Consorci Provincial de Bombers de València

Anunci del Consorci Provincial de Bombers de València sobre decret núm. 202000457 de la presidència-delegada, de 20 de maig de 2020, sobre aprovació de Política de Seguretat de la Informació del Consorci.

Anuncio del Consorcio Provincial de Bomberos de Valencia sobre decreto núm. 202000457 de la presidencia-delegada, de 20 de mayo de 20209, sobre aprobación de la Política de Seguridad de la Información del Consorcio.

ANUNCI

Maria Josep Amigó Laguarda, presidenta-delegada del Consorci per al Servei de Prevenció, Extinció d'Incendis i Salvament de la Província de València, en ús de les atribucions que tinc conferides, vinc a disposar.

La informació constitueix un actiu de primer ordre per al Consorci Provincial de Bombers de València des del moment en què resulta essencial per a la prestació dels seus serveis.

D'altra banda, les tecnologies de la informació i les comunicacions s'han fet imprescindibles també i cada vegada més per a les administracions públiques. No obstant això, les indiscutibles millores que aporten al tractament de la informació venen acompanyades de nous riscos i, per tant, és necessari introduir mesures específiques per a protegir tant la informació com els serveis que depenguen d'ella.

El marc normatiu de l'Administració electrònica que sorgeix a partir de la Llei 11/2007, de 22 de juny, d'accés electrònic dels ciutadans als serveis públics, considera la seguretat com un element fonamental per a la confiança en les relacions entre les administracions públiques i entre aquestes i els ciutadans, sent un dels seus pilars el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat (d'ara en avant *ENS) en l'àmbit de l'Administració Electrònica.

Les tendències tecnològiques actuals cap a l'accés en mobilitat, la virtualització i el paradigma de «núvol», i la necessitat de tractament d'ingents quantitats d'informació, fins i tot procedents de les pròpies xarxes socials, han portat, no sols a les organitzacions sinó també als Governs, a implicar-se en la política de seguretat als més alts nivells de decisió.

La Llei 39/2015, d'1 d'octubre, del Procediment Administratiu Comú de les Administracions Públiques, assenyala en el seu article 13.h) que els qui, de conformitat amb l'article 3, tenen capacitat d'obrar davant les Administracions Públiques, són titulars, en les seues relacions amb elles, del dret a la protecció de dades de caràcter personal i, en particular, a la seguretat i confidencialitat de les dades que figuren en els fitxers, sistemes i aplicacions de les Administracions Públiques.

Per la seua part la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, determina, en el seu article 3.2, que les Administracions Públiques es relacionaran entre si i amb els seus òrgans, organismes públics i entitats vinculats o dependents a través de mitjans electrònics, que asseguren la interoperabilitat i seguretat dels sistemes i solucions adoptades per cadascuna d'elles i garantiran la protecció de les dades de caràcter personal i facilitaran preferentment la prestació conjunta de serveis als interessats. L'articulació de les qüestions relatives a la seguretat de la informació a les quals fan esment les lleis referides, es du a terme en l'actualitat a través del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, modificat al seu torn pel Reial decret 951/2015, de 23 d'octubre, sent la seua finalitat la creació de les condicions de confiança en l'ús dels mitjans electrònics, que permeta als ciutadans i a les Administracions públiques, l'exercici de drets i el compliment de deures a través d'aquests mitjans.

Així mateix, han entrat en vigor, el Reglament (UE) 2016/679 del Parlament Europeu i del Consell de 27 d'abril de 2016 relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE (Reglament general de protecció de dades); la Llei orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals.

La Política de Seguretat de la Informació constitueix el marc de referència orientat a facilitar la definició, gestió, administració i implementació dels mecanismes i procediments de seguretat establits en el Reial decret 3/2010, de 8 de gener.

L'article 11 del citat Reial decret 3/2010, de 8 de gener, exigeix que tots els òrgans superiors de les Administracions públiques disposen formalment de la seua política de seguretat, que s'aprovarà pel titular de l'òrgan superior corresponent. Aquesta política de seguretat s'establirà amb base en els principis bàsics recollits en el capítol II de la pròpia norma (seguretat integral, gestió de riscos, prevenció, reacció i recuperació, línies de defensa, reavaluació periòdica, i funció diferenciada) i desenvoluparà una sèrie de requisits mínims consignats en el ja esmentat article 11.1.

El present Decret, per tant, té la finalitat d'aprovar la Política de Seguretat de la Informació del Consorci, així com establir l'estructura organitzativa per a definir-la, implantar-la i gestionar-la

Vist l'informe del responsable de la Unitat de Sistemes i Innovació tecnològica del 12 de març de 2020.

Vist l'informe del responsable de l'Assessoria Jurídica del 26 de març de 2020.

Vista la proposta de la Gerència, amb data de l'11 de maig de 2020, en sentit positiu.

Vist a l'annex la Política de Seguretat de la Informació, modificada en el sentit que indica l'Informe de l'Assessoria Juridica.

Per tot el que s'ha exposat, en compliment del que es disposa en l'article 11 del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica i en ús de les facultats que em confereix l'article 32 desl estatuts vigents i la delegació efectuada pel president del Consorci, per Decret núm. 604, de 25 de juliol de 2019 (article 31 Estatuts i 9.4 de la Llei 40/2015, d'1 d'octubre, de RJSP).

DISPOSE:

Primer: Aprovar la Política de Seguretat de la Informació del Consorci per al Servei de Prevenció Extinció d'Incendis i de Salvament de la Província de València, el text de la qual s'adjunta com a annex.

Segon: Publicar la present resolució i la Política de Seguretat de la Informació en el Butlletí Oficial de la Província, en el Portal de l'Empleat i en la pàgina Web el Consorci.

València, a 20 de maig de 2020.—El secretari general, Juan Jiménez Hernandis.—La presidenta-delegada, Maria Josep Amigó Laguarda.

ANUNCIO

Maria Josep Amigó Laguarda, presidenta-delegada del Consorcio para al Servicio de Prevención, Extinción de Incendios y Salvamento de la Provincia de Valencia, en uso de las atribuciones que tienen conferidas, vengo a disponer.

La información constituye un activo de primer orden para la Consorcio Provincial de Bomberos de Valencia desde el momento en que resulta esencial para la prestación de sus servicios. Por otro lado, las tecnologías de la información y las comunicaciones se han hecho imprescindibles también y cada vez más para las administraciones públicas. Sin embargo, las indiscutibles mejoras que aportan al tratamiento de la información vienen acompañadas de nuevos riesgos y, por lo tanto, es necesario introducir medidas específicas para proteger tanto la información como los servicios que dependan de ella.

El marco normativo de la Administración electrónica que surge a partir de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, considera la seguridad como un elemento fundamental para la confianza en las relaciones entre las administraciones públicas y entre éstas y los ciudadanos, siendo uno de sus pilares el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica.

Las tendencias tecnológicas actuales hacia el acceso en movilidad, la virtualización y el paradigma de «nube», y la necesidad de tratamiento de ingentes cantidades de información, incluso procedentes de las propias redes sociales, han llevado, no solo a las organizaciones sino también a los Gobiernos, a implicarse en la política de seguridad a los más altos niveles de decisión.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, señala en su artículo 13.h) que quienes, de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, del derecho a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por su parte la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, determina, en su artículo 3.2, que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. La articulación de las cuestiones relativas a la seguridad de la información a las que hacen mención las leyes referidas, se lleva a cabo en la actualidad a través del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, modificado a su vez por el Real Decreto 951/2015, de 23 de octubre, siendo su finalidad la creación de las condiciones de confianza en el uso de los medios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Asimismo, han entrado en vigor, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Real Decreto 3/2010, de 8 de enero.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1.

El presente Decreto, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información del Consorcio, así como establecer la estructura organizativa para definirla, implantarla y gestionarla

Visto el informe del responsable de la Unidad de Sistemas e Innovación tecnológica del 12 de marzo de 2020.

Visto el informe de la Asesoría Jurídica del 26 de marzo de 2020.

Vista la propuesta de la Gerencia, del 11 de mayo de 2020, con sentido positivo.

Visto en el anexo la Política de Seguridad de la Información, modificado en el sentido que indica el Informe de Asesoría Jurídica.

Por lo expuesto, en cumplimiento de lo dispuesto en el articulo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y en uso de las facultades que me confiere el artículo 32 de los estatutos vigentes y la delegación efectuada por el presidente del Consorcio, por Decreto núm. 604, de 25 de julio de 2019 (artículo 31 Estatutos y 9.4 de la Ley 40/2015, de 1 de octubre, de RJSP).

