LORENZO PÉREZ SARRIÓN, SECRETARIO GENERAL DE LA SINDICATURA DE COMPTES,

CERTIFICO: Que el presente documento se corresponde con el texto consolidado autorizado por el Consell en su sesión realizada el día 9 de junio de 2021.

Fecha y firma electrónica según codificación al margen.

ACUERDO DEL CONSELL DE LA SINDICATURA DE COMPTES DE LA COMUNITAT VALENCIANA, DE FECHA 5 DE JUNIO DE 2019, POR EL QUE SE APRUEBA EL DOCUMENTO DE POLÍTICAS GENERALES DE GESTIÓN Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE ESTA INSTITUCIÓN.

1. APROBACIÓN Y ENTRADA EN VIGOR

Este documento ha sido aprobado el día 5 de junio de 2019 por el Consell de la Sindicatura de Comptes de la Comunitat Valenciana y entrará en vigor el día siguiente a su publicación en el *Boletín Oficial de Les Corts*.

2. INTRODUCCIÓN

Para poder desarrollar las funciones asignadas a la Sindicatura de Comptes con la economía, eficiencia y eficacia exigibles, es imprescindible la utilización intensiva de las tecnologías de la información y las comunicaciones (TIC), cuya gestión debe estar siempre orientada a facilitar la consecución de los objetivos de la Institución.

La Sindicatura de Comptes siempre ha asumido como propio el compromiso de garantizar que las TIC se utilizan de una forma segura. El Consell de la Sindicatura de Comptes mediante el Acuerdo de 25 de febrero de 2009 aprobó el documento que contenía las políticas generales de gestión y seguridad de los sistemas de información (SI) y fue una de las primeras instituciones valencianas en adoptar un compromiso con la seguridad de la información de este tipo.

Aunque las políticas de seguridad aprobadas en 2009 estaban alineadas con los principios de la seguridad de la información vigentes, el transcurso del tiempo y la publicación de diversas normas jurídicas, entre ellas el Real Decreto 3/2010, de 8 de enero, por el que se aprueba el Esquema Nacional de Seguridad (ENS) hicieron necesario adaptar las políticas

de seguridad a la evolución tecnológica y normativa, lo que tuvo lugar mediante acuerdo del Consell de 23 de marzo de 2017.

La tarea de adaptación de las políticas de seguridad de la información que se aborda en este documento, que sustituye al aprobado en 2017, es una de las revisiones previstas en el artículo 7.1 que atribuye a la Comisión de Informática y Gestión de Seguridad de la Información (CIGSI) las propuestas de modificación del documento y se ha realizado conforme a las guías de seguridad del Centro Criptológico Nacional CCN-STIC-805, Esquema Nacional de Seguridad/Política de Seguridad de la Información, CCN-STIC-801, Esquema Nacional de Seguridad/Responsables y funciones, y resto de normas y buenas prácticas en la materia publicadas o actualizadas desde la última revisión del documento de Políticas de Seguridad.

Las políticas contenidas en el presente documento son la plasmación del compromiso que adquiere el Consell de la Sindicatura de garantizar el adecuado funcionamiento de los SI y pretenden que esta utilización más intensiva de las TIC se realice de acuerdo con los códigos de buenas prácticas reconocidos internacionalmente (Cobit y UNE-ISO/IEC 27002, principalmente).

En sí mismas, las políticas aquí definidas constituyen un elemento de buenas prácticas en materia de seguridad de la información, tal como se detalla en el apartado 5 del Código de Buenas Prácticas para los Controles de la Seguridad de la Información UNE-ISO/IEC 27002.

3. ALCANCE

3.1. Alcance de ámbito personal

Las políticas de gestión y seguridad de los sistemas de información de la Sindicatura de Comptes contenidas en el presente documento y las normas que las desarrollan son de carácter obligatorio para todo el personal de la Sindicatura de Comptes y para todos aquellos que obtengan acceso autorizado a su red.

3.2. Alcance de ámbito objetivo

Las políticas de gestión y seguridad de los SI abarcan los siguientes elementos:

- Toda la información referida a datos o relacionada con la funcionalidad de los sistemas de información de la Sindicatura de Comptes, cualquiera que sea el soporte en que se encuentre.

- Todos los recursos implicados en los SI de la Sindicatura de Comptes.

4. MISIÓN U OBJETIVOS DEL ORGANISMO

Corresponde a la Sindicatura de Comptes de la Comunitat Valenciana, de acuerdo con el artículo 1 de su Ley de creación "el control externo económico y presupuestario de la actividad del sector público valenciano …"

El objetivo fundamental de la Sindicatura es, por tanto, realizar esa labor de fiscalización con el mayor grado de economía y eficiencia en la gestión de los medios y eficacia en el logro de los objetivos de fiscalización fijados en los planes aprobados por el Consell.

