IV. SINDICATURA DE COMPTES

Acord del Consell de la Sindicatura de Comptes de la Comunitat Valenciana, de data 23 de març de 2017, pel qual s'aprova el document de polítiques generals de gestió i seguretat dels sistemes d'informació d'aquesta institució

1. APROVACIÓ I ENTRADA EN VIGOR

Aquest document ha sigut aprovat el dia 23 de març de 2017 pel Consell de la Sindicatura de Comptes de la Comunitat Valenciana i entrarà en vigor a l'endemà de la seua publicació en el *Butlletí Oficial de les Corts*.

2. INTRODUCCIÓ

Per a poder desenvolupar les funcions assignades a la Sindicatura de Comptes amb l'economia, eficiència i eficàcia exigibles, és imprescindible la utilització intensiva de les tecnologies de la informació i les comunicacions (TIC), la gestió de les quals ha d'estar sempre orientada a facilitar la consecució dels objectius de la Institució.

La Sindicatura de Comptes sempre ha assumit com a propi el compromís de garantir que les TIC s'utilitzen d'una forma segura. El Consell de la Sindicatura de Comptes mitjançant l'Acord de 25 de febrer de 2009, va aprovar el document que contenia les polítiques generals de gestió i seguretat dels sistemes d'informació (SI) i va ser una de les primeres institucions valencianes a adoptar un compromís amb la seguretat de la informació d'aquest tipus.

Encara que les polítiques de seguretat aprovades en 2009 estan alineades amb els principis de la seguretat de la informació vigents, el transcurs del temps i la publicació de diverses normes jurídiques, com ara el Reial Decret 3/2010, de 8 de gener, pel qual s'aprova l'Esquema Nacional de Seguretat (ENS), fan necessari adaptar les polítiques de seguretat a l'evolució tecnològica i normativa.

La tasca d'adaptació de les polítiques de seguretat de la informació és la que s'aborda en aquest document que substitueix a l'aprovat el 2009 i s'ha realitzat d'acord amb les guies de seguretat del Centre Criptològic Nacional CCN-STIC-805, Esquema Nacional de Seguretat/Política de Seguretat de la Informació i CCN-STIC-801, Esquema Nacional de Seguretat/Responsables i funcions.

Les polítiques contingudes en el present document són la plasmació del compromís que adquireix el Consell de la Sindicatura de garantir l'adequat funcionament dels SI, i pretenen que aquesta utilització més intensiva de les TIC es realitze d'acord amb els codis de bones pràctiques reconeguts internacionalment (Cobit i UNE-ISO/IEC 27002, principalment).

En si mateixes, les polítiques definides ací constitueixen un element de bones pràctiques en matèria de seguretat de la informació, tal com es detalla en l'apartat 5 del Codi de Bones Pràctiques per als Controls de la Seguretat de la Informació UNE-ISO/IEC 27002.

IV. SINDICATURA DE COMPTES

Acuerdo del Consell de la Sindicatura de Comptes de la Comunitat Valenciana, de fecha 23 de marzo de 2017, 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 23 de marzo de 2017 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 están 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) hacen necesario adaptar las políticas de seguridad a la evolución tecnológica y normativa.

La tarea de adaptación de las políticas de seguridad de la información es la que se aborda en este documento que sustituye al aprobado en 2009 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 y CCN-STIC-801, Esquema Nacional de Seguridad/Responsables y funciones.

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. ABAST

3.1. Abast d'àmbit personal

Les polítiques de gestió i seguretat dels sistemes d'informació de la Sindicatura de Comptes contingudes en el present document i les normes que les desenvolupen són de caràcter obligatori per a tot el personal de la Sindicatura de Comptes i per a tots aquells que obtinguen accés autoritzat a la seua xarxa.

3.2. Abast d'àmbit objectiu

Les polítiques de gestió i seguretat dels SI contenen els elements següents:

– Tota la informació referida a dades o relacionada amb la funcionalitat dels sistemes d'informació de la Sindicatura de Comptes, siga quin siga el suport en què es troba.

– Tots els recursos implicats en els SI de la Sindicatura de Comptes.

4. MISSIÓ O OBJECTIUS DE L'ORGANISME

Correspon a la Sindicatura de Comptes de la Comunitat Valenciana, d'acord amb l'article 1 de la seua Llei de creació «el control extern econòmic i pressupostari de l'activitat del sector públic valencià ...»

