DONOSTIA
SAN SEBASTIÁN
Lehendakaritza
Presidencia
Ijentea, 1 | Tel. 010 - 943481000 | www.donostia.eus
20003 Donostia / San Sebastián

IRAGARKIA

Informazioaren Segurtasun-Politika eta Donostiako Udaleko Informazioaren Segurtasun-Batzordearen osaeraren aldaketaren onarpena.

DONOSTIAKO UDALA

Tokiko Gobernu Batzarrak, 2024ko uztailaren 9an egindako bilkuran, honako erabakia hartu zuen:

Datuen babesari buruzko araudian (Datuak Babesteko Erregelamendu Orokorra (2016/679 EB) eta Datu Pertsonalak Babesteari eta Eskubide Digitalak Bermatzeari buruzko abenduaren 5eko 3/2018 Lege Organikoa) eta segurtasunari buruzkoan (urtarrilaren 8ko 3/2010 Errege Dekretua, Segurtasun Eskema Nazionala arautzen duena) ezarritakoa aplikatuz, 2016ko otsailaren 16an, Donostiako Udaleko TGBak hainbat neurri hartu zituen, besteak beste, Informazioaren Segurtasunerako Batzordea sortzea– batzorde horren osaera geroago berrikusi da, Horrez gain, 2016ko maiatzaren 17an, Donostiako Udaleko TGBak Informazioaren Segurtasunerako Politika onartu zuen.

Donostiako Udalak, informazioaren eta zerbitzuen segurtasuna etengabe hobetzeko jardueren esparruan eta aurreko araudia indargabetzen duen Segurtasun Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuaren erregulazioak egindako aldaketen ondoren, aldaketak eta egokitzapenak sartu behar ditu Informazioaren Segurtasun Politikan, Informazioaren Segurtasun Batzordeari ere eragiten dioten rol eta erantzukizunetan, Xedapen Iragankor Bakarrean xedatutakoaren arabera, indarrean sartu eta ENS berrira egokitzeko lantzen joango diren beste batzuk alde batera utzi gabe.

311/2022 Errege Dekretuaren berritasunen artean, azpimarratzekoa da 2. artikuluan ezarritakoak 2016ko Instrukzioaren arau-lerruna igotzen duela. Horren arabera, administrazio publikoen zerbitzuak ematen zituzten edo soluzio-hornitzaileak ziren erakunde pribatuek, SENaren aplikazio-eremuan,

ANUNCIO

Aprobación de la Modificación y Aprobación de la Política de Seguridad de la Información y de la Composición del Comité de Seguridad de la Información del Ayuntamiento de San Sebastián.

AYUNTAMIENTO DE SAN SEBASTIÁN

La Junta de Gobierno Local, en sesión celebrada el día 9 de julio de 2024, ha acordado lo siguiente:

En aplicación a lo establecido en la normativa de protección de datos (Reglamento General de Protección de Datos (Reglamento (UE) 2016/679) y Ley Orgánica 3/2018, de 5 diciembre, de Protección de Datos de Carácter Personal y Garantía de los Derechos Digitales) y de seguridad (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad), con fecha de 16 de febrero de 2016 la JGL del Ayuntamiento de San Sebastián adoptó diversas medidas entre las que destacaban la creación, del Comité de Seguridad de la Información –comité cuya composición ha sido revisada con posterioridad en virtud de los acuerdos de la Junta. Posteriormente, con fecha de 17 de mayo de 2016, la JGL aprobó la Política de Seguridad de la Información del Ayuntamiento de San Sebastián.

El Ayuntamiento de Donostia-San Sebastián en el marco de las actuaciones de mejora continua de la seguridad de la información y los servicios y tras los cambios introducidos por la regulación del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad que deroga la anterior normativa, precisa incorporar modificaciones y adaptaciones en la Política de Seguridad de la Información, en los roles y responsabilidades que afectan también al Comité de Seguridad de la Información, sin perjuicio de aquellas otras que se irán abordando para adaptar el sistema de gestión de la seguridad al nuevo ENS , según lo dispuesto en la Disposición Transitoria Única.

Entre las novedades que introduce este Real Decreto 311/2022, cabe destacar que lo establecido en su artículo 2, es que eleva el rango normativo de la Instrucción de 2016 que exigía que las entidades privadas que prestaban servicios o eran proveedores de soluciones de las administraciones

10740n XVII

egiaztatu behar zuten beren sistemek SENaren II. eranskineko neurriak zituztela, bai adostasun-adierazpen baten bidez, bai sistemen kategoriaren araberako ziurtagiri baten bidez. Orain, gainera, betebehar horren barruan sartzen da Informazioaren Segurtasunerako Politika propioa ere izatea.

públicas, en el ámbito de aplicación del ENS, acreditasen que sus sistemas contaban con las medidas del Anexo II del ENS bien mediante una declaración de conformidad o una certificación en función de la categoría de los sistemas. Ahora, además, esta obligación incluye que dispongan también de su propia Política de Seguridad de la Información.

Rolen eta erantzukizunen egokitzapenak, eta, ondorioz, Segurtasun Batzordearenak, indargabetutako 3/2010 Errege Dekretuan jada jasota zegoen eginkizunak bereizteko beharretik datoz, eta 311/2022 Errege Dekretuaren 11. artikuluaren printzipioetako bat ere bada, erantzukizunak bereizteari buruzkoa: *Informazio-sistemetan, informazioaren arduraduna, zerbitzuaren arduraduna, segurtasunaren arduraduna eta sistemaren arduraduna bereiziko dira.* Horrela, Informazioaren Segurtasunerako Batzordean sartzen ziren rol batzuk bereizteko beharra adierazten da.

Respecto a las adaptaciones de los roles y responsabilidades y, en consecuencia, del Comité de Seguridad, devienen de la necesidad de separar funciones que ya venía recogida en el derogado RD 3/2010 y que también se incluye como uno de los principios del artículo 11 sobre diferenciación de responsabilidades del Real Decreto 311/2022: *En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.* Así se indica la necesidad de diferenciar diferentes roles, algunos de los cuales se integraban dentro del Comité de Seguridad de la Información.