Las TIC constituyen una herramienta ineludible que debe ser utilizada de forma adecuada para minimizar los riesgos, siempre existentes, 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 (sólo quienes están autorizados pueden acceder a la información).

- Asegurar el cumplimiento de las leyes, regulaciones y estándares aplicables.

5. PRINCIPIOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los principios en materia de gestión de la seguridad de los SI que se adoptan son los siguientes:

- Consideración de la seguridad de SI como un proceso integral.

- Gestión de la seguridad basada en riesgos.

- Prevención, reacción y recuperación.

- Líneas de defensa.

- Reevaluación periódica.

- La seguridad como función diferenciada.

De estos principios se extraen las siguientes consideraciones que deberán trasladarse a todo el personal de la Sindicatura de Comptes y, en su caso, a todos los que en cualquier momento tengan acceso autorizado a red:

- La seguridad de los sistemas de información como objetivo en sí mismo.

- Concienciación. El personal de la Sindicatura debe ser consciente de la necesidad de contar con sistemas de información y redes seguros y colaborar a su consecución. La seguridad de una red viene dada por su eslabón más débil.

- Responsabilidad. Todo el personal, a su nivel, es responsable de la seguridad de los sistemas de información y redes.

- Respuesta. De acuerdo con las funciones asignadas, se debe actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes que afecten a la seguridad de los SI.

- Formación. Se establecerán los planes de formación y concienciación necesarios para que los usuarios de la red sepan utilizar de forma adecuada todas las herramientas que mejoran la seguridad en el uso de los SI.

- Seguimiento. Se practicarán evaluaciones periódicas sobre el nivel de seguridad de la red cuyas propuestas de mejora se trasladarán al Consell para su incorporación a las políticas, protocolos y demás normas que regulen la utilización de los SI de la Sindicatura de Comptes.

6. MARCO NORMATIVO

El marco normativo para el desarrollo de la gestión de los servicios y competencias de la Sindicatura de Comptes de la Comunitat Valenciana es el siguiente:

- Ley Orgánica 1/2006, de 10 de abril, de reforma del Estatuto de Autonomía de la Comunitat Valenciana.

- Ley de la Generalitat Valenciana 6/1985, de 11 de mayo, de Sindicatura de Comptes, texto consolidado tras la aprobación de la ley 16/2017, de 10 de noviembre.

- Reglamento de Régimen Interior de la Sindicatura de Comptes, aprobado por acuerdo del Consell de la Sindicatura de Comptes en fecha 23 de mayo de 2018, publicado en el DOGV 8308 de 1 de junio de 2018.

- Acuerdo de 12 de septiembre de 2012, del Consell de la Sindicatura de Comptes por el cual se aprueba la constitución de la sede electrónica de esta Institución y se regula su funcionamiento.

- Acuerdo de 12 de septiembre de 2012, del Consell de la Sindicatura de Comptes, por el cual se crea y se regula el funcionamiento del Registro Electrónico de esta Institución.

- Decreto 220/2014, de 12 de diciembre, del Consell, por el que se aprueba el Reglamento de Administración Electrónica de la Comunitat Valenciana.

- 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.

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

- Ley 6/2020, d'11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza..

7. ORGANIZACIÓN DE 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.

7.1. Responsabilidad de la seguridad de la información

El máximo responsable de la seguridad de la información en la Sindicatura de Comptes es el Consell de la Sindicatura, quien, de acuerdo con las competencias que tiene atribuidas, aprueba las políticas generales contenidas en este documento.

La Comisión de Informática y de Gestión de Seguridad de la Información (CIGSI) revisará bienalmente la política de seguridad de la información aprobada y propondrá al Consell de la Sindicatura de Comptes las modificaciones que considere necesarias.

Además, el Consell de la Sindicatura aprobará la normativa de seguridad de la información de primer y segundo nivel, a partir de las propuestas que le formule la CIGSI, tal como se recoge en el punto 11 de este documento.

Para completar el esquema organizativo en materia de seguridad de la información se actualiza la composición y funciones de la CIGSI y se asignan las funciones del responsable de seguridad de la información y responsable de seguridad del sistema tal y como se detalla en los apartados siguientes.

7.2. Comisión de Informática y de Gestión de Seguridad de la Información

La Comisión de informática y de Gestión de Seguridad de la Información de la Sindicatura estará compuesta por los siguientes miembros, con voz y voto:

- Un síndic que actuará como presidente.

- El director del gabinete técnico.

- El jefe de la unidad de auditoría de sistemas de información.

- El responsable del departamento de informática.

- La responsable de la biblioteca-archivo.

- El letrado jefe.

- La técnica de administración electrónica y aplicaciones corporativas.

- El secretario general de la Sindicatura, que actuará como Secretario de la Comisión.