DISPONGO:

Primero: Aprobar la Política de Seguridad de la Información del Consorcio para el Servicio de Prevención Extinción de Incendios y de Salvamento de la Provincia de Valencia, cuyo texto se adjunta como anexo.

Segundo: Publicar la presente resolución y la Política de Seguridad de la Información en el Boletín Oficial de la Provincia, en el Portal del Empleado y en la pagina Web el Consorcio.

Valencia, a 20 de mayo de 2020.—El secretario general, Juan Jiménez Hernandis.—La presidenta-delegada, Maria Josep Amigó Laguarda.

ANNEX

POLÍTICA DE SEGURETAT DE LA INFORMACIÓ PER AL CONSORCI PROVINCIAL DE BOMBERS PER A L'EXTINCIÓ D'INCENDIS I SALVAMENT DE LA PROVINCIA DE VALÈNCIA

INTRODUCCIÓ

El Consorci per al Servei de Prevenció i Extinció d'Incendis de la província de València (d'ara endavant, el Consorci) utilitza sistemes automatitzats de tractament d'informació i de comunicacions per al compliment de les seues finalitats. Estos sistemes han de ser utilitzats i administrats amb diligència, i s'han de prendre les mesures adequades per a protegir-los enfront de danys accidentals o deliberats que puguen afectar la integritat o confidencialitat de la informació tractada o a la disponibilitat dels serveis.

L'objectiu de la present política de seguretat de la informació és establir els mecanismes bàsics que garantisquen la qualitat de la informació i la prestació continuada dels serveis mitjançant l'adopció d'accions preventives, la supervisió continuada de l'activitat i la resposta àgil als incidents que es puguen produir.

Les mesures mínimes de seguretat exigides pel Reial Decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració Electrònica, han d'aplicar-se i complir-se, i el personal del Consorci ha d'assumir que la seguretat de la informació és una part integral de la gestió quotidiana i dels sistemes que la suporten i que, en conseqüència, ha de prendre's en consideració des de la seua concepció i durant tot el seu cicle de vida. La protecció de la

ANEXO

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONSORCIO PROVINCIAL DE BOMBEROS PARA LA EXTINCIÓN DE INCENDIOS Y SALVAMENTO DE LA PROVINCIA DE VALENCIA

INTRODUCCIÓN

El Consorcio para el Servicio de Prevención y Extinción de Incendios de la provincia de Valencia (en adelante, el Consorcio) utiliza sistemas automatizados de tratamiento de información y de comunicaciones para el cumplimiento de sus fines. Estos sistemas deben ser utilizados y administrados con diligencia, y se deben tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la integridad o confidencialidad de la información tratada o a la disponibilidad de los servicios.

El objetivo de la presente política de seguridad de la información es el de establecer los mecanismos básicos que garanticen la calidad de la información y la prestación continuada de los servicios mediante la adopción de acciones preventivas, la supervisión continuada de la actividad y la respuesta ágil a los incidentes que se puedan producir.

Las medidas mínimas de seguridad exigidas por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, deben aplicarse y cumplirse, y el personal del Consorcio debe asumir que la seguridad de la información es una parte integral de la gestión cotidiana y de los sistemas que la soportan y que, en consecuencia, debe tomarse en consideración desde su concepción y durante todo su ciclo de

informació i la prevenció, resposta, reacció davant qualsevol incident i la recuperació dels sistemes han de formar part de les obligacions de tot el personal del Consorci als seus respectius àmbits de responsabilitat.

vida. La protección de la información y la prevención, respuesta, reacción ante cualquier incidente y la recuperación de los sistemas deben formar parte de las obligaciones de todo el personal de el Consorcio en sus respectivos ámbitos de responsabilidad.

Els requisits de seguretat i els recursos necessaris per a satisfer-los han de ser identificats i inclosos en la planificació dels sistemes i en els procediments de contractació de solucions tecnològiques que comporten tractament d'informació.

Los requisitos de seguridad y los recursos necesarios para satisfacerlos deben ser identificados e incluidos en la planificación de los sistemas y en los procedimientos de contratación de soluciones tecnológicas que comporten tratamiento de información.

Prevenció

El personal al servei del Consorci ha d'evitar, o almenys previndre, en tant que siga possible, que la informació o els serveis es vegen perjudicats per incidents de seguretat. Per això és necessari conéixer i observar les mesures mínimes de seguretat determinades per l'Esquema Nacional de Seguretat, així com establir els controls addicionals que resulten aconsellables després de dur a terme la corresponent avaluació d'amenaces i riscos. Aquests controls, i els rols i responsabilitats de seguretat de tot el personal, han d'estar clarament definits i documentats.

Prevención

El personal al servicio del Consorcio debe evitar, o al menos prevenir, en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello es necesario conocer y observar las medidas mínimas de seguridad determinadas por el Esquema Nacional de Seguridad, así como establecer los controles adicionales que resulten aconsejables después de llevar a cabo la correspondiente evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Per a garantir el compliment d'Esta política, el personal ha de recaptar les autoritzacions oportunes per a la posada en producció de qualsevol sistema, avaluar regularment la seguretat, dur a terme revisions dels canvis de configuració realitzats de manera rutinària i sol·licitar la revisió periòdica per part de tercers amb la finalitat d'obtindre una avaluació independent de l'estat de la seguretat.

Para garantizar el cumplimiento de esta política, el personal debe recabar las autorizaciones oportunas para la puesta en producción de cualquier sistema, evaluar regularmente la seguridad, llevar a cabo revisiones de los cambios de configuración realizados de forma rutinaria y solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente del estado de la seguridad.

Detecció

L'estat dels serveis basats en l'ús de tecnologies de la informació i de les

Detección

El estado de los servicios basados en el uso de tecnologías de la información y de las

comunicacions (d'ara en davant, serveis TIC) ha de ser monitoritzat de manera contínua amb la finalitat de detectar anomalies en els seus nivells de qualitat, segons el que s'estableix en l'article 9 de l'Esquema Nacional de Seguretat.

És necessari establir mecanismes de detecció i anàlisi d'incidents relacionats amb la seguretat de la informació, així com canals que permeten la seua supervisió per part de la direcció, de manera regular i, especialment, quan es produïsca una desviació significativa dels paràmetres que s'hagen preestablit com a normals.

Resposta

El Consorci ha de dotar-se de mecarismes per garantir una resposta adecuada enfront de qualsevol situació d'anomalia o incident de seguretat detectat. Per això, desenvoluparà mecanismes adequats per a la notificació dels incidents i l'intercanvi d'informació relacionada amb els equips de resposta a incidents en l'àmbit autonòmic (CSIRT-GV[1]) i estatal (CCN-CERT[2]).

Recuperació

comunicaciones (en adelante, servicios TIC) debe ser monitorizado de manera continua con el fin de detectar anomalías en sus niveles de calidad, según lo establecido en el artículo 9 del Esquema Nacional de Seguridad.

Es necesario establecer mecanismos de detección y análisis de incidentes relacionados con la seguridad de la información, así como canales que permitan su supervisión por parte de la dirección, de forma regular y, especialmente, cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Respuesta

El Consorcio debe dotarse de mecanismos para garantizar una respuesta adecuada ante cualquier situación anómala o incidente de seguridad detectado. Para ello, desarrollará mecanismos adecuados para la notificación de los incidentes y el intercambio de información relacionada con los equipos de respuesta a incidentes de ámbito autonómico (CSIRT-GV[3]) y estatal (CCN-CERT[4]).

Recuperación

1 CSIRT-CV (https://www.csirtcv.gva.es/) és el Centre de Seguretat TIC de la Comunitat Valenciana. Actualment CSIRT-CV està adscrit a la Direcció General de Tecnologies de la Informació i les Comunicacions dins de la Conselleria d'Hisenda i Model Econòmic.

2 El Centre Criptològic Nacional (CCN, https://www.ccn-cert.cni.es) és l'Organisme responsable de coordinar l'acció dels diferents organismes de l'Administració que utilitzen medis o procedimients de xifra, de garantir la seguretat de las Tecnologies de la Informació en aquest àmbit, d'informar sobre l'adquisició coordinada del material criptològic i de formar al personal de l'Administració especialista en aquest camp. El CCN fou creat a l'any 2004, a través del Reial Decret 421/2004, adscribint-se al Centre Nacional d'Inteligència (CNI).