LEHENENGO.- Donostiako Udalaren informazioren segurtasun-politika eguneratua onartzea, I. ERANSKIN gisa atxikitzen dena.

PRIMERO.- Aprobar la Política de Seguridad de la información actualizada del Ayuntamiento de San Sebastián que se adjunta a este acuerdo como ANEXO I.

BIGARRENA.- Donostiako Udaleko Informazioaren Segurtasunerako Batzordearen osaera eguneratzea. Organo horrek Segurtasun Eskema Nazionalaren eta Datu Pertsonalen Babesaren arloan erabakiak hartzeko eginkizunak ditu, eta jarraian adierazi dugun moduan osatuko da:

SEGUNDO.- Actualizar la composición del Comité de Seguridad de la Información del Ayuntamiento de San Sebastián, órgano con funciones decisorias en materia de Esquema Nacional de Seguridad y Protección de Datos Personales, que pasará a conformarse como se indica a continuación:

- **Batzordeko presidentea:** Informazioaren Segurtasuna Udalean zeharka ezartzeari buruzko ahalmenak eskuordetuta dituen zinegotzia.
- **Zerbitzuen arduraduna:** [Lehendakaritzako zuzendaria]
- **Informazioaren arduraduna:** [Lehendakaritzako zerbitzu orokorren burua]
- **Kanporatutako informazioko sistemei buruzko segurtasun arduraduna:** Kontratazioaz arduratzen diren departamentuetako zuzendariak, hirugarrenen erantzukizuneko kanpoko informazio sistemak dituzten udal zerbitzuei dagokienez.

- **Presidencia del Comité:** Concejal/a en quien se encuentren delegadas las facultades relativas a la implementación en el Ayuntamiento, con carácter transversal, de la Seguridad de la Información
- **Responsable de Servicios:** [Director/a de Presidencia]
- **Responsable de Información:** [Jefe/a de Servicios Generales de Presidencia]
- **Responsable de Seguridad respecto a los sistemas de información Municipales externalizados:** Directores/as de Departamento encargados/as de su contratación, respecto de los servicios municipales cuyos sistemas de información están externalizados y son responsabilidad de terceros.

- **Kanporatu gabeko udal informazioko sistemei buruzko segurtasun arduraduna:** DonostiaTIK Erakunde Autonomoko zuzendaria, barnean kudeatzen diren eta barneko erantzukizunekoak diren informazio sistemak dituzten udal zerbitzuei dagokienez.

- **Kanporatu gabeko udal informazioko sistemei buruzko sistema arduraduna:** DonostiaTIK erakunde autonomoko sistema- eta ustiapen-zerbitzuko burua, udal sare korporatiboan sartzen diren barne erantzukizuneko eta kudeaketako udal zerbitzuei dagokienez.

- **Datuak Babesteko kide anitzeko organo delegatuko lehendakaria**, haren ordezkari gisa, edo hark eskuordetutako organo horretako kide den presidentetzako teknikari juridikoa. Hitza izango du, baina botorik ez. Era berean, Batzordeko idazkari gisa jardungo du.

- **Responsable de Seguridad respecto a los sistemas de información Municipales no externalizados:** El/La Director/a del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales cuyos sistemas de información son responsabilidad y se gestionan internamente.

- **Responsable de Sistemas respecto a los sistemas de información Municipales no externalizados:** El/La Jefe/a del servicio de sistemas y explotación del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales que se incluyan en la red corporativa municipal y sobre los sistemas de información que son responsabilidad y se gestionan internamente.

- **El/la Presidente/a del órgano colegiado Delegado de Protección de Datos**, en representación del mismo, o el/la técnico/a jurídico/a de Presidencia que forme parte de dicho órgano en quien aquél delegue. Participará con voz pero sin voto. Actuará, a su vez, como Secretario del Comité.

HIRUGARRENA.- Batzordeko kidearen izendapena eta organo horren eginkizunak eraginpeko alderdiei jakinaraztea, akordio hau eta Informazioaren Segurtasun Politika igorriz.

TERCERO.- Comunicar la designación de miembro del comité y las funciones de este órgano, a las partes afectadas mediante la remisión de este acuerdo y la Política de Seguridad de la Información.

LAUGARRENA.-Informazioaren segurtasunari buruzko politika eta Informazioaren Segurtasunerako Batzordea izeneko kide anitzeko organoa Gipuzkoako Aldizkari Ofizialean eta Donostiako Udalaren Gardentasun Atarian argitaratzeko agintzea, pribatutasun-atalean.

CUARTO.- Ordenar la publicación de la política de Seguridad de la información y de la actualización del órgano colegiado denominado Comité de Seguridad de la Información en el Boletín Oficial de Gipuzkoa y en el Portal de Transparencia del Ayuntamiento de San Sebastián, en su apartado de privacidad.

I. ERANSKINA: DONOSTIAKO UDALAREN INFORMAZIOAREN SEGURTASUNERAKO POLITIKA

1. ONARTZEA ETA INDARREAN JARTZEA

Donostiako Udaleko Tokiko Gobernu Batzarrak, 2024ko uztailaren 9an, 2016ko maiatzaren 17an onartutako Informazioaren Segurtasunerako Politikaren aldaketa onartu zuen.

Informazioaren Segurtasunerako Politika hori (aurrerantzean, Politika) egun horretatik aurrera izango da eraginkorra, politika berri batek ordezten duen arte.

2. SARRERA

Administrazio Elektronikoa garatzeko, informazioaren eta komunikazioaren teknologien sistemek informazio asko tratatu behar dute. Informazioa askotariko mehatxu eta ahultasunen pean egoten da, eta mehatxuok kalte egin diezaiekete sistema horiei. 3/2010 Errege Dekretuak, urtarrilaren 8koak, Segurtasunerako Eskema Nazionala (SEN) Administrazio Elektronikoaren eremuan arautzen duenak, xede hau dauka: bermatzea informazio sistemek kontrolik gabeko etenik edo aldaketarik gabe emango dituztela beren zerbitzuak eta zainduko dutela informazioa beren zehaztapen funtzionalen arabera, eta informazioa ez zaiola helaraziko baimenik gabeko ezein pertsonari.