Cuando un miembro desempeñe las funciones legalmente previstas para el Delegado de protección de Datos, continuará como tal, pero sin capacidad de voto.

La Comisión de Informática y Gestión de Seguridad de la Información tendrá las siguientes competencias:

- Asumirá las funciones de responsable de la información, 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.

- Asumirá las funciones de responsable del 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:

    - 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.
    - Revisar cada dos años la política de seguridad y proponer al Consell de la Sindicatura las modificaciones que sean necesarias.
    - Proponer al Consell de la Sindicatura de Comptes la modificación de las políticas o la adopción de normas de desarrollo de las políticas generales en materia de seguridad de la información de nivel 2. A tal efecto se podrán constituir grupos de trabajo con participación de funcionarios de la Sindicatura ajenos a la propia Comisión.
    - Aprobar la normativa de seguridad de la información de nivel 3, como los procedimientos operativos de seguridad de las TIC e instrucciones técnicas.
    - Propuesta y análisis de los proyectos y planes de inversión en materia de SI que garanticen la alineación de la organización y medios de los SI con los objetivos generales de la Sindicatura de Comptes.
    - Revisión y seguimiento de las incidencias en la seguridad de la información.

- Revisión y propuesta de las iniciativas principales para mejorar la seguridad de la información.
- Seguimiento de las medidas adoptadas para implantar controles sobre seguridad de la información.
- Competencia en materia de gestión documental, ciclo de vida del documento electrónico, así como firma, sello electrónico y certificados de la Sindicatura.

7.3. Responsable en materia 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 Sindicatura de Comptes.

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, 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 a la CIGSI.

- Firmar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

- Informar a la CIGSI 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.

7.4. Responsable del sistema

Se asignan las funciones de responsable del sistema al responsable del departamento de informática.

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.

- Así mismo dará cuenta a la Comisión de Informática y Gestión 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.

7.5. Administrador de la seguridad del sistema

Bajo la dependencia del responsable de seguridad se asigna la responsabilidad de administrador de seguridad del sistema al jefe de la unidad de auditoría de sistemas de información y apoyo.

Las funciones del administrador de la seguridad del sistema comprenden las siguientes:

- 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.

7.6. Atribución de responsabilidades en materia de seguridad de la información al resto de órganos o personal de la Sindicatura

Todo el personal de la Sindicatura tiene la responsabilidad de aplicar en lo referente a las funciones que tiene asignadas las políticas de seguridad y su normativa de desarrollo.

Los auditores y jefes de departamentos serán responsables de los procedimientos y la información que se genere en el ejercicio de las funciones y trabajos que se les asignen y deberán verificar que en los procedimientos aplicados se cumplen las políticas de seguridad y su normativa de desarrollo, tramitando una incidencia informática cuando detecten incoherencias en los procedimientos con las políticas de seguridad.

8. CONCIENCIACIÓN Y FORMACIÓN

Constituye un objetivo de primer orden de la Sindicatura de Comptes lograr la plena conciencia respecto a que la seguridad de la información afecta a todo el personal y miembros de la Institución y a todas las actividades de acuerdo con el principio de seguridad integral recogido en el artículo 5 del ENS. Por ello, la Sindicatura de Comptes propondrá y organizará sesiones formativas y de concienciación para que todos los empleados adquieran conciencia de los riesgos que se corren.

Previo informe del responsable del sistema, el responsable de seguridad propondrá a la CIGSI una política de formación y concienciación en el tratamiento a seguir de la información. La CIGSI aprobará esa política de formación y trasladará a la Comisión de Formación la planificación de cursos o actividades en materia de seguridad de la información necesarios para su cumplimiento.

9. DATOS DE CARÁCTER PERSONAL

La Sindicatura de Comptes trata datos de carácter personal. El registro de actividades de tratamiento de datos personales, elaborado y publicado por la Sindicatura de Comptes en su sede electrónica recoge las características de todos los tratamientos llevados a cabo por la Institución.

Todos los sistemas de información 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 registro.

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.

10. 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 riesgos (artículo 6 del Real Decreto 3/2010, de 8 de enero, ENS) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero, ENS).

- Los responsables de la información y del servicio son los encargados, contando en el proceso con la participación y asesoramiento del responsable de seguridad y del responsable del sistema, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardias a implantar.

- Los responsables de la información y del servicio son los responsables de los riesgos sobre la información y los servicios, respectivamente, y por tanto, de aceptar los riesgos residuales calculados en el análisis, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

- 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 proporcionadas a los riesgos y estar justificadas, deberá revisarse cada año por parte del responsable de seguridad, que elevará un informe a la CIGSI.