3 CSIRT-CV (https://www.csirtcv.gva.es/) es el Centro de Seguridad TIC de la Comunitat Valenciana. Actualmente CSIRT-CV está adscrito a la Dirección General de Tecnologías de la Información y las Comunicaciones dentro de la Conselleria de Hacienda y Modelo Económico.

4 El Centro Criptológico Nacional (CCN, https://www.ccn-cert.cni.es) es el Organismo responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, de garantizar la seguridad de las Tecnologías de la Información en ese ámbito, de informar sobre la adquisición coordinada del material criptológico y de formar al personal de la Administración especialista en este campo. El CCN fue creado en el año 2004, a través del Real Decreto 421/2004, quedando adscrito al Centro Nacional de Inteligencia (CNI).

Per tal de garantir la disponibilitat dels serveis crítics, el Consorci haurà de desenvolupar plans de continuitat i de recuperació dels sistemes TIC, com part del seu pla general de continuitat del servei. Estos plans han d'estar permanentment actualitzats i la seua eficàcia ha de ser verificada mitjançant proves periòdiques.

Para garantizar la disponibilidad de los servicios críticos, el Consorcio debe desarrollar planes de continuidad y de recuperación de los sistemas TIC, como parte de su plan general de continuidad del servicio. Estos planes deben estar permanentemente actualizados y su eficacia debe ser verificada mediante pruebas periódicas.

ÀMBIT

Esta política és d'aplicació a tots els sistemes TIC del Consorci i a tot el personal. Als contractes que es suscribeixen amb tercers, s'establirà l'obligació de complir amb esta politica per part del contractista i del seu personal, si la mateixa fora d'aplicació.

ALCANCE

Esta política es de aplicación a todos los sistemas TIC del Consorcio y a todo su personal. En los contratos que se suscriban con terceros, se establecerá la obligación de cumplir con esta política por parte del contratista y de su personal, si la misma fuera de aplicación.

MISIÓ

El Consorci es crea per a la prestació dels serveis de prevenció i extinció d'incendis i salvament al seu àmbit territorial, d'acord amb l'article 7 dels vigents estatuts.

MISIÓN

El Consorcio se crea para la prestación de los servicios de Prevención y Extinción de Incendios y Salvamento en su ámbito territorial, de acuerdo al artículo 7 de los vigentes Estatutos.

Tant per al compliment dels seus fins específics, com per al seu funcionament com entitat de dret públic, el Consorci fa ús d'informació i de sistemes automatitzats per al seu tractament, que han de ser convincentment protegits, supervisats i auditats.

Tanto para el cumplimiento de sus fines específicos, como para su funcionamiento como entidad de derecho público, el Consorcio hace uso de información y de sistemas automatizados para su tratamiento, que deben ser convenientemente protegidos, supervisados y auditados.

MARC NORMATIU

A l'apartat corresponent del Sistema de Gestió de la Seguretat de la Informació, es mantindrà un llistat de disposicions normatives a les que està subjecta el Consorci i que guarden, en major o menor mesura, relació amb la seguretat de la informació.

El menat llistat es mantindrà actualitzat i serà objecte de revisió anual per part de la persona Responsable de l'Assessoria Jurídica del Consorci.

MARCO NORMATIVO

En el apartado correspondiente del Sistema de Gestión de la Seguridad de la Información, se mantendrá un listado de disposiciones normativas a las que está sujeta el Consorcio y que guardan, en mayor o menor medida, relación con la seguridad de la información.

El mencionado listado se mantendrá actualizado y será objeto de revisión anual por parte de la persona Responsable de Asesoría Jurídica del Consorcio.

DESENVOLUPAMENT DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

Per al desenvolupament de la present Política, el Consorci es dotarà d'una sèrie d'instruments que permeten abordar els diferents aspectes de la seguretat de la informació. Amb això es tracta de donar concreció a la concepció abstracta de la seguretat que suposa la política i portar-la al terreny de la seua aplicació pràctica. Estos elements són els que es relacionen a continuació.

Anàlisi de riscos

L'article 6 del Reial Decret 3/2010. de 8 de gener, el qual regula l'Esquema Nacional de Seguretat, estableix que l'anàlisi i la gestió dels riscos són parts essencials del procés de seguretat i han de mantindre's permanentment actualitzats. La gestió de riscos ha de permetre el manteniment d'un entorn controlat, que minimitze el risc fins a un nivell acceptable i que involucre a la direcció de les diferents unitats administratives del Consorci en l'acceptació d'un determinat risc residual.

L'anàlisi i la gestió dels riscos es duran a terme mitjançant eines i metodologies comunament acceptades per les administracions públiques i prenent com a referència les guies i directrius que publiquen el CCN-CERT o el CSIRT-CV.

Tots els sistemes subjectes a aquesta Política hauran de realitzar una anàlisi de riscos, avaluant les amenaces i els riscos als quals estan exposats. Esta anàlisi es repetirà:

- Regularment, almenys una vegada a l'any.
- Excepcionalment:
  - Quan canvie significativament la informació tractada, el que fa referència a aquesta informació

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Para el desarrollo de la presente Política, el Consorcio se dotará de una serie de instrumentos que permitan abordar los diferentes aspectos de la seguridad de la información. Con ello se trata de dar concreción a la concepción abstracta de la seguridad que supone la política y llevarla al terreno de su aplicación práctica. Estos elementos son los que se relacionan a continuación.

Análisis de riesgos

El artículo 6 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, establece que el análisis y la gestión de los riesgos son partes esenciales del proceso de seguridad y deben mantenerse permanentemente actualizados. La gestión de riesgos debe permitir el mantenimiento de un entorno controlado, que minimice el riesgo hasta un nivel aceptable y que involucre a la dirección de las diferentes unidades administrativas del Consorcio en la aceptación de un determinado riesgo residual.

El análisis y la gestión de los riegos se llevarán a cabo mediante herramientas y metodologías comúnmente aceptadas por las administraciones públicas y tomando como referencia las guías y directrices que publiquen el CCN-CERT o el CSIRT-CV.

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Excepcionalmente:
  - Cuando cambie significativamente la información manejada, en lo que haga referencia a esa información.

- Quan canvien significativament els serveis prestats, el que afecte als sistemes nous o modificats.
- Quan es produixca un incident greu de seguretat.

- Quan es reporten vulnerabilitats greus.

- Cuando cambien significativamente los servicios prestados, en lo que afecte a los sistemas nuevos o modificados.
- Cuando ocurra un incidente grave de seguridad.

- Cuando se reporten vulnerabilidades graves.

L'anàlisi i la gestió han d'estar presents en totes les fases del cicle de vida dels sistemes. La selecció i l'aplicació dels controls de seguretat, així com l'avaluació de la seua eficàcia, han de prendre's en consideració durant el disseny, implantació, contractació, adquisició i explotació dels sistemes i serveis del Consorci, sent objecte d'especial atenció la finalització dels mateixos i la destinació de la informació que tracten.

El análisis y la gestión de riesgos deben estar presentes en todas las fases del ciclo de vida de los sistemas. La selección y la aplicación de los controles de seguridad, así como la evaluación de su eficiencia, deben tomarse en consideración durante el diseño, implantación, contratación, adquisición y explotación de los sistemas y servicios del Consorcio, siendo objeto de especial atención la finalización de los mismos y el destino de la información que traten.

El Consorci valora especialment, als processos de contractació, les empreses, productes i serveis que puguen acreditar un determinat nivell de seguretat o que disposen de les certificacions de seguretat pertinents, d'acord amb la normativa d'aplicació.

El Consorcio valorará especialmente, en los procesos de contratación, las empresas, productos y servicios que puedan acreditar un determinado nivel de seguridad o que dispongan de las certificaciones de seguridad pertinentes, de acuerdo a la normativa de aplicación.

Classificació de la informació

Els actius d'informació que tracte el Consorci han d'estar inventariats, i classificats. El nivell de protecció i les mesures de seguretat que s'aplicaran a la informació han de basar-se en la seua classificació i els mecanismes i criteris per a dur-la a terme han de ser formalment aprovats i coneguts per tot el personal.

Clasificación de la información

Los activos de información que trate el Consorcio deben estar inventariados y clasificados. El nivel de protección y las medidas de seguridad que se aplicarán a la información deben basarse en su clasificación y los mecanismos y criterios para llevarla a cabo deben ser formalmente aprobados y conocidos por todo el personal.