SENa betetze aldera, Donostiako Udalak, herritarren eskura dauden izapide elektronikoen euskarri diren informazio sistemei eragin diezaieketen arriskuak ezaguturik, eta kontuan hartuta herritarrek beren aktiborik baliotsuena jartzen dutela haren eskura (bere informazioa), badaki behar besteko arretaz administratu behar direla, eta neurri egokiak hartu behar direla horiek babesteko, tratatutako informazioaren edo emandako zerbitzuen eskuragarritasunari, osotasunari edo konfidentzialtasunari eragin diezaioketen ustekabeko edo nahita egindako kalteen aurrean.

Hala, Donostiako Udalean SENaren eremuaren barnean dauden departamentu eta/edo arlo guztiek kontuan izan behar dute IKTen segurtasuna sistemaren bizi zikloaren etapa bakoitzaren zati integrala dela, sortzen denetik zerbitzutik kentzen

ANEXO I: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE SAN SEBASTIÁN

1. APROBACIÓN Y ENTRADA EN VIGOR

La Junta de Gobierno Local del Ayuntamiento de Donostia/San Sebastián el día 9 de julio de 2024 aprobó la modificación de la Política de Seguridad de la Información aprobada el día 17 de mayo de 2016.

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

El desarrollo de la Administración Electrónica implica el tratamiento de gran cantidad de información por parte de los sistemas de tecnologías de la información y de las comunicaciones. La información está sometida a diferentes tipos de amenazas y de vulnerabilidades que pueden afectar a estos sistemas. El Real Decreto 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Al objeto de dar cumplimiento al ENS, el Ayuntamiento Donostia/San Sebastián, conocedora de los riesgos que pueden afectar a los sistemas de información, que soportan los trámites electrónicos puestos a disposición a la ciudadanía, y teniendo en cuenta que ésta pone a su disposición su activo más valioso “su propia Información” es consciente de que éstos deben ser administrados con la suficiente diligencia, y que se deben de tomar las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

De este modo, todos los departamentos y/o áreas del Ayuntamiento San Sebastián, que se encuentran dentro del ámbito del ENS, tienen presente que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta

den arte, bai eta garapen- edo eskuratze-erabakiak hartzean eta ustiapeneko jarduerak egitean ere. Segurtasun baldintzak eta finantzaketa premiak identifikatu eta plangintzan, eskaintzak eskatzeko orduan eta IKT proiektuetarako lizitazio pleguetan sartu behar dira.

Beraz, Donostiako Udalaren ustez, informazioaren kalitatea eta zerbitzuen etengabeko prestazioa bermatzea da Informazioaren Segurtasunaren helburua, prebentzioz jardunez, eguneroko jarduera gainbegiratuz gorabehera oro hautemateko eta halakoei azkar erantzuteko, ahalik eta lasterren leheneratze aldera.

su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por tanto, para el Ayuntamiento San Sebastián, el objetivo de la Seguridad de la Información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible.

3. DONOSTIAKO UDALAREN XEDEA

Donostiako Udalak, bere interesak eta esleituta dituen funtzio eta eskumenak kudeatzeko, herritarren beharrak eta nahiak asetzen laguntzen duten jarduerak sustatzen ditu eta zerbitzu publikoak ematen ditu. Horretarako, haren esku jartzen du izapidetze elektronikoa egitea, herritarrek gai publikoetan parte har dezaten bultzatzeko. Horrela, partaidetza-bide berriak ezarriko dira, demokrazia parte-hartzailearen garapena eta ekintza publikoaren eraginkortasuna bermatzeko.

Bestalde, Udalak eta herritarrek teknologia berriak gehiago erabil ditzaten sustatu nahi da. Hona hemen, besteak beste, lortu nahi diren helburu nagusiak: herritarrei Udalak eskaintzen dituen zerbitzuetarako sarbidea erraztea, harreman elektronikoa sustatuz, eta harreman horretan segurtasuna eta konfiantza ziurtatzea eta bermatzea.

3. MISIÓN DEL AYUNTAMIENTO DE DONOSTIA / SAN SEBASTIÁN

El Ayuntamiento de San Sebastián, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población. Para ello pone a disposición de la misma la realización de tramitación electrónica con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: facilitar el acceso de la ciudadanía a los servicios que ofrece el Ayuntamiento mediante el fomento de la relación electrónica así como asegurar y garantizar la seguridad y la confianza en esta relación.

4. IRISMENA

Irismena bi ikuspuntutatik zehaztuko da: batetik, antolamenduarena eta, bestetik, informazio sistemei edo irismen funtzionalari dagokiena.

Azken horri dagokionez, politika hori Donostiako Udalaren informazio-sistemei aplikatuko zaie, administrazio digitalerako beharrezkoak direnei, tratatutako informazioaren segurtasuna eta erakundeak emandako zerbitzuak behar bezala bermatzeko, herritarrei eta Udalari beren

4. ALCANCE

Se determinará el alcance desde un doble punto de vista, el organizativo por un lado y el relativo a sistemas de información o alcance funcional, por otro lado.

En cuanto a este último, esta Política se aplicará a los sistemas de información del Ayuntamiento de San Sebastián necesarios para la administración digital, con el objetivo de garantizar adecuadamente la Seguridad de la Información tratada y los servicios prestados por la entidad, de forma que se facilite a la

eskubideak baliatzeko eta betebeharrak bitarteko elektronikoen bidez betetzeko aukera emateko.

Administrazio eta herritarren arteko harremanetarako erabiltzen diren baliabideak enpresa pribatuek sortu dituzte eta oraindik ere mantentzen dituzte. Zerbitzuak, aplikazioak eta web-orriak dira, eta horien kudeaketa kanpoko enpresa horiei eskatu diete hainbat sailek eta udal-erakundek. Horiei dagokienez, SENen eremuan sartu beharko dira, eta enpresa horiei jakinarazi beharko zaizkie Udalak, bere erakunde autonomoek eta sozietate publikoek bete beharreko segurtasun-irizpideak, baliabideak segurtasun-baldintza horietara egokitu ditzaten.