11. DESARROLLO NORMATIVO DE LA POLÍTICA DE SEGURIDAD

11.1. Cuerpo normativo

- El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en cuatro niveles, según el ámbito de aplicación y nivel de detalle técnico, de manera que cada norma de un determinado nivel se fundamente en las normas de nivel superior. Dichos niveles de desarrollo son los siguientes:

    a) Primer nivel normativo: Políticas de seguridad de la información. Constituyen las directrices básicas para la utilización de medios electrónicos en la Sindicatura de Comptes y que se plasman en la presente norma. Serán aprobadas o modificadas por el Consell de la Sindicatura de Comptes a propuesta de la CIGSI.

    b) Segundo nivel normativo: Las normas de seguridad TIC de desarrollo de las políticas de seguridad de la información establecen con un mayor grado de detalle dentro de un ámbito determinado esas políticas. Dan respuesta, sin detalles de implementación ni tecnológicos, a qué se puede hacer y qué no en relación con un cierto tema desde el punto de vista de la seguridad. Serán aprobadas o modificadas por el Consell de la Sindicatura de Comptes a propuesta de la CIGSI.

c) Tercer nivel normativo: Procedimientos operativos e instrucciones técnicas de seguridad de la información. Son documentos que dan respuesta a la forma en que se puede realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos en ella establecidos y pueden incluir detalles de implementación y tecnológicos. El responsable de seguridad propondrá a la CIGSI los procedimientos e instrucciones técnicas para su aprobación.

d) Cuarto nivel normativo. Guías y protocolos de carácter técnico que recogen la forma de trabajar en procedimientos concretos y/o con determinadas aplicaciones. Serán aprobadas por los responsables funcionales de los procedimientos de gestión. En concreto, los protocolos de trabajo de la aplicación de gestión de las fiscalizaciones serán aprobados por el responsable del gabinete técnico de la Sindicatura de Comptes.

Cada nivel normativo debe respetar la legislación aplicable relacionada y lo prescrito por los niveles superiores en materia de seguridad de la información.

El responsable de seguridad y el de sistemas serán los encargados de mantener la documentación de seguridad actualizada y organizada y gestionar los mecanismos de acceso a la misma.

- Materias objeto de desarrollo normativo

Los documentos mencionados en el apartado anterior deberán abordar, al menos, los siguientes aspectos:

- Condiciones para el acceso a la información
- Uso del equipamiento informático y de comunicaciones
- Gestión de incidentes y problemas
- Continuidad de operaciones
- Seguridad con terceros
- Clasificación y tratamiento de la información
- Análisis y gestión de riesgos
- Seguridad física y del personal
- Prevención de virus y código malicioso
- Ciclo de vida de los sistemas de información
- Mejora continua. Niveles de madurez
- Elaboración, publicación y revisión de la política de seguridad de la información y de los documentos complementarios

12. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Sindicatura de Comptes (síndics, secretario general y personal) tienen la obligación de conocer y cumplir la política y la normativa de seguridad de la información, siendo responsabilidad de la CIGSI disponer los medios necesarios para que la información llegue a los afectados.

Las políticas de seguridad de la información se publicarán en el BOCV y las normas de desarrollo normativo de estas políticas se comunicarán por correo electrónico a todos los miembros de la Sindicatura (personal y altos cargos) cuando sean aprobadas o modificadas y estarán disponibles para sus destinatarios en la Intranet corporativa.

Todo el personal que se incorpore a la Sindicatura de Comptes o que vaya a tener acceso a alguno de sus sistemas de información o a la información gestionada a través de ellos, será informado de la política de seguridad y sus normas de desarrollo.

Los incumplimientos de las políticas y normas de seguridad de la información se tramitarán de acuerdo con las previsiones establecidas en la Ley de Sindicatura de Comptes y con el procedimiento sancionador general aplicable los funcionarios públicos previsto en el Estatuto Básico del Empleado público.

13. TERCERAS PARTES

Los contratos o convenios que suscriba la Sindicatura de Comptes partir de la entrada en vigor de estas políticas que contemplen o requieran el acceso del personal a las instalaciones o sistemas de información de la Sindicatura de Comptes, deberán incluir una cláusula de cumplimiento de esta política, junto con un procedimiento de verificación adecuado. Los contratos y convenios firmados con anterioridad a esa fecha se revisarán en el mismo sentido. Se establecerán con estas empresas o entidades procedimientos de actuación ante incidentes de seguridad.

14. PROCESO DE REVISIÓN DE LA POLÍTICA DE SEGURIDAD

Las propuestas de revisión de la política de seguridad las elaborará la CIGSI y serán aprobadas por el Consell de la Sindicatura de Comptes.

15. DISPOSICIÓN DEROGATORIA

Se deroga el Acuerdo de la Sindicatura de Comptes, de fecha 23 de marzo de 2017 por el que se aprobó el documento de políticas generales de gestión y seguridad de los sistemas de información de la Sindicatura de Comptes de la Comunitat Valenciana.

València, 5 de junio de 2019. **El síndic major**.