L'objectiu fonamental de la Sindicatura és, per tant, realitzar aqueixa labor de fiscalització amb el major grau d'economia i eficiència en la gestió dels mitjans i eficàcia per aconseguir els objectius de fiscalització fixats en els plans aprovats pel Consell.

Les TIC constitueixen una eina ineludible que ha de ser utilitzada de forma adequada per minimitzar els riscos, sempre existents, que comporta la seua utilització, i garantir raonablement la seguretat de la informació, la qual cosa inclou:

– Assegurar la disponibilitat dels SI i de les dades emmagatzemades en aquests SI (els usuaris autoritzats tenen accés a la informació i els seus actius associats quan ho requereixen).

– Assegurar la integritat de la informació emmagatzemada en els SI (la informació i els seus mètodes de procés són exactes i complets).

– Preservar la confidencialitat de les dades sensibles (només els que estan autoritzats poden accedir a la informació).

– Assegurar el compliment de les lleis, regulacions i estàndards aplicables.

5. PRINCIPIS DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Els principis en matèria de gestió de la seguretat dels SI que s'adopten són els següents:

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:

– Consideració de la seguretat de SI com un procés integral.

– Gestió de la seguretat basada en riscos.

– Prevenció, reacció i recuperació.

– Línies de defensa.

– Reavaluació periòdica.

– La seguretat com a funció diferenciada.

D'aquests principis s'extreuen les consideracions següents que hauran de traslladar-se a tot el personal de la Sindicatura de Comptes i, si escau, a tots els que en qualsevol moment tinguin accés autoritzat a xarxa:

– La seguretat dels sistemes d'informació com a objectiu en si mateix.

– Conscienciació. El personal de la Sindicatura ha de ser conscient de la necessitat de comptar amb xarxes i sistemes d'informació segurs i col·laborar a la seua consecució. La seguretat d'una xarxa ve donada per la seua baula més feble.

– Responsabilitat. Tot el personal, al seu nivell, és responsable de la seguretat dels sistemes d'informació i xarxes.

– Resposta. D'acord amb les funcions assignades, s'ha d'actuar de manera oportuna i cooperativa per prevenir, detectar i respondre a incidents que afecten la seguretat dels SI.

– Formació. S'establiran els plans de formació i conscienciació necessaris perquè els usuaris de la xarxa sàpiguen utilitzar de forma adequada totes les eines que milloren la seguretat en l'ús dels SI.

– Seguiment. Es practicaran avaluacions periòdiques sobre el nivell de seguretat de la xarxa, les propostes de millora de la qual es traslladaran al Consell per a la seua incorporació a les polítiques, protocols i altres normes que regulen la utilització dels SI de la Sindicatura de Comptes.

6. MARC NORMATIU

El marc normatiu per al desenvolupament de la gestió dels serveis i competències de la Sindicatura de Comptes de la Comunitat Valenciana és el següent:

– Llei Orgànica 1/2006, de 10 d'abril, de reforma de l'Estatut d'Autonomia de la Comunitat Valenciana.

– Llei de la Generalitat Valenciana 6/1985, d'11 de maig, de Sindicatura de Comptes.

– Acord de 19 de setembre de 1986, de la Comissió de Coordinació, Organització i Règim de les Institucions de la Generalitat de les Corts Valencianes, pel qual s'aprova el Reglament de Règim Interior de la Sindicatura de Comptes.

– 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.

– Acuerdo de 19 de septiembre de 1986, de la Comisión de Coordinación, Organización y Régimen de las Instituciones de la Generalitat de las Corts Valencianes, por el que se aprueba el Reglamento de Régimen Interior de la Sindicatura de Comptes.

– Acord de 12 de setembre de 2012, del Consell de la Sindicatura de Comptes pel qual s'aprova la constitució de la seu electrònica d'aquesta Institució i es regula el seu funcionament.

– Acord de 12 de setembre de 2012, del Consell de la Sindicatura de Comptes, pel qual es crea i es regula el funcionament del Registre Electrònic d'aquesta Institució.

– Decret 220/2014, de 12 de desembre, del Consell, pel qual s'aprova el Reglament d'Administració Electrònica de la Comunitat Valenciana.

– Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

– Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de Desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de Protecció de Dades de Caràcter Personal.

– Llei 59/2003, de 19 de desembre, de Signatura Electrònica.