Donostiako Udalarekin nolabaiteko harremana duten langile guztiek, SENaren irismenaren eraginpean daudenek, Informazioaren Segurtasunerako Politika hau eta segurtasun araudia ezagutu eta bete behar dituzte, eta Informazioaren Segurtasunerako Batzordearen ardura da informazioa eraginpeko langileengana iristeko beharrezkoak diren baliabideak izatea.

ciudadanía y al Ayuntamiento el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Existen recursos que se utilizan para las relaciones entre administraciones y la ciudadanía que han sido creadas y siguen siendo mantenidas por empresas privadas. Son servicios, aplicaciones y páginas web, cuya gestión ha sido encargado a éstas empresas externas por diferentes departamentos e incluso su entes municipales. En lo que a éstos se refiere, se deberán incluir dentro del ámbito de la ENS, y se deberá notificar a estas empresas los criterios de seguridad por los que se rige el Ayuntamiento y sus entes municipales, a fin de que adecúen los recursos a estos requisitos de seguridad.

Todos el personal que de una forma y otra, se relaciona con el Ayuntamiento San Sebastián, afectados por el alcance del ENS tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. ARAU ESPARRUA

Donostiako Udalaren jardueren eta, bereziki, herritarrei zerbitzu elektronikoak ematearen arau esparrua arau hauek osatzen dute:

- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.
- Ebazpena, 2016ko urriaren 13koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasuneko Jarraibide Teknikoa onartzen duena, Segurtasun Eskema Nazionalaren arabera.
- Ebazpena, 2016ko urriaren 7koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasunaren Egoerari buruzko Txostenaren Segurtasuneko Jarraibide Teknikoa onartzen duena.

5. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades del Ayuntamiento de San Sebastián, y, en particular, la prestación de sus servicios electrónicos a la ciudadanía, está integrado por las siguientes normas:

- Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Ebazpena, 2018ko martxoaren 27koa, Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasunaren Auditoretzaren Segurtasuneko Jarraibide Teknikoa onartzen duena.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Ebazpena, 2018ko apirilaren 13koa, Funtzio Publikoaren Estatu Idazkaritzarena, Segurtasun Gorabeheren Jakinarazpenaren Segurtasuneko Jarraibide Teknikoa onartzen duena.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babesteari eta Eskubide Digitalak Bermatzeari buruzkoa.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen prozesamenduan eta datu horien zirkulazioan pertsona fisikoak babesteari buruzkoa eta 95/46/EE Zuzentaraua, Datuen Babeserako Erregelamendu Orokorra, indargabetzen duena.
- 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).
- 7/1985 Legea, apirilaren 2koa, Toki Araubidearen Oinarriak arautzen dituena, apirilaren 21eko 11/1999 Legeak aldatua.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- 1308/1992 Errege Dekretua, urriaren 23koa, Armadaren Errege Institutu eta Behatokiaren Laborategia denboraren patroi nazionalaren gordailuzain eta Espainiako Metrologia Zentroari lotutako laborategi izendatzen duena.
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- 34/2002 Legea, uztailaren 11koa, informazioaren eta merkataritza elektronikoaren gizarteko zerbitzuei buruzkoa.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 57/2003 Legea, abenduaren 16koa, tokiko administrazioa modernizatzeko neurriak ezarri zituena.
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
- 1553/2005 Errege Dekretua, abenduaren 23koa, Nortasun Agiri Nazionala eta haren sinadura elektronikoko ziurtagiriak emateko modua arautzen duena.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- 37/2007 Legea, azaroaren 16koa, Sektore Publikoko Informazioa Berrerabiltzeari buruzkoa.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

- 25/2007 Legea, urriaren 18koa, komunikazio elektronikoei eta komunikazioen sare publikoei buruzko datuak gordetzeari buruzkoa.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- 56/2007 Legea, abenduaren 28koa, Informazioaren Gizartea bultzatzeko neurriei buruzkoa.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.

- 1494/2007 Errege Dekretua, azaroaren 12koa, desgaitasuna duten pertsonek informazioaren gizartearekin eta gizarte-hedabideekin lotutako teknologiak, produktuak eta zerbitzuak eskuratzeko oinarrizko baldintzei buruzko Erregelamendua onartzen duena.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

- 1495/2011 Errege Dekretua, urriaren 24koa, Estatuko sektore publikoko informazioa berrerabiltzeari buruzko azaroaren 16ko 37/2007 Legea garatzen duena.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.

- 19/2013 Legea, abenduaren 9koa, Gardentasunari, Informazio Publikoa Eskuratzeko Bideari eta Gobernu Onari buruzkoa.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

- 11/2022 Lege Orokorra, ekainaren 28koa, Telekomunikazioei buruzkoa.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.

- 39/2015 Legea, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkidearena.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- 40/2015 Legea, urriaren 1ekoa, Sektore Publikoaren Araubide Juridikoarena.
- Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público.

- 5/2015 Legegintzako Errege Dekretua, urriaren 30ekoa, Enplegatu Publikoaren Oinarrizko Estatutuaren Legearen Testu Bategina onartzen duena.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

- 9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB zuzentarauak Espainiako ordenamendu juridikoan sartzen dituena.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

- 12/2018 Errege Lege Dekretua, irailaren 7koa, Informazio Sare eta Sistemen Segurtasunarena.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

- 1112/2018 Errege Dekretua, irailaren 7koa, Sektore publikoko webguneen eta gailu mugikorretarako aplikazioen erabilerraztasunari buruzkoa.
- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

