejora continua. En este sentido, las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y de los sistemas de protección, bien por la aparición o incremento de los riesgos o bien en cumplimiento de la normativa vigente en cada momento.

5. Datos de carácter personal.

El ICAC trata los datos de carácter personal de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y la Ley Orgánica 3/2018 cuyo objeto es adaptar al mismo el ordenamiento jurídico español y completar sus disposiciones.

La Organización sólo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

De este modo, con la LOPDGDD se han adaptado las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos. De este análisis de riesgos se pueden derivar medidas que se superpongan a las ya descritas como obligatorias para el ENS según la categorización del sistema.

El documento "RATs[2] del ICAC", publicado en su portal web, recoge las actividades de tratamiento de datos personales y los responsables correspondientes. Todos los sistemas de información del ICAC se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento RATs. Asimismo, el organismo dispone de una Política de Privacidad publicada en todos los canales de interacción con el ciudadano, así como en la intranet.

6. Gestión de riesgos

La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica previstos en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS.

[2] RAT: Registro de actividades de tratamiento de datos de carácter personal

7. Formación y concienciación del personal

El ICAC desarrollará actividades específicas orientadas a la formación y concienciación de su personal en materia de seguridad de la información, así como orientadas a la difusión de la Política de Seguridad de la Información y su desarrollo normativo, en particular entre el personal de nueva incorporación.

8. Terceras partes

Cuando el ICAC comparta información o permita el acceso a sus sistemas a terceras partes, ya sea en el marco de contratos, convenios u otros instrumentos jurídicos, dichas terceras partes deberán cumplir los requisitos de seguridad establecidos en la normativa vigente y en la presente Política General de Seguridad de la Información, garantizando un nivel de protección adecuado de la información y de los servicios afectados.

El ICAC velará porque estas obligaciones queden debidamente recogidas en los correspondientes acuerdos, sin perjuicio de los mecanismos de control y supervisión que resulten de aplicación.

9. Entrada en vigor y proceso de revisión

Esta Política General de Seguridad de la Información es efectiva desde la fecha de su aprobación y será válida hasta que sea reemplazada por una nueva.

Texto aprobado en Madrid, por el Presidente del ICAC.

Firmado electrónicamente.