7. ORGANITZACIÓ DE SEGURETAT

La responsabilitat sobre la seguretat de la informació dels SI recau sobre tota l'organització i es reparteix d'acord amb les funcions i responsabilitats de cada lloc o òrgan.

7.1. Responsabilitat de la seguretat de la informació

El màxim responsable de la seguretat de la informació a la Sindicatura de Comptes és el Consell de la Sindicatura, que, d'acord amb les competències que té atribuïdes, aprova les polítiques generals contingudes en aquest document.

La Comissió d'Informàtica i de Gestió de Seguretat de la Informació (CIGSI) revisarà biennalment la política de seguretat de la informació aprovada, i proposarà al Consell de la Sindicatura de Comptes les modificacions que considere necessàries.

A més, el Consell de la Sindicatura aprovarà la normativa de seguretat de la informació de primer i segon nivell, a partir de les propostes que formule la CIGSI, tal com es recull en el punt 11 d'aquest document.

Per completar l'esquema organitzatiu en matèria de seguretat de la informació s'actualitza la composició i funcions de la Comissió d'Informàtica i de Gestió de Seguretat de la Informació i s'assignen les funcions del responsable de seguretat de la informació i responsable de seguretat del sistema tal i com es detalla en els apartats següents.

7.2. Comissió d'Informàtica i de Gestió de Seguretat de la Informació

La Comissió d'Informàtica i de Gestió de Seguretat de la Informació de la Sindicatura estarà composta pels membres següents:

– 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.

– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

– Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

– Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

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:

– Un síndic que actuarà com a president

– El director del gabinet tècnic

– El cap de la unitat d'auditoria de sistemes d'informació

– El responsable del departament d'informàtica

– La responsable de la biblioteca-arxiu

– El lletrat en cap

– El secretari general de la Sindicatura, que actuarà com a secretari de la Comissió

La Comissió d'Informàtica i Gestió de Seguretat de la Informació tindrà les competències següents:

– Assumirà les funcions de responsable de la informació, tal com vénen definides en el Reial Decret 3/2010, de 8 de gener, pel qual s'aprova l'ENS, entre les quals es troben les següents:

– Establir les necessitats de seguretat de la informació que es maneja.

– Efectuar valoracions de l'impacte que tindria un incident que afectés la seguretat de la informació per a cada tipus d'informació.

– Aprovar o modificar el nivell de seguretat requerit per a cada tipus d'informació.

– Assumirà les funcions de responsable del servei, tal com vénen definides en el Reial Decret 3/2010, de 8 de gener, pel qual s'aprova l'ENS, entre les quals es troben les següents:

– Determinar els requisits de seguretat del servei prestat.

– Efectuar valoracions de l'impacte que tindria un incident que afectés la seguretat de la informació per a cada servei.

– Aprovar o modificar el nivell de seguretat requerit per als serveis prestats.

– Revisar cada dos anys la política de seguretat i proposar al Consell de la Sindicatura les modificacions que calguen.

– Proposar al Consell de la Sindicatura de Comptes la modificació de les polítiques o l'adopció de normes de desenvolupament de les polítiques generals en matèria de seguretat de la informació de nivell 2. Amb aquesta finalitat es podran constituir grups de treball amb participació de funcionaris de la Sindicatura aliens a la mateixa Comissió.

– Aprovar la normativa de seguretat de la informació de nivell 3, com els procediments operatius de seguretat de les TIC i instruccions tècniques.

– Proposta i anàlisi dels projectes i plans d'inversió en matèria de SI que garantisquen l'alineació de l'organització i

– 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.

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

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

mitjans dels SI amb els objectius generals de la Sindicatura de Comptes.

– Revisió i seguiment de les incidències en la seguretat de la informació.

– Revisió i proposta de les iniciatives principals per millorar la seguretat de la informació.

– Seguiment de les mesures adoptades per a implantar controls sobre seguretat de la informació.

7.3. Responsable en matèria de seguretat de la informació

El responsable de seguretat és la persona que determina les decisions per satisfer els requisits de seguretat de la informació i del servei.

El responsable de seguretat de la informació serà el secretari general de la Sindicatura de Comptes.

Les funcions del responsable de seguretat seran les següents:

– Mantenir la seguretat de la informació manejada i dels serveis prestats pels sistemes d'informació, d'acord amb la política de seguretat de la informació.