Planificació i coordinació

Amb caràcter anual, el Consorci definirà un conjunt d'objectius de seguretat que han d'incloure una descripció de la línia o línies d'actuació previstes, els projectes que els

Planificación y coordinación

Con carácter anual, el Consorcio definirá un conjunto de objetivos de seguridad que deben incluir una descripción de la línea o líneas de actuación previstas, los proyectos en los que se

concreten, els objectius a aconseguir i els indicadors de compliment i el procés corresponent. Aquests objectius han de prendre en consideració els resultats de les auditories i de l'anàlisi de riscos.

L'esquema organitzatiu de la seguretat de la informació inclou els òrgans de coordinació i decisió necessaris per a l'aplicació i control de les mesures de seguretat.

Accés a la informació

El personal que tracte la informació a través dels sistemes del Consorci ha d'estar degudament acreditat i identificat mitjançant credencials electròniques personals i intransferibles.

Els privilegis d'accés a la informació han de limitar-se als estrictament imprescindibles per al desenvolupament de les funcions de cada lloc de treball.

Registres d'activitats

Les actuacions del personal sobre els sistemes podran ser registrades en aplicació de les exigències legals de traçabilitat o amb la finalitat de verificar el compliment d'aquesta política. Aquest registre comportarà la retenció d'informació per al seu monitoratge, anàlisi, investigació i documentació.

Els accessos a la informació que impliquen modificacions d'aquesta o que suposen l'accés a dades especialment sensibles han de quedar registrats amb el nivell de detall suficient per a garantir el compliment normatiu i la traçabilitat de les accions efectuades.

Ús dels sistemes i mitjans electrònics

Amb caràcter general, el Consorci no permet la utilització dels mitjans electrònics corporatius

concretan, los objetivos a alcanzar y los indicadores de cumplimiento y progreso correspondientes. Estos objetivos deben tomar en consideración los resultados de las auditorías y del análisis de riesgos.

El esquema organizativo de la seguridad de la información incluye los órganos de coordinación y decisión necesarios para la aplicación y control de las medidas de seguridad.

Acceso a la información

El personal que trate información a través de los sistemas del Consorcio debe estar debidamente acreditado e identificado mediante credenciales electrónicas personales e intransferibles.

Los privilegios de acceso a la información deben limitarse a los estrictamente imprescindibles para el desarrollo de las funciones de cada puesto de trabajo.

Registros de actividad

Las actuaciones del personal sobre los sistemas podrán ser registradas en aplicación de las exigencias legales de trazabilidad o con el fin de verificar el cumplimiento de esta política. Ese registro conllevará la retención de información para su monitorización, análisis, investigación y documentación.

Los accesos a la información que implican modificaciones de ésta o que suponen el acceso a datos especialmente sensibles deben quedar registrados con el nivel de detalle suficiente para garantizar el cumplimiento normativo y la trazabilidad de las acciones efectuadas.

Uso de los sistemas y medios electrónicos

Con carácter general, el Consorcio no permite la utilización de los medios electrónicos

per a ús personal. Aquesta prohibició no serà aplicable en aquells casos en els quals el servei siga dissenyat específicament amb la finalitat de permetre l'ús de dispositius personals o en aquells altres en els quals l'ús personal del servei siga autoritzat de manera explícita. Aquesta autorització únicament podrà concedir-se si el servei afectat no permet el tractament d'informació sensible del Consorci.

corporativos para uso personal. Esta prohibición no será de aplicación en aquellos casos en los que el servicio sea diseñado específicamente con el fin de permitir el uso de dispositivos personales o en aquellos otros en los que el uso personal del servicio sea autorizado de forma explícita. Esta autorización únicamente podrá concederse si el servicio afectado no permite el tratamiento de información sensible de el Consorcio.

Confidencialitat i deure de secret

Aquelles persones al servei del Consorci que tracten informació que no tinga el caràcter de pública han d'observar la necessària reserva, confidencialitat i sigil. Aquesta obligació perdura després d'haver finalitzat el vincle amb el Consorci.

Confidencialidad y deber de secreto

Aquellas personas al servicio del Consorcio que traten información que no tenga el carácter de pública han de observar la necesaria reserva, confidencialidad y sigilo. Esta obligación perdura después de haber finalizado el vínculo con el Consorcio.

Aquest compromís ha de fer-se constar, de manera individual i per escrit, mitjançant una declaració responsable de confidencialitat.

Este compromiso debe hacerse constar, de forma individual y por escrito, mediante una declaración responsable de confidencialidad.

Instal·lacions i equipament

Els sistemes i les infraestructures informàtiques i de comunicacions que no formen part dels llocs de treball han de situar-se en zones aïllades, d'accés restringit i suficientment protegides.

Instalaciones y equipamiento

Los sistemas y las infraestructuras informáticas y de comunicaciones que no formen parte de los puestos de trabajo deben ubicarse en zonas aisladas, de acceso restringido y suficientemente protegidas.

Sistemes d'informació

Els sistemes d'informació del Consorci han de proporcionar la funcionalitat estrictament necessària per tal d'acomplir la finalitat que haja motivat el seu disseny o adquisició. Aquesta finalitat ha d'estar documentada i formalment aprovada pels seus responsables.

Sistemas de información

Los sistemas de información del Consorcio deben proporcionar la funcionalidad estrictamente necesaria para cumplir la finalidad que haya motivado su diseño o adquisición. Esta finalidad debe estar documentada y formalmente aprobada por sus responsables.

Els responsables de les diferents unitats administratives del Consorci són responsables dels sistemes d'informació que donen suport als processos que desenvolupen. En el cas de sistemes comuns, aquesta responsabilitat l'exercirà la Gerència.

Los responsables de las distintas unidades administrativas del Consorcio son responsables de los sistemas de información que dan soporte a los procesos que desarrollan. En el caso de sistemas comunes, esta responsabilidad la ejercerá la Gerencia.

Les funcions d'operació, administració, manteniment i registre d'activitat han d'estar documentades i subjectes a control.

Protecció de la informació no automatitzada

La informació del Consorci en suport no electrònic ha de ser protegida amb el mateix nivell de seguretat que la que haja sigut sotmesa a tractament automatitzat.

Els documents hauran d'emmagatzemar-se en una ubicació adequada, evitant la seua proximitat a sistemes de refrigeració, canalitzacions d'aigua o instal·lacions que puguen afectar el paper.

Es guardaran en els armaris o calaixeres i s'evitarà l'acumulació de documents sobre les taules que puga causar pèrdues o filtracions d'informació.

La documentació rebutjada ha de destruir-se de manera segura. En el cas que el volum de documentació a destruir siga elevat, pot resultar aconsellable contractar la retirada i destrucció a un proveïdor extern. En aquest cas, els contractes establiran les clàusules de confidencialitat pertinents i l'obligació de proporcionar certificats de destrucció segura.

Sistema de Gestió de la Seguretat de la Informació

La planificació, organització i control dels recursos relatius a la seguretat de la informació requereix ser abordada de manera sistemàtica i documentada. El conjunt de procediments, normes i guies de seguretat que es desenvolupen haurà de ser integrat en un Sistema de Gestió de la Seguretat de la Informació (d'ara en endavant, SGSI), que siga periòdicament revisat, verificat mitjançant

Las funciones de operación, administración, mantenimiento y registro de actividad deben estar documentadas y sujetas a control.

Protección de la información no automatizada

La información de el Consorcio en soporte no electrónico debe ser protegida con el mismo nivel de seguridad que la que haya sido sometida a tratamiento automatizado.

Los documentos deberán almacenarse en una ubicación adecuada, evitando su cercanía a sistemas de refrigeración, canalizaciones de agua o instalaciones que puedan afectar al papel.

Se guardarán en los armarios o cajoneras y se evitará la acumulación de documentos sobre las mesas que pueda causar pérdidas o filtraciones de información.

La documentación desechada debe destruirse de manera segura. En el caso de que el volumen de documentación a destruir sea elevado, puede resultar aconsejable contratar la retirada y destrucción a un proveedor externo. En este caso, los contratos establecerán las cláusulas de confidencialidad pertinentes y la obligación de proporcionar certificados de destrucción segura.