• 14/2019 Errege Lege Dekretua, urriaren 31koa, zeinaren bitartez premiazko neurriak hartu diren segurtasun publikoko arrazoiengatik administrazio digitalaren, sektore publikoko kontratazioaren eta telekomunikazioen alorretan.	• Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
• 3/2020 Errege Lege Dekretua, otsailaren 4koa, premiazko neurriena, zeinaren bitartez Europar Batasuneko hainbat zuzentarau Espainiako ordenamendu juridikoan jasotzen diren sektore publikoko kontratazio arloan: aseguru pribatuetan, pentsio-plan eta funtsenetan, zerga-arloan eta zerga-auzietan.	• Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales.
• 6/2020 Legea, azaroaren 11koa, konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.	• Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
• 24/2021 Errege Lege Dekretua: 9/2017 Legea eta 3/2020 Errege Lege Dekretua aldatzekoa.	• Real Decreto-ley 24/2021: modificación de la Ley 9/2017 y del Real Decreto-ley 3/2020.
• 203/2021 Errege Dekretua, martxoaren 30ekoa, sektore publikoaren bitarteko elektronikoen bidezko jardunaren eta funtzionamenduaren erregelamendua onartzen duena.	• Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
• 10/2021 Legea, uztailaren 9koa, Urrutiko Lanari buruzkoa.	• Ley 10/2021, de 9 de julio, de trabajo a distancia.
• 2/2016 Legea, apirilaren 7koa, Euskadiko Toki Erakundeei buruzkoa.	• Ley 2/2016, de 7 de abril, de Instituciones Locales de Euskadi.
• 4/2019 Foru Araua, martxoaren 11koa, Gobernu Onari buruzkoa, foru gobernantza publikoaren esparruan.	• Norma Foral 4/2019, de 11 de marzo, de Buen Gobierno en el marco de la gobernanza pública foral.
• Donostiako Udaleko Tokiko Gobernu Batzordearen 2016ko maiatzaren 17ko Ebazpena, Informazioaren Segurtasunerako Politika eta ondorengo aldaketak onartu zituena.	• Resolución de la Junta de Gobierno Local del Ayuntamiento de Donostia/San Sebastián del día 17 de mayo de 2016 aprobó la Política de Seguridad de la Información y sucesivas modificaciones.
• 163/2018 EBAZPENA, abenduaren 12koa, Jaurlaritzaren Idazkaritzako eta Legebiltzarrarekiko Harremanetarako zuzendariarena, zeinaren bidez Gipuzkoako Foru Aldundiarekin sinatutako lankidetza hitzarmena, administrazio elektronikoko oinarrizko irtenbideak elkarri ematekoa, argitaratzea xedatzen baita.	• RESOLUCIÓN 163/2018, de 12 de diciembre, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, por la que se dispone la publicación del Convenio de colaboración suscrito con la Diputación Foral de Gipuzkoa, para la prestación mutua de soluciones básicas de administración electrónica.

- Euskal Autonomia Erkidegoko Administrazio Orokorrak 2017ko martxoaren 24an Estatuko Administrazio Orokorrarekin eta 2018ko abenduaren 5ean Gipuzkoako Foru Aldundiarekin sinatutako lankidetza hitzarmenei atxikitzeko protokoloa, elkarri administrazio elektronikoko oinarrizko irtenbideak emateko.
- Eta aplikatzekoa den gainerako legeria guztia, esaterako, Ondare Historikoari buruzko Legea, Jabetza Intelektuala Babesteari buruzkoa, etab.

- Protocolo de adhesión a los convenios de colaboración para la prestación mutua de soluciones básicas de administración electrónica suscritos por la Administración General de la Comunidad de Euskadi con la Administración General del Estado el 24 de marco de 2017 y con la Diputación Foral de Guipúzkoa el 5 de diciembre de 2018.
- Y por toda la demás legislación que resulte de aplicación, como la Ley de Patrimonio Histórico, de Protección de la Propiedad Intelectual etc.

Arau esparruaren parte dira, halaber, Donostiako Udalaren Administrazio Elektronikoari aplikatzekoak diren gainerako arauak, aurrekoetatik eratorriak eta egoitza elektronikoetan argitaratuak, Politika honen aplikazio eremuaren barrukoak, bai eta Donostiako Udalaren Osoko Bilkurak 2012ko maiatzaren 18an onartutako Segurtasun Agiria ere.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de San Sebastián derivadas de las anteriores y publicadas en las sedes electrónica comprendidas dentro del ámbito de aplicación de de la presente Política así como el Documento de Seguridad de 18 de mayo de 2012 aprobado por el Pleno del Ayuntamiento de San Sebastián.

Segurtasun Batzordea erregistro bat mantentzeaz arduratuko da, aplikatu beharreko arau-esparruarekin, nahitaez bete beharreko segurtasun-jarraibide teknikoak barne:

El Comité de Seguridad se encargará de mantener un registro con el marco normativo aplicable, incluyendo las instrucciones técnicas de seguridad de obligado cumplimiento:

•Informazio Sistemen Segurtasunaren Auditoretzako ITS,

• Segurtasun Eskema Nazionalaren araberako ITSak,

•Segurtasunaren Egoerari buruzko Txostenaren STI,

• Segurtasun-intzidenteak jakinarazteko ITSak

- ITS de Auditoría de la Seguridad de los Sistemas de Información,
- ITS de Conformidad con el Esquema Nacional de Seguridad,
- ITS de Informe del Estado de la Seguridad,
- ITS de Notificación de Incidentes de Seguridad

Era berean, DonostiaTIKeko Segurtasun Batzordea arduratuko da artikulu horretan aipatzen diren CCNren segurtasun jarraibideak eta gidak identifikatzeaz. Jarraibide eta gida horiek informazio sistemei aplikatu beharko zaizkie, Segurtasun Eskema Nazionalean ezarritakoa hobeto betetzeko.

Así mismo, el Comité de Seguridad de DonostíaTIK será el responsable de identificar las instrucciones y guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación a los sistemas de información para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. ARTIKULUAK BETETZEA

Donostiako Udalak, Segurtasun Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuan oinarrizko printzipioak eta gutxieneko baldintzak jasotzen dituzten artikuluak betetzeko, babestu beharreko informazioaren eta zerbitzuen araberako segurtasun neurri batzuk ezarri ditu, eragindako sistemen kategoria kontuan hartuta.

6. CUMPLIMIENTO DE ARTÍCULOS

El Ayuntamiento de San Sebastián para lograr el cumplimiento de los artículos del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los

servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Segurtasuna prozesu integral eta gutxieneko pribilegio gisa

Segurtasuna prozesu integral bat da, eta sistemarekin zerikusia duten elementu tekniko, pertsonal, material eta juridiko eta antolamenduzko elementu guztiek osatzen dute. Segurtasun Eskema Nazionala Donostiako Udalari aplikatzeko orduan, printzipio hori izango da oinarri, unean uneko ezein jarduera edo egoeraren araberako tratamendu salbuetsita.