– Supervisar el compliment de la política de seguretat, les seues normes, procediments i configuració de seguretat dels sistemes.

– Assessorar, en col·laboració amb el responsable del sistema, els responsables de la informació i els responsables del servei en la realització dels preceptius anàlisi de riscos, i revisar el procés de gestió del risc, elevant un informe anual a la CIGSI.

– Signar la declaració d'aplicabilitat, que comprèn la relació de mesures de seguretat seleccionades per a un sistema.

– Informar la CIGSI de les actuacions realitzades en matèria de seguretat de la informació i dels incidents de seguretat.

– Promoure la formació i conscienciació en matèria de seguretat de la informació.

7.4. Responsable del sistema

S'assignen les funcions de responsable del sistema al responsable del departament d'informàtica.

Les funcions del responsable del sistema comprenen les següents:

– Tindrà la responsabilitat de desenvolupar, operar i mantenir el sistema d'informació durant tot el seu cicle vital, de les seues especificacions, instal·lació i verificació del seu correcte funcionament.

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.

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.

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 topologia i sistema de gestió del sistema d'informació, i establir els criteris d'ús i els serveis disponibles.

– Assegurar-se que les mesures específiques de seguretat s'integren adequadament dins el marc general de seguretat.

– Implantar les mesures necessàries per garantir la seguretat del sistema durant tot el seu cicle de vida, seguint les observacions del responsable de seguretat.

– Informar el responsable de seguretat.

– Així mateix donarà compte a la Comissió d'Informàtica i Gestió de Seguretat de la Informació dels riscos i incompliments de les polítiques que detecte per tal d'adoptar les mesures correctores que en corresponguen.

– Gestionar les autoritzacions concedides als usuaris en els sistemes sota la seua responsabilitat, privilegis concedits, incloent el monitoratge de l'activitat, amb la supervisió del responsable de seguretat.

– Monitoritzar l'estat de seguretat del sistema, sota la supervisió del responsable de seguretat.

– Informar els responsables de la informació, del servei i de seguretat de les anomalies detectades.

– Col·laborar en la investigació i resolució d'incidents de seguretat.

El responsable del sistema, tot i que manté la responsabilitat, podrà nomenar delegats que es faran càrrec de les funcions delegades relacionades amb l'operació, manteniment, instal·lació i verificació del correcte funcionament del sistema d'informació.

7.5. Administrador de la seguretat del sistema

Sota la dependència del responsable de seguretat, s'assigna la responsabilitat d'administrador de seguretat del sistema al cap de la unitat d'auditoria de sistemes d'informació i suport.

Les funcions de l'administrador de la seguretat del sistema comprenen les següents:

– Monitoritzar l'estat de seguretat del sistema, analitzant la informació proporcionada per l'eina de gestió d'esdeveniments de seguretat i mecanismes d'auditoria tècnica instal·lats en el sistema.

– Supervisar que tot l'equipament s'ajusta a l'autoritzat.

– Supervisar les activitats dels administradors del sistema: actuacions i aplicació dels procediments de seguretat establits.

– Supervisar que les activitats dels usuaris del sistema són conformes amb les autoritzacions concedides.

– 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. Reconeixement de responsabilitats en matèria de seguretat de la informació a la resta d'òrgans o personal de la Sindicatura

Pel que fa a les funcions que té assignades, tot el personal de la Sindicatura té la responsabilitat d'aplicar les polítiques de seguretat i la normativa de desenvolupament.

Els auditors i caps de departaments seran responsables dels procediments i la informació que es genere en l'exercici de les funcions i treballs que se'ls assignen i hauran de verificar que en els procediments aplicats es compleixen les polítiques de seguretat i la normativa de desenvolupament, tramitant una incidència informàtica quan detecten incoherències en els procediments amb les polítiques de seguretat.

8. CONSCIENCIACIÓ I FORMACIÓ

Constitueix un objectiu de primer ordre de la Sindicatura de Comptes aconseguir la plena consciència respecte al fet que la seguretat de la informació afecta tot el personal i membres de la Institució i totes les activitats, d'acord amb el principi de seguretat integral recollit en l'article 5 de l'ENS. Per això, la Sindicatura de Comptes proposarà i organitzarà sessions formatives i de conscienciació perquè tots els empleats tinguen consciència dels riscos que es corren.