Sistema de Gestión de la Seguridad de la Información

La planificación, organización y control de los recursos relativos a la seguridad de la información requiere ser abordada de forma sistemática y documentada. El conjunto de procedimientos, normas y guías de seguridad que se desarrollen deberá ser integrado en un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI), que sea periódicamente revisado, verificado mediante

auditories i adaptat a les necessitats del Consorci i als requisits legals vigents a cada moment.

El SGSI del Consorci estarà orientat a acomplir el que es preveu en l'Esquema Nacional de Seguretat i inclourà els documents següents:

- Declaració d'aplicabilitat de les mesures previstes a l'Annex II de l'Esquema Nacional de Seguretat.
- Llistat d'actius d'informació i sistemes amb la seua valoració corresponent en funció de les diferents dimensions de seguretat.
- Procediments de seguretat, amb indicacions concretes sobre la forma de tractar la informació i d'actuar sobre els sistemes, i que han de descriure com acomplir el que hi ha previst a l'Esquema Nacional de Seguretat.
- Normes de seguretat, que regularan l'ús correcte i les responsabilitats dels usuaris i que tindran caràcter d'obligatori.

El sistema de gestió de la seguretat de la informació ha d'estar sotmés a monitorització, control i millora continua per mantindre's la seua eficàcia enfront de la constant evolució de les amenaces i dels sistemes tècnics de protecció.

Guies de seguretat

Les guies de seguretat han de tindre caràcter formatiu i estaran orientades a instruir i orientar als usuaris en la correcta aplicació de les mesures de seguretat per a les que no existisquen procediments concrets. Les esmentades guies de seguretat es posaran a disposició del personal de manera que resulte senzill el seu accés i es promoga el seu

auditorías y adaptado a las necesidades de el Consorcio y a los requisitos legales vigentes en cada momento.

El SGSI del Consorcio estará orientado a dar cumplimiento a lo previsto en el Esquema Nacional de Seguridad e incluirá los documentos siguientes:

- Declaración de aplicabilidad de las medidas previstas en el Anexo II del Esquema Nacional de Seguridad.
- Lista de activos de información y sistemas con su valoración correspondiente en función de las diferentes dimensiones de la seguridad.
- Procedimientos de seguridad, con indicaciones concretas sobre la forma de manejar la información y de actuar sobre los sistemas, y que deben describir cómo dar cumplimiento a lo previsto en el Esquema Nacional de Seguridad.
- Normas de seguridad, que regularán el uso correcto y las responsabilidades de los usuarios y que tendrán carácter obligatorio.

El sistema de gestión de la seguridad de la información debe estar sometido a monitorización, control y mejora continuos para mantener su eficacia ante la constante evolución de las amenazas y de los sistemas técnicos de protección.

Guías de seguridad

Las guías de seguridad deben tener un carácter formativo y estarán orientadas a instruir y orientar a los usuarios en la correcta aplicación de las medidas de seguridad para las que no existan procedimientos concretos. Dichas guías de seguridad se podrán a disposición del personal de modo que resulte sencillo su acceso y se promueva su conocimiento y

coneixement i aplicació, tant si són d'origen intern, com si han sigut elaborades per organismes externs al Consorci.

Especials requisits de seguretat dels actius del Consorci

El Consorci, per al compliment de les seues finalitats, tracta informacions diverses i compta amb sistemes per a dur a terme aquests tractaments. Els actius d'informació i els sistemes constitueixen l'objecte de protecció d'aquesta política, havent d'aplicar-se les mesures que corresponga en funció de la seua criticitat i del que estiga previst a cada moment en la normativa vigent.

La seguretat de la informació s'aborda des de cinc dimensions diferents:

- La **confidencialitat**, que pren en consideració les conseqüències que tindria la revelació d'informació a persones no autoritzades o que no necessiten conéixer-la.
- La **integritat**, que considera l'impacte que podria tindre la modificació malintencionada o involuntària de la informació.
- L'**autenticitat**, que valora les conseqüències derivades que la informació no fora autèntica.
- La **traçabilitat**, que es planteja els problemes que suposaria el fet de no poder verificar els accessos o modificacions duts a terme sobre una certa informació.
- La **disponibilitat**, que considera les conseqüències que tindria per a la que una persona o un sistema interconnectat no puguera accedir a un sistema dins del període de servei establit i anunciat pel Consorci.

aplicación, tanto si son de origen interno, como si han sido elaboradas por organismos externos al Consorcio.

Especiales requisitos de seguridad de los activos del Consorcio

El Consorcio, para el cumplimiento de sus fines, trata informaciones diversas y cuenta con sistemas para llevar a cabo esos tratamientos. Los activos de información y los sistemas constituyen el objeto de protección de esta política, debiendo aplicarse las medidas que corresponda en función de su criticidad y de lo que se prevea en cada momento en la normativa vigente.

La seguridad de la información se aborda desde cinco dimensiones diferentes:

- La **confidencialidad**, que toma en consideración las consecuencias que tendría la revelación de información a personas no autorizadas o que no necesitan conocerla.
- La **integridad**, que considera el impacto que podría tener la modificación malintencionada o involuntaria de la información.
- La **autenticidad**, que valora las consecuencias derivadas de que la información no fuera auténtica.
- La **trazabilidad**, que se plantea los problemas que supondría el hecho de no poder verificar los accesos o modificaciones llevados a cabo sobre una cierta información.
- La **disponibilidad**, que considera las consecuencias que tendría para la que una persona o un sistema interconectado no pudiera acceder a un sistema dentro del periodo de servicio establecido y anunciado por el Consorcio.

Amb caràcter general, el Consorci valorarà, conforme als criteris establits en l'Esquema Nacional de Seguretat, la disponibilitat dels sistemes i la integritat, confidencialitat, autenticitat i traçabilitat de la informació.

Con carácter general, el Consorcio valorará, conforme a los criterios establecidos en el Esquema Nacional de Seguridad, la disponibilidad de los sistemas y la integridad, confidencialidad, autenticidad y trazabilidad de la información.

ORGANITZACIÓ DE LA SEGURETAT

L'Esquema Nacional de Seguretat preveu que en els sistemes d'informació de les administracions públiques existisquen tres rols diferenciats:

- El responsable de la informació (RINFO), que determinarà els requisits de la informació tractada.
- El responsable del servei (RSERV), que determinarà els requisits dels serveis prestats.
- El responsable de seguretat (RSEG), que prendrà les decisions per a satisfer els requisits de seguretat de la informació i dels serveis.

ORGANIZACIÓN DE LA SEGURIDAD

El Esquema Nacional de Seguridad prevé que en los sistemas de información de las administraciones públicas existan tres roles diferenciados:

- El responsable de la información (RINFO), que determinará los requisitos de la información tratada.
- El responsable del servicio (RSERV), que determinará los requisitos de los servicios prestados.
- El responsable de seguridad (RSEG), que tomará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilitat de la seguretat dels sistemes d'informació ha d'estar diferenciada de la responsabilitat sobre la prestació dels serveis i la Política de Seguretat de la Informació del Consorci és la que ha de detallar les atribucions de cada responsable i els mecanismes de coordinació i de resolució de conflictes.

La responsabilidad de la seguridad de los sistemas de información debe estar diferenciada de la responsabilidad sobre la prestación de los servicios y la Política de Seguridad de la Información del Consorcio es la que debe detallar las atribuciones de cada responsable y los mecanismos de coordinación y de resolución de conflictos.

Malgrat això, i per l'estructura organitzativa i de plantilla d'aquest Consorci, en aquesta Política s'opta per aglutinar els tres rols, RINFO, RSERV i RSEG en el Comité de Seguretat de la Informació, on s'hauran de resoldre els hipotètics conflictes d'interessos que pugueren sorgir.

Pese a ello, y por la estructura organizativa y de plantilla de este Consorcio, en esta Política se opta por aglutinar los tres roles, RINFO, RSERV y RSEG en el Comité de Seguridad de la Información, donde se deberán resolver los hipotéticos conflictos de intereses que pudieran surgir.