Erabateko arreta jarriko zaie prozesuan parte hartzen duten pertsonei eta horien arduradun hierarkikoei, ez daitezen segurtasunerako arrisku iturriak izan ezjakintasunagatik, antolaketa edo koordinazio faltagatik eta jarraibide desegokiak betetzeagatik.

Informazio sistemak diseinatu eta osatzeko orduan, behar bezala funtzionatzeko beharrezkoak diren gutxieneko pribilegioak eman behar dira; horretarako, alderdi hauek txertatu behar dira:

a) Sistemak ezinbestekoa den funtzionaltasuna emango du erakundeak bere eskumen- edo kontratu-helburuak lor ditzan.

b) Jarduteko, administratzeko eta jarduera erregistratzeko funtzioak beharrezkoak diren gutxienekoak izango dira, eta baimena duten pertsonek baimendutako kokaleku edo ekipamenduetatik soilik egiten dituztela ziurtatuko da; hala badagokio, ordutegiak eta sarrera puntu gaituak murrizteko eskatu ahal izango dira.

c) Ustiapen sistema batean, konfigurazioa kontrolatuz, lortu nahi den helbururako beharrezkoak edo egokiak ez diren funtzioak ezabatu edo desaktibatuko dira. Sistemaren ohiko erabilerak erraza eta segurua izan behar du, halako moldez non erabiltzailearen ekintza kontzientea beharko baita erabilera ez-seguru bat egiteko.

d) Teknologia bakoitzerako segurtasuna konfiguratzeko gidak aplikatuko dira, sistemaren kategorizaziora egokituta, beharrezkoak edo egokiak ez diren funtzioak ezabatu edo desaktibatzeko.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de San Sebastián, estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

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

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

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

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

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

Etengabeko zaintza, aldizkako ebaluazioa eta integritatea, sistemaren eguneraketa eta segurtasun prozesuaren etengabeko hobekuntza

Donostiako Udalaren etengabeko zaintzari esker, ohiz kanpoko jarduerak edo portaerak detektatu ahal izango dira, eta erantzun egokia eman ahalko zaie.
Aktiboen segurtasun egoera etengabe ebaluatzeak aukera emango du horien bilakaera neurtu, ahultasunak hauteman eta konfigurazio akatsak identifikatzeko.

Segurtasun neurriak aldian-aldian ebaluatu eta eguneratuko dira, haien eraginkortasuna arriskuen bilakaerara eta babes sistemetara egokitzeko, eta, beharrezkoa izanez gero, segurtasuna berriz planteatu ahalko da.

Sistemaren aktiboen katalogo eguneratuan edozein elementu fisiko edo logiko sartu edo aldatzeko, aldez aurreko baimen formala beharko da.

Etengabeko ebaluazioari eta monitorizazioari esker, sistemen segurtasun egoera egokitu ahalko da eta, hala, konfigurazio akatsak, identifikatutako ahultasunak eta haiei eragiten dieten eguneratzeak artatuko dira, eta horietan gertatutako gorabehera oro goiz detektatu ahalko da.

Ezarritako segurtasun prozesu integrala etengabe eguneratu eta hobetu beharko da. Horretarako, informazioaren teknologien segurtasunaren kudeaketari buruz Estatuko eta nazioarteko jardunbidean onartutako irizpide eta metodoak aplikatuko dira.

Langileen kudeaketa eta profesionaltasuna

SENaren esparruan Donostiako Udalaren informazio sistemekin zerikusia duen barneko zein kanpoko pertsona orok segurtasunaren arloan dituen betebeharrei, obligazioei eta erantzukizunei buruzko prestakuntza eta informazioa jasoko du. Haien jarduna ikuskatuko da, ezarritako prozedurak betetzen dituztela egiaztatzeko.

Sistemaren erabilera seguruaren esanahia eta irismena segurtasun arau batzuetan zehaztu eta jasoko da, eta arau horiek Donostiako udaleko Tokiko Gobernu Batzordea onartuko ditu. Era berean, langileek beren lanpostua betetzeko izan behar dituzten prestakuntza- eta esperientzia-betekizunak zehaztuko dira.

Vigilancia continua, reevaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento de San Sebastián permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Gestión de personal y profesionalidad

Todo el personal, propio o ajeno relacionado con los sistemas de información del Ayuntamiento de San Sebastián dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la Junta de Gobierno Local. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Langile kualifikatuek aztertu eta ikuskatuko dute informazio sistemen segurtasuna. Langileok prestatuta egongo dira informazio sistemen bizi-zikloaren fase guztietan aritzeko: plangintza, diseinua, eskuratzea, eraikitzea, hedatzea, ustiatzea, mantentzea, gorabeherak kudeatzea eta suntsitzea.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Objektiboki eta diskriminaziorik gabe, zerbitzuak ematen dizkiguten erakundeek profesional kualifikatuak edukitzea eta kudeaketa maila eta emandako zerbitzuen heldutasun maila egokiak izatea eskatuko da.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Arriskuetan oinarritutako segurtasunaren kudeaketa, arriskuen analisia eta kudeaketa

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

Arriskuen analisia eta kudeaketa segurtasun prozesuaren funtsezko zati bat izango da, eta etengabe eguneratuko da.