Amb un informe previ del responsable del sistema, el responsable de seguretat proposarà a la CIGSI una política de formació i conscienciació en el tractament que cal seguir de la informació. La CIGSI aprovarà aquesta política de formació i traslladarà a la Comissió de Formació la planificació de cursos o activitats en matèria de seguretat de la informació necessaris per al seu compliment.

9. DADES DE CARÀCTER PERSONAL

La Sindicatura de Comptes tracta dades de caràcter personal. El document de seguretat de la informació recull els fitxers afectats i els responsables corresponents. Tots els sistemes d'informació s'ajustaran als nivells de seguretat requerits per la normativa per a la naturalesa i finalitat de les dades de caràcter personal recollides en l'esmentat document de seguretat.

En cas de conflicte amb la normativa de seguretat prevista en aquestes polítiques, prevaldrà la norma que presente un major nivell d'exigència respecte a la protecció de les dades personals.

10. GESTIÓ DE RISCOS

– La gestió de riscos s'ha de fer de manera contínua sobre els sistemes d'informació, d'acord amb els principis de gestió de la seguretat basada en riscos (article 6 del Reial Decret 3/2010, de 8 de gener, ENS) i reavaluació periòdica (article 9 del Reial Decret 3/2010, de 8 de gener, ENS).

– Els responsables de la informació i del servei són els encarregats –comptant en el procés amb la participació i

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 documento de seguridad de la información recoge los ficheros afectados y los responsables correspondientes. 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 documento de seguridad.

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

l'assessorament del responsable de seguretat i del responsable del sistema–, de realitzar les preceptives anàlisis de riscos, i de seleccionar les salvaguardes que s'han d'implantar.

– Els responsables de la informació i del servei són els responsables dels riscos sobre la informació i els serveis, respectivament, i per tant, d'acceptar els riscos residuals calculats en l'anàlisi, i de realitzar el seu seguiment i control, sense perjudici de la possibilitat de delegar aquesta tasca.

– El procés de gestió de riscos –que comprèn les fases de categorització dels sistemes, anàlisi de riscos i selecció de mesures de seguretat que cal aplicar, les quals hauran de ser proporcionades als riscos i estar justificades–, s'ha de revisar cada any per part del responsable de seguretat, que elevarà un informe a la CIGSI.

11. DESENVOLUPAMENT NORMATIU DE LA POLÍTICA DE SEGURETAT

11.1. Cos normatiu

El cos normatiu sobre seguretat de la informació és d'obligat compliment i es desenvoluparà en quatre nivells segons l'àmbit d'aplicació i nivell de detall tècnic, de manera que cada norma d'un determinat nivell es fonamente en les normes de nivell superior. Aquests nivells de desenvolupament són els següents:

a) Primer nivell normatiu: Polítiques de seguretat de la informació. Constitueixen les directrius bàsiques per a la utilització de mitjans electrònics a la Sindicatura de Comptes i que es plasmen en la present norma. Seran aprovades o modificades pel Consell de la Sindicatura de Comptes a proposta de la CIGSI.

b) Segon nivell normatiu: Les normes de seguretat TIC de desenvolupament de les polítiques de seguretat de la informació, estableixen aquestes polítiques amb un major grau de detall dins d'un àmbit determinat. Donar resposta sense detalls d'implementació ni tecnològics, a què es pot fer i què no en relació amb un cert tema des del punt de vista de la seguretat. Seran aprovades o modificades pel Consell de la Sindicatura de Comptes a proposta de la CIGSI.

c) Tercer nivell normatiu: Procediments operatius i instruccions tècniques de seguretat de la informació. Són documents que responen a la forma en què es pot realitzar una determinada tasca respectant els principis de seguretat de l'organització i els processos interns establits, i poden incloure detalls d'implementació i tecnològics. El responsable de seguretat proposarà a la CIGSI els procediments i instruccions tècniques per aprovar-los.

d) Quart nivell normatiu. Guies i protocols de caràcter tècnic que recullen la forma de treballar en procediments concrets i/o amb determinades aplicacions. Les guies seran aprovades pels responsables funcionals dels procediments de gestió i, en concret, els protocols de treball de l'aplicació de gestió de les fiscalitzacions, els aprovarà el responsable del Gabinet Tècnic de la Sindicatura de Comptes.

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 nivell normatiu ha de respectar la legislació aplicable relacionada i el que prescriuen els nivells superiors en matèria de seguretat de la informació.