Funcions i responsabilitat de la Presidència

Són funcions de la Presidència del Consorci, en relació amb la seguretat de la informació, les

Funciones y responsabilidades de la Presidencia

Son funciones de la Presidencia del Consorcio, en relación con la seguridad de la información,

següents:

a) Assumir la responsabilitat última de l'ús que es realitze de la informació, així com de la disponibilitat, accessibilitat i interoperabilitat dels serveis.
b) Assumir la responsabilitat última de qualsevol error o negligència que porte a un incident de confidencialitat o d'integritat de la informació, o bé de disponibilitat del servei.
c) Designar a les persones integrants del Comité de Seguretat de la Informació, així com a les persones que exerciran les funcions de responsable del sistema (RSIS) i administrador de seguretat (AS), en nomenclatura de l'Esquema Nacional de Seguretat.
d) Determinar, a proposta del Comité de Seguretat de la Informació, els nivells de seguretat de la informació i la categoria dels serveis.
e) Amb l'assistència del Comité de Seguretat de la Informació i de les persones administradores de la seguretat, mantindre la seguretat de la informació tractada pel Consorci i dels serveis prestats pels sistemes d'informació, així com promoure la formació i conscienciació del personal al servei del Consorci en matèria de seguretat de la informació.

Funcions de la persona responsable del sistema

La funció de responsable del sistema (RSIS) l'exercirà la persona que siga designada per la Presidència del Consorci amb aquest efecte. El responsable del sistema podrà delegar determinades funcions en els administradors de seguretat (AS). Aquestes delegacions, que es faran en funció de criteris tècnics, s'han de fer constar en els procediments del Sistema de Gestió de la Seguretat de la Informació.

las siguientes:

a) Asumir la responsabilidad última del uso que se haga de la información, así como de la disponibilidad, accesibilidad e interoperabilidad de los servicios.
b) Asumir la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información, o bien de disponibilidad del servicio.
c) Nombrar a las personas integrantes del Comité de Seguridad de la Información, así como a las personas que ejercerán las funciones de responsable del sistema (RSIS) y administrador de seguridad (AS), en nomencaltura del Esquema Nacional de Seguridad.
d) Determinar, a propuesta del Comité de Seguridad de la Información, los niveles de seguridad de la información y la categoría de los servicios.
e) Con la asistencia del Comité de Seguridad de la Información y de las personas administradoras de la seguridad, mantener la seguridad de la información manejada por el Consorcio y de los servicios prestados por los sistemas de información, así como promover la formación y concienciación del personal al servicio del Consorcio en materia de seguridad de la información.

Funciones de la persona responsable del sistema

La función de responsable del sistema (RSIS) la ejercerá la persona que sea designada por la Presidencia del Consorcio a tal efecto. El responsable del sistema podrá delegar determinadas funciones en los administradores de seguridad (AS). Estas delegaciones, que se harán en función de criterios técnicos, se deben hacer constar en los procedimientos del Sistema de Gestión de la Seguridad de la Información.

Les funcions del responsable del sistema són les següents:

a) Informar i rendir comptes a la Presidència i al Comité de Seguretat de la Informació en matèria de seguretat dels sistemes i equips del Consorci.
b) Valorar els resultats de l'anàlisi de riscos i proposar la presa de decisions sobre la manera de tractar-los.
c) Assumir la responsabilitat tècnica sobre la prestació dels serveis basats en els sistemes de la informació del Consorci.
d) Supervisar el desenvolupament, operació i manteniment dels sistemes durant tot el seu cicle de vida.
e) Definir els principis de gestió de cada sistema i establir les polítiques d'ús i els serveis disponibles.
f) Assegurar-se que les mesures generals i polítiques de seguretat estan integrades en els sistemes.
g) Prendre decisions urgents en matèria de suspensió o interrupció temporal del servei, si es detecten deficiències greus de seguretat.
h) Vetlar per l'elaboració dels procediments operatius de seguretat.
i) Proposar plans i objectius de millora de la seguretat.
j) Promoure la formació del personal a càrrec seu en matèria de seguretat.
k) Elaborar plans de continuïtat que garantisquen la prestació del servei en cas d'incidències.
l) Gestionar els acords de nivell de servei.
m) Vetlar per la seguretat física de les instal·lacions en les quals se situen els sistemes de tractament d'informació, i de la gestió del personal a càrrec seu.

Las funciones del responsable del sistema son las siguientes:

a) Informar y rendir cuentas a la Presidencia y al Comité de Seguridad de la Información en materia de seguridad de los sistemas y equipos del Consorcio.
b) Valorar los resultados del análisis de riesgos y proponer la toma de decisiones sobre la manera de tratarlos.
c) Asumir la responsabilidad técnica sobre la prestación de los servicios basados en los sistemas de la información del Consorcio.
d) Supervisar el desarrollo, operación y mantenimiento de los sistemas durante todo su ciclo de vida.
e) Definir los principios de gestión de cada sistema y establecer las políticas de uso y los servicios disponibles.
f) Asegurarse de que las medidas generales y políticas de seguridad están integradas en los sistemas.
g) Tomar decisiones urgentes en materia de suspensión o interrupción temporal del servicio, si se detectan deficiencias graves de seguridad.
h) Velar por la elaboración de los procedimientos operativos de seguridad.
i) Proponer planes y objetivos de mejora de la seguridad.
j) Promover la formación del personal a su cargo en materia de seguridad.
k) Elaborar planes de continuidad que garanticen la prestación del servicio en caso de incidencias.
l) Gestionar los acuerdos de nivel de servicio.
m) Velar por la seguridad física de las instalaciones en las que se ubiquen los sistemas de tratamiento de información, y de la gestión del personal a su cargo.

Funcions i responsabilitats de la/es persona/es encarregada/es de l'administració de seguretat

Le(s) persone(s) encarregade(s) de l'administració de la seguretat dels sistemes (AS) serà(n) designade(s) per la Presidència del Consorci a proposta del responsable del sistema, i tindrà(n) encomanades les funcions de seguretat orientades a l'assegurament de la prestació del servei i els mitjans de tractament de la informació. Aquestes funcions es concreten en les següents:

a) Assumir, sota la supervisió del responsable del sistema, la responsabilitat del disseny, implantació i control de les mesures tècniques de seguretat en cada sistema i aplicar els procediments operatius.
b) Dur a terme la gestió, configuració i actualització del *hardware* i *software* en el qual es basen els mecanismes de seguretat dels sistemes.
c) Gestionar les autoritzacions d'ús i perfils d'accés als sistemes.
d) Elaborar els plans de recuperació de sistemes.
e) Monitoritzar contínuament l'estat de seguretat dels sistemes.
f) Registrar els incidents de seguretat.
g) Informar, periòdicament o a sol·licitud d'aquest, al Comité de Seguretat de la Informació.
h) Exercir les funcions delegades pel responsable del sistema en el seu àmbit de competència.
i) Col·laborar en la resolució i investigació d'incidents de seguretat.

Funciones y responsabilidades de la(s) persona(s) encargada(s) de la administración de seguridad

La(s) persona(s) encargada(s) de la administración de la seguridad de los sistemas (AS) será(n) designada(s) por la Presidencia del Consorcio a propuesta del responsable del sistema, y tendrá(n) encomendadas las funciones de seguridad orientadas al aseguramiento de la prestación del servicio y los medios de tratamiento de la información. Estas funciones se concretan en las siguientes:

a) Asumir, bajo la supervisión del responsable del sistema, la responsabilidad del diseño, implantación y control de las medidas técnicas de seguridad en cada sistema y aplicar los procedimientos operativos.
b) Llevar a cabo la gestión, configuración y actualización del hardware y software en el que se basan los mecanismos de seguridad de los sistemas.
c) Gestionar las autorizaciones de uso y perfiles de acceso a los sistemas.
d) Elaborar los planes de recuperación de sistemas.
e) Monitorizar continuamente el estado de seguridad de los sistemas.
f) Registrar los incidentes de seguridad.
g) Informar, periódicamente o a solicitud de éste, al Comité de Seguridad de la Información.
h) Ejercer las funciones delegadas por el responsable del sistema en su ámbito de competencia.
i) Colaborar en la resolución e investigación de incidentes de seguridad.

Funcions i responsabilitats del rol de responsable de seguretat

Donat que el rol de responsable de la seguretat de la informació (RSEG) es troba integrat al

Funciones y responsabilidades del rol de responsable de seguridad

Dado que el rol de responsable de la seguridad de la información (RSEG) se encuentra

Comie de Seguretat de la Información, els membres d'este Comité tindràn encomanades de forma col.legiada les funcions de seguretat orientades a la protecció de la informació. Aquestes funcions es concreten en les següents:

a) Mantindre i administrar el Sistema de Gestió de la Seguretat de la Informació.

b) Coordinar l'elaboració de polítiques, normes i guies de seguretat.

c) Dur a terme l'anàlisi dels riscos que afronten els sistemes de tractament de la informació i proposar accions per al seu tractament al Comité de Seguretat de la Informació.

d) Proposar al Comité de Seguretat de la Informació la categorització dels actius del Consorci i l'aplicabilitat de les mesures de protecció contemplades en l'Esquema Nacional de Seguretat.

e) Coordinar la realització periòdica d'auditories de seguretat i de conformitat amb l'Esquema Nacional de Seguretat.

f) Monitoritzar el compliment estricte dels controls de seguretat.

g) Registrar els incidents de seguretat, notificar-los a les autoritats de control, si de cas, i dur a terme el seu seguiment fins a la completa resolució d'aquests.

El Comité de Seguretat de la Informació

El Comité de Seguretat de la Informació té la funció d'assessorar la Presidència del Consorci en la presa de decisions relacionades amb la seguretat de la informació, i de proposar iniciatives sobre aquest tema.

Composició

El Comité de Seguretat de la Informació està

integrado en el Comité de Seguridad de la Información, los miembros de este Comité tendrán encomendadas de forma colegiada las funciones de seguridad orientadas a la protección de la información. Estas funciones se concretan en las siguientes:

a) Mantener y administrar el Sistema de Gestión de la Seguridad de la Información.

b) Coordinar la elaboración de políticas, normas y guías de seguridad.

c) Llevar a cabo el análisis de los riesgos que afrontan los sistemas de tratamiento de la información y proponer acciones para su tratamiento al Comité de Seguridad de la Información.

d) Proponer al Comité de Seguridad de la Información la categorización de los activos del Consorcio y la aplicabilidad de las medidas de protección contempladas en el Esquema Nacional de Seguridad.

e) Coordinar la realización periódica de auditorías de seguridad y de conformidad con el Esquema Nacional de Seguridad.

f) Monitorizar el cumplimiento estricto de los controles de seguridad.

g) Registrar los incidentes de seguridad, notificarlos a las autoridades de control, en su caso, y llevar a cabo su seguimiento hasta la completa resolución de los mismos.

El Comité de Seguridad de la Información

El Comité de Seguridad de la Información tiene la función de asesorar a la Presidencia del Consorcio en la toma de decisiones relacionadas con la seguridad de la información, y de proponer iniciativas al respecto.

Composición

El Comité de Seguridad de la Información está

integrat per:

a) La persona que ocupe la Gerència del Consorci, que actuarà com a president/a.
b) Les persones que ocupen els següents llocs, segons la Relació de Llocs de treball del Consorci, com a vocals:
   - Inspector/a Cap del Cos de Bombers
   - Cap de Servei de Recursos Humans
   - Responsable dels Serveis Econòmics
   - Responsable d'Assessoria Jurídica
   - Un/a oficial o tècnic/a del Cos de Bombers
c) Un administrador de seguretat, que actuarà com a vocal
d) La persona que exercisca les funcions de Delegat de Protecció de Dades, com a vocal.
e) La persona nomenada com a Responsable del Sistema (RSIS), que actuarà com a secretari/a.

En el cas en què dos rols coincidisquen en una mateixa persona, la Presidència del Consorci designarà a un altre vocal per a aconseguir el número màxim de nou (9) membres del Comité de Seguretat de la Informació.

Funcions

Són funcions del Comité de Seguretat de la Informació les que a continuació s'enumeren:

a) Assumir les funcions que s'estableixen en l'Esquema Nacional de Seguretat, i en la present Política, per als rols de responsable de la informació (RINFO), de responsable del servei (RSERV), i de responsable de seguretat (RSEG).
b) Proposar la planificació de les auditories necessàries per a garantir el compliment

integrado por:

a) La persona que ocupe la Gerencia del Consorcio, que actuará como presidente/a.
b) Las personas que ocupen los siguientes puestos, según la Relación de Puestos de Trabajo del Consorcio, como vocales:
   - Inspector/a Jefe del Cuerpo de Bomberos
   - Jefatura de Servicio de Recursos Humanos
   - Responsable de los Servicios Económicos
   - Responsable de Asesoría Jurídica
   - Un/a oficial o técnico/a del Cuerpo de Bomberos
c) Un/a administrador/a de seguridad, que actuará como vocal
d) La persona que ejerza las funciones de Delegado de Protección de Datos, como vocal
e) La persona nombrada como responsable del sistema, que actuará como secretario/a.

En el caso en que dos roles coincidan en una misma persona, la Presidencia del Consorcio designará a otro vocal para alcanzar el número máximo de nueve (9) miembros del Comité de Seguridad de la Información

Funciones

Son funciones del Comité de Seguridad de la Información las que a continuación se enumeran:

a) Asumir las funciones que se establecen en el Esquema Nacional de Seguridad, y en la presente Política, para los roles de responsable de la información (RINFO), de responsable del servicio (RSERV), y de responsable de seguridad (RSEG).
b) Proponer la planificación de las auditorías necesarias para garantizar el

de la legalitat vigent i el cicle de vida del Sistema de Gestió de la Seguretat de la Informació.

c) Analitzar els riscos que afronta el Consorci i proposar la presa de decisions executives sobre la manera de gestionar-los i el nivell de risc residual que resulta acceptable.

d) Proposar els objectius de seguretat i la seua planificació, i establir les necessitats de recursos per a la seua execució.

e) Vetlar perquè s'establisquen mecanismes de continuïtat de les activitats davant incidents de seguretat.

f) Supervisar l'eficàcia de les mesures de seguretat establides per a protegir la informació i garantir la disponibilitat i correcte funcionament dels serveis prestats pels sistemes d'informació.

g) Proposar les mesures encaminades a dirigir l'estratègia corporativa en matèria de seguretat i supervisar el Sistema de Gestió de la Seguretat de la Informació.

h) Proposar a la Direcció canvis en la Política de Seguretat de la Informació.

i) Proposar l'adopció de les normes en matèria de seguretat de la informació i d'ús de recursos tecnològics.

j) Dirigir la política de comunicació de les qüestions relacionades amb la seguretat de la informació.

k) Analitzar els resultats més significatius de les auditories periòdiques.

l) Proposar la priorització de les línies d'actuació en matèria de seguretat.

m) Resoldre els conflictes de responsabilitats en matèria de seguretat de la informació que puguen sorgir, així

cumplimiento de la legalidad vigente y el ciclo de vida del Sistema de Gestión de la Seguridad de la Información.

c) Analizar los riesgos que afronta el Consorcio y proponer la toma de decisiones ejecutivas sobre el modo de gestionarlos y el nivel de riesgo residual que resulta aceptable.

d) Proponer los objetivos de seguridad y su planificación, y establecer las necesidades de recursos para su ejecución.

e) Velar para que se establezcan mecanismos de continuidad de las actividades ante incidentes de seguridad.

f) Supervisar la eficacia de las medidas de seguridad establecidas para proteger la información y garantizar la disponibilidad y correcto funcionamiento de los servicios prestados por los sistemas de información.

g) Proponer las medidas encaminadas a dirigir la estrategia corporativa en materia de seguridad y supervisar el Sistema de Gestión de la Seguridad de la Información.

h) Proponer a la Dirección cambios en la Política de Seguridad de la Información.

i) Proponer la adopción de las normas en materia de seguridad de la información y de uso de recursos tecnológicos.

j) Dirigir la política de comunicación de las cuestiones relacionadas con la seguridad de la información.

k) Analizar los resultados más significativos de las auditorías periódicas.

l) Proponer la priorización de las líneas de actuación en materia de seguridad.

m) Resolver los conflictos de responsabilidades en materia de seguridad de la información que puedan

com els possibles conflictes d'interessos entre les funcions de RINFO, RSERV i RSEG.

Règim de funcionament

El Comité de Seguretat de la Informació regirà el seu funcionament, amb caràcter general, en el que s'estableix en la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic. Es reunirà amb caràcter ordinari almenys una vegada a l'any i, amb caràcter extraordinari, quan així ho decidisca el seu president, o a proposta d'almenys un terç dels seus membres.