El responsable de seguretat i el de sistemes seran els encarregats de mantenir la documentació de seguretat actualitzada i organitzada i gestionar-hi els mecanismes d'accés.

11.2. Matèries objecte de desenvolupament normatiu

Els documents esmentats a l'apartat anterior hauran d'abordar, almenys, els següents aspectes:

– Condicions per a l'accés a la informació

– Ús de l'equipament informàtic i de comunicacions

– Gestió d'incidents i problemes

– Continuïtat d'operacions

– Seguretat amb tercers

– Classificació i tractament de la informació

– Anàlisi i gestió de riscos

– Seguretat física i del personal

– Prevenció de virus i codi maliciós

– Cicle de vida dels sistemes d'informació

– Millora contínua. Nivells de maduresa

– Elaboració, publicació i revisió de la política de seguretat de la informació i dels documents complementaris.

12. OBLIGACIONS DEL PERSONAL

Tots els membres de la Sindicatura de Comptes (síndics, secretari general i personal) tenen l'obligació de conèixer i complir la política i la normativa de seguretat de la informació, i és responsabilitat de la CIGSI disposar dels mitjans necessaris perquè la informació arribe als afectats.

Les polítiques de seguretat de la informació es publicaran en el *Butlletí Oficial de les Corts* i les normes de desplegament normatiu d'aquestes polítiques es comunicaran per correu electrònic a tots els membres de la Sindicatura (personal i alts càrrecs) quan siguen aprovades o modificades i estaran disponibles per als seus destinataris en la Intranet corporativa.

Tot el personal que s'incorpore a la Sindicatura de Comptes o que haja de tenir accés a algun dels seus sistemes d'informació o a la informació gestionada per mitjà d'aquests sistemes, serà informat de la política de seguretat i les seues normes de desenvolupament.

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.

11.2. 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 *Butlletí Oficial de les Corts* 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.

Els incompliments de les polítiques i normes de seguretat de la informació es tramitaran d'acord amb les previsions establides en la Llei de Sindicatura de Comptes i amb el procediment sancionador general aplicable als funcionaris públics previst en l'Estatut Bàsic de l'Empleat Públic.

13. TERCERES PARTS

Els contractes o convenis que subscriga la Sindicatura de Comptes a partir de l'entrada en vigor d'aquestes polítiques que consideren o requerisquen l'accés del personal a les instal·lacions o sistemes d'informació de la Sindicatura de Comptes, hauran d'incloure una clàusula de compliment d'aquesta política, juntament amb un procediment de verificació adequat. Els contractes i convenis signats amb anterioritat a aquesta data es revisaran en el mateix sentit. S'establiran amb aquestes empreses o entitats procediments d'actuació davant incidents de seguretat.

14. PROCÉS DE REVISIÓ DE LA POLÍTICA DE SEGURETAT

Les propostes de revisió de la política de seguretat les elaborarà la CIGSI i seran aprovades pel Consell de la Sindicatura de Comptes.

15. DISPOSICIÓ DEROGATÒRIA

Es deroga l'Acord de la Sindicatura de Comptes, de data 25 de febrer de 2009 pel qual es va aprovar el document de polítiques generals de gestió i seguretat dels sistemes d'informació de la Sindicatura de Comptes de la Comunitat Valenciana.

València, 23 de març de 2017
El síndic major
Vicent Cucarella Tormo

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 25 de febrero de 2009 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, 23 de marzo de 2017
El síndic major
Vicent Cucarella Tormo

BUTLLETÍ OFICIAL DE LES CORTS
Subscripcions: Servei de Publicacions de les Corts
<*subscripcions@corts.es*>
Plaça de Sant Llorenç, 4 • 46003 València
Telèfon: 96 387 61 00
<*http://www.cortsvalencianes.es*>
Edita: Servei de Publicacions de les Corts
ISSN: 1136-3339
Dipòsit legal: V-319-1983

CORTS VALENCIANES

BUTLLETÍ OFICIAL DE LES CORTS
Subscripciones: Servicio de Publicaciones de Les Corts
<*subscripcions@corts.es*>
Plaza de San Lorenzo, 4 • 46003 Valencia
Teléfono: 96 387 61 00
<*http://www.cortsvalencianes.es*>
Edita: Servicio de Publicaciones de Les Corts
ISSN: 1136-3339
Depósito legal: V-319-1983