El funcionament del Comité de Seguretat de la Informació es regirà pels següents principis:

- El president, previ informe del responsable del sistema, establirà l'ordre del dia i convocarà les reunions.
- Les actes de les reunions del Comité de Seguretat de la Informació tindran la classificació de confidencials i la difusió estarà restringida als membres que l'integren. El Comité, durant les reunions, pot decidir quins aspectes de les seues decisions i deliberacions poden ser públics i l'abast de la comunicació.
- El Comité quedarà vàlidament constituït quan compareguen, almenys, la meitat dels seus membres i estiga present el responsable del sistema o el delegat de protecció de dades.
- Per a totes les comunicacions del Comité de Seguretat de la Informació s'utilitzaran els mitjans electrònics corporatius.
- El Comité de Seguretat de la Informació ha d'ajustar el seu funcionament al que es preveu en la legislació vigent amb caràcter general relativa al funcionament

surgir, así como los posibles conflictos de intereses entre las funciones de RINFO, RSERV y RSEG.

Régimen de funcionamiento

El Comité de Seguridad de la Información regirá su funcionamiento, con carácter general, en lo establecido en la Ley 40/22015, de 1 de octubre, de Régimen Jurídico del Sector Público. Se reunirá con carácter ordinario al menos una vez al año y, con carácter extraordinario, cuando así lo decida su presidente, o a propuesta de al menos un tercio de sus miembros.

El funcionamiento del Comité de Seguridad de la Información se regirá por los siguientes principios:

- El presidente, previo informe del responsable del sistema, establecerá el orden del día y convocará las reuniones.
- Las actas de las reuniones del Comité de Seguridad de la Información tendrán la clasificación de confidenciales y la difusión estará restringida a los miembros que lo integren. El Comité, durante las reuniones, puede decidir qué aspectos de sus decisiones y deliberaciones pueden ser públicos y el alcance de la comunicación.
- El Comité quedará válidamente constituido cuando comparezcan, al menos, la mitad de sus miembros y esté presente el responsable del sistema o el delegado de protección de datos.
- Para todas las comunicaciones del Comité de Seguridad de la Información se utilizarán los medios electrónicos corporativos.
- El Comité de Seguridad de la Información debe ajustar su funcionamiento a lo previsto en la legislación vigente con carácter general

dels òrgans col·legiats.

relativa al funcionamiento de los órganos colegiados.

Funcions i responsabilitats derivades de l'aplicació de la normativa en matèria de tractament de dades de caràcter personal.

La normativa en matèria de Protecció de Dades de Caràcter Personal té nombrosos punts de contacte amb l'Esquema Nacional de Seguretat, en particular el que concern la necessitat que d'establir una responsabilitat sobre les decisions que definisquen les finalitats dels tractaments i sobre la seguretat d'aquests.

Addicionalment, aquesta normativa contempla la figura de la persona delegada de protecció de dades (d'ara en endavant, DPD), amb un rol específic d'assessorament i supervisió del compliment del que es disposa en la normativa de protecció de dades i de les polítiques del Consorci en matèria de protecció de dades personals. Atés que és previsible que el DPD haja de compaginar aquesta funció amb unes altres, és necessari evitar conflictes d'interessos entre les diverses tasques. El DPD actua com a assessor i supervisor intern, per la qual cosa no pot ocupar un lloc dins de l'organització que el porte a determinar les finalitats i els mitjans del processament de dades personals. Si aquesta figura s'associa a un dels anteriors perfils de seguretat relacionats en l'Esquema Nacional de Seguretat, s'haurà de tindre en compte aquesta incompatibilitat.

El DPD serà designat per la Direcció del Consorci i rendirà comptes, en matèria de tractament de dades de caràcter personal, directament a aquesta, la qual té la capacitat d'adoptar o promoure decisions basades en les recomanacions, propostes o avaluacions del DPD.

OBLIGACIONS DEL PERSONAL

Funciones y responsabilidades derivadas de la aplicación de la normativa en materia de tratamiento de datos de carácter personal.

La normativa en materia de Protección de Datos de Carácter Personal tiene numerosos puntos de contacto con el Esquema Nacional de Seguridad, en particular en lo que atañe a la necesidad de que se establezca una responsabilidad sobre las decisiones que definan los fines de los tratamientos y sobre la seguridad de los mismos.

Adicionalmente, esta normativa contempla la figura de la persona delegada de protección de datos (en adelante, DPD), con un rol específico de asesoramiento y supervisión del cumplimiento de lo dispuesto en normativa de protección de datos y de las políticas del Consorcio en materia de protección de datos personales. Dado que es previsible que el DPD deba compaginar esta funciones con otras, es necesario evitar conflictos de intereses entre las diversas tareas. El DPD actúa como asesor y supervisor interno, por lo que no puede ocupar un puesto dentro de la organización que lo lleve a determinar los fines y los medios del procesamiento de datos personales. Si esta figura se asocia a uno de los anteriores perfiles de seguridad relacionados en el Esquema Nacional de Seguridad, se deberá tener en cuenta esta incompatibilidad.

El DPD será designado por la Dirección del Consorcio y rendirá cuentas, en materia de tratamiento de datos de carácter personal, directamente a ésta, la cual tiene tiene la capacidad de adoptar o promover decisiones basadas en las recomendaciones, propuestas o evaluaciones del DPD.

OBLIGACIONES DEL PERSONAL

El personal del Consorci té l'obligació de conéixer i complir aquesta Política de Seguretat de la Informació i la normativa de seguretat que d'ella es derive, sent responsabilitat del Comité de Seguretat de la Informació disposar els mitjans necessaris per a fer-la arribar als afectats.

El personal del Consorcio tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad que de ella se derive, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para hacerla llegar a los afectados.

Les persones amb responsabilitat en l'ús, operació o administració de sistemes TIC rebran formació per al tractament segur dels sistemes en la mesura en què la necessiten per a dur a terme les seues funcions.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para llevar a cabo sus funciones.

El Comité de Seguretat de la Informació determinarà el caràcter obligatori o voluntari de les accions formatives.

El Comité de Seguridad de la Información determinará el carácter obligatorio o voluntario de las acciones formativas.

TERCERS

En cas que el Consorci preste serveis a altres organismes o tracte informació d'altres organismes, se'ls farà partícips d'aquesta Política de Seguretat de la Informació, i s'establiran canals de coordinació i procediments d'actuació per a la reacció davant incidents de seguretat.

TERCEROS

En el caso de que el Consorcio preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, y se establecerán canales de coordinación y procedimientos de actuación para la reacción ante incidentes de seguridad.

Quan el Consorci utilitze serveis de tercers o cedisca informació a tercers, se'ls farà partícips d'aquesta Política de Seguretat i de la normativa de seguretat que concernisca aquests serveis o informació. Aquest tercer quedarà subjecte a les obligacions establides en aquesta normativa, podent desenvolupar els seus propis procediments operatius per a satisfer-la. S'establiran procediments específics d'enviament i resolució d'incidències. Es garantirà que el personal de tercers estiga adequadament conscienciat en matèria de seguretat, almenys al mateix nivell que l'establit en esta Política.

Cuando el Consorcio utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la normativa de seguridad que ataña a dichos servicios o información. Dicho tercero quedará sujeto a las obligaciones establecidas en esta normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Quan algun aspecte de la Política no puga ser satisfet per un tercer, es requerirà un informe

Cuando algún aspecto de la Política no pueda ser satisfecho por un tercero, se requerirá un

del Comité de Seguretat de la Informació que precise els riscos en què s'incorre i la manera de tractar-los.

APROVACIÓ I REVISIÓ DE LA POLÍTICA DE SEGURETAT DE LA INFORMACIÓ

A fi de donar compliment al principi de millora continua del procés de seguretat, establida a l'article 11 del RD 3/2010, de 8 de gener, pel que es regula l'Esquema Nacional de Seguretat a l'àmbit de l'Administració Electrònica, el Comité de Seguretat de la Información inclourà, al menys una vegada a l'anyo, entre els temes a discutir, la revisió, actualització i propostes de modificacions de la Política de Seguretat.

Les modificacions de la Política de Seguretat de la Informació, s'efectuaran per la Presidència del Consorci a proposta del Comité de Seguretat de la Informació, previ informe de l'Assesoria Jurídica.

informe del Comité de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos.

APROBACIÓN Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

A fin de dar cumplimiento al principio de mejora continua del proceso de seguridad, establecida en el articulo 11 del RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el Comité de Seguridad de la Información incluirá, al menos una vez al año, entre los temas a discutir, la revisión, actualización y propuestas de modificaciones de la Política de Seguridad.

La modificaciones de la Política de Seguridad de la Información, se efectuarán por la Presidencia del Consorcio a propuesta del Comité de Seguridad de la Información, previo informe de la Asesoría Jurídica.