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

Arriskuen kudeaketari esker, ingurune kontrolatua mantendu eta arriskuak maila onargarrietara gutxitu ahalko dira. Maila horiek murrizteko, segurtasun neurriak egokiro aplikatuko dira, modu orekatuan eta tratatutako informazio motara, eman beharreko zerbitzuetara eta dituzten arriskuetara egokituta.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Kudeaketa hori egiteko, sistemak dituen arriskuak aztertu eta tratatuko dira. Ezertan eragotzi gabe II. eranskinean ezarritakoa, nazioartean onartutako metodologiaren bat erabiliko da. Arriskuak arindu edo ezabatzeko hartutako neurriek justifikatuta egon beharko dute eta, nolanahi ere, neurrion eta arriskuen arteko proportzionaltasuna mantenduko da.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Segurtasuneko gorabeherak, prebentzioa, detekzioa, erreakzioa eta leheneratzea

Incidentes de seguridad, prevención, detección, reacción y recuperación

Donostiako Udalak segurtasun gorabeherak kudeatzeko zenbait prozedura ditu, 33.artikuluan jasotakoaren arabera; halaber, dagokion Segurtasuneko Jarraibide Teknikoa du, bai eta detekzio mekanismoak, sailkapen irizpideak, analisi- eta ebazpen-prozedurak eta alderdi interesdunei jakinarazteko bideak ere.

El Ayuntamiento de San Sebastián, dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

Sistemaren segurtasunak prebentzioaren, detekzioaren eta erantzunaren alderdiei buruzko ekintzak barne hartuko ditu, haren ahultasunak minimizatzeko eta haren gaineko mehatxuak saihesteko, edo, mehatxuok gauzatzen badira, tratatzen duen informazioan edo ematen dituen

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que

zerbitzuetan eragin larririk ez izatea lortzeko.

Prebentzio neurriek asmoa kentzeko edo esposizioa murrizteko osagaiak eduki ahalko dituzte, eta mehatxuak gauzatzeko aukera ezabatu edo murriztu beharko dute.

Detekzio neurrien xedea zibergertakari bat dagoenean hura hautematea izango da.

Erantzun neurriak dagokion unean kudeatuko dira, eta segurtasun gorabehera batek ukitutako informazioa eta zerbitzuak lehengoratzeko xedea izango dute.

Informazio sistemaren bidez, datuak eta informazioa euskarri elektronikoan gordeko direla bermatuko da.

Era berean, sistemak eskuragarri jarriko ditu zerbitzu guztiak, informazio digitalaren bizi ziklo osoan, ondare digitala babesteko oinarri izango diren ikusmolde eta prozeduren bidez.

Elkarri konektatutako beste informazio sistema batzuen aurrean defendatzeko eta prebenitzeko lerroak egotea

Donostiako Udalak informazio sistema babesteko estrategia bat ezarri du, zeina zenbait segurtasun geruzaz osatuta baitago eta, geruzok, aldi berean, antolamenduzko zenbait neurriz eta zenbait neurri fisiko eta logikoz osatuta baitaude. Hala, geruza bat arriskuan jartzen denean, erantzun egokia garatu daiteke saihestu ezin izan diren gertakarientzat eta, hala, sistema osoa arriskuan jartzeko probabilitatea murriztu eta azken inpaktua minimizatuko da.

Informazio sistemaren perimetroa babestuko da, bereziki, Udalaren sistema sare publikoetara konektatzen denean, 9/2014 Lege Orokorrak, maiatzaren 9koak, Telekomunikazioei buruzkoak zehazten dituen moduan; horretarako, segurtasun gorabeherak prebenitzeko, detektatzeko eta horiei erantzuteko lanak indartuko dira.

Nolanahi ere, sistema beste sistema batzuekin konektatzeak sortzen dituen arriskuak aztertuko dira, eta haien arteko lotura puntua kontrolatuko da. Sistemen arteko konexioa egokia izan dadin, dagokion Segurtasuneko Jarraibide Teknikoan xedatutakoa beteko da.

maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento de San Sebastián, ha implementado una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Erantzukizunak bereiztea, antolamendua eta segurtasun prozesua ezartzea

Donostiako Udalak korporazioko kide guztiak barne hartuta antolatu du bere segurtasuna; horretarako, argi eta garbi bereizitako erantzukizunak dituzten hainbat segurtasun rol izendatu ditu, dokumentu honetako «SEGURTASUNAREN ANTOLAMENDUA» atalean jasota dagoen moduan.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento de San Sebastián, ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Baimena eta sarbideen kontrola

Donostiako Udalak informazio sistemarako sarbidea kontrolatzeko zenbait mekanismo ezarri ditu; hala, behar bezala baimendutako erabiltzaile, prozesu, gailu eta beste informazio sistemetara mugatu du, eta baimendutako funtzioetarako soilik.

Autorización y control de los accesos

El Ayuntamiento de San Sebastián, ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los/las usuarios/as, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Instalazioen babesa

Donostiako Udalak sarbide fisikoa kontrolatzeko zenbait mekanismo ezarri ditu, baimenik gabe fisikoki sartzea eta informazioari eta baliabideei kalteak eragitea saihesteko, segurtasun perimetroen, kontrol fisikoen eta eremuetako babes orokorren bidez.

Protección de las instalaciones

El Ayuntamiento de San Sebastián, ha implementado mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Segurtasun produktuak erostea eta segurtasun zerbitzuak kontratatzea

Segurtasun produktuak erosteko edo segurtasun zerbitzuak kontratatzeko, Donostiako Udalak kontuan hartuko ditu sistemaren kategoriaren araberako erabilera eta zehaztutako segurtasun maila, erosketaren xede den segurtasun funtzionaltasuna ziurtatuta dutenak.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento de San Sebastián, tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Segurtasun zerbitzuak kontratatzeko, profesionaltasunari buruz adierazitakoa hartuko da kontuan.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Biltegiratutako eta iragaitzazko informazioaren babesa eta jardueraren jarraitutasuna

Donostiako Udalak arreta berezia jarriko du ekipamendu edo gailu eramangarri edo mugikorren, gailu periferikoen, informazio euskarrien eta sare irekietako komunikazioen bidez biltegiratutako eta iragaitzazko informazioan, eta halakoak bereziki aztertu beharko dira babes egokia lortzeko.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de San Sebastián, prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Errege Dekretu honen aplikazio eremuan sartzen diren informazio sistemek sortutako dokumentu

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los

elektronikoak epe luzera lehengoratu eta kontserbatzea bermatzen duten prozedurak aplikatuko dira, hala eska daitekeenean.

documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Errege Dekretu honek aipatzen duen informazio elektronikoaren zuzeneko kausa edo ondorio izan den euskarri ez-elektronikoko informazio orok haren segurtasun maila berean egon behar du babestuta. Horretarako, euskarri motari dagozkion neurriak aplikatuko dira, aplikatzekoak diren arauen arabera.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Sistemek segurtasun kopiak izango dituzte, eta beharrezkoak diren baliabideak ezarriko dira ohiko baliabideak galduz gero eragiketen jarraitutasuna bermatzeko.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Jarduera erregistratzea eta kode kaltegarria detektatzea

Registro de actividad y detección de código dañino

Donostiako Udalak, Errege Dekretu honen xedea betetze aldera, ukitutako pertsonen ohorerako, norberaren eta familiaren intimitaterako, eta bakoitzaren irudirako eskubidea erabat bermatuz, eta datu pertsonalen babesari buruzko araudi publikoari eta lan-araudiari jarraikiz, bai eta aplikagarriak diren gainerako xedapenei ere, erabiltzaileen jarduerak erregistratuko ditu, eta bidegabeak edo baimenik gabeak diren jarduerak monitorizatu, aztertu, ikertu eta dokumentatzeko behar-beharrezkoa den informazioa gordeko du, jarduten ari den pertsona une oro identifikatzeko aukera emanez.

El Ayuntamiento de San Sebastián, con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará las actividades de los/las usuarios/as, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Informazio sistemen segurtasuna zaintze aldera, administrazio publikoen jarduteko printzipioak zorrotz betetzen direla bermatuta, Datuak Babesteko Erregelamendu Orokorrean xedatutakoarekin bat etorriz, eta xedea mugatzeari, datuak minimizatzeari eta datuak mugatzeari buruz horietan jasotakoa errespetatuta, Udalak, behar-beharrezkoa den neurrian eta modu orekatuan, sartzen edo irteten diren komunikazioak aztertu ahal izango ditu, eta informazioaren segurtasunaren helburuetarako soilik, halako moldez non informazio-sare eta -sistemetara baimenik gabe sartzea eragotzi, zerbitzu-ukapenaren erasoak gelditu, kode kaltegarria asmo txarrez banatzea saihestu eta aipatutako informazio-sare eta -sistemei beste kalte batzuk eragitea eragotzi ahal izango baita.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Zuzentzeko edo, hala badagokio, erantzukizunak eskatzeko, informazio sisteman sartzen den erabiltzaile bakoitzak modu bakarrean identifikatuta egon beharko du, halako moldez non uneoro jakingo baita nork jasotzen dituen sartzeko eskubideak, nolakoak diren, eta nork egin duen jarduera jakin bat.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Azpiegitura eta zerbitzu komunak

Donostiako Udalak kontuan hartuko du administrazio publikoen azpiegitura eta zerbitzu komunak erabiltzea, partekatuak edo zeharkakoak barne, lagungarria izango dela Errege Dekretu honetan xedatutakoa betetzeko.

Infraestructuras y servicios comunes

El Ayuntamiento de San Sebastián, tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto.

Betetze profil espezifikoak eta konfigurazio seguruak inplementatzeko erakundeen egiaztapena

Donostiako Udalak kontuan hartuko du tokiko erakundeentzako aplikagarriak diren berariazko betetze profilen aplikazioa.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento de San Sebastián, tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

7. SEGURTASUNAREN ANTOLAMENDUA

Donostiako Udaleko Informazioaren Segurtasunaren Antolamenduaren honela egituratzen da.

7. ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa de la Organización de la Seguridad de la Información en el Ayuntamiento de San Sebastián se establece en la forma que se indica a continuación.

7.1 Informazioaren Segurtasuneko rolak

Hona hemen informazioaren segurtasuneko funtsezko rolak:

- Zerbitzuen arduraduna: [Lehendakaritzako zuzendaria]
- Informazio-arduraduna: [Lehendakaritzako Zerbitzu Orokorretako burua]
- Udaleko informazio-sistema korporatiboei buruzko segurtasun-arduraduna: DonostiaTIK erakunde autonomoko zuzendaria, informazio-sistemen ardura duten eta barnean kudeatzen diren udal-zerbitzuei dagokienez.
- Segurtasuneko arduraduna kanporatutako udal-informazioko sistemei dagokienez:

7.1 Roles de Seguridad de la Información

Los roles fundamentales en la Seguridad de la Información son los siguientes:

- Responsable de Servicios: [Director/a de Presidencia]
- Responsable de Información: [Jefe/a de Servicios Generales de Presidencia]
- Responsable de Seguridad respecto a los sistemas de información municipales corporativos : El/La Director/a del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales cuyos sistemas de información son responsabilidad de DonostiaTIK y se gestionan internamente.
- Responsable de Seguridad respecto a los sistemas de información municipales

horiek kontratatzeaz arduratzen diren saileko zuzendariak, hirugarrenen ardura diren informazio-sistemak dituzten udal-zerbitzuei dagokienez.

- Udaleko informazio-sistema korporatiboei buruzko sistemaren arduraduna: DonostiaTIK erakunde autonomoko sistema- eta ustiapen-zerbitzuko burua, udal-sare korporatiboan sartzen diren udal-zerbitzuei eta barnean kudeatzen diren informazio-sistemei dagokienez.

externalizados: Directores/as de Departamento encargados/as de su contratación, respecto de los servicios municipales cuyos sistemas de información son responsabilidad de terceros.

- Responsable de Sistema respecto a los sistemas de información municipales corporativos: El/La Jefe/a del servicio de sistemas y explotación del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales que se incluyan en la red corporativa municipal y sobre los sistemas de información que son responsabilidad de DonostiaTIK y se gestionan internamente.

7.2 Segurtasun Batzordea

Segurtasun Batzordea kargu eta pertsona hauek osatuko dute:

- Batzordeko lehendakaria: Gobernantza arloko zinegotzi arduraduna
- Zerbitzuen arduraduna: [Lehendakaritzako zuzendaria]
- Informazio-arduraduna: [Lehendakaritzako Zerbitzu Orokorretako burua]
- Udaleko informazio-sistema korporatiboei buruzko segurtasun-arduraduna: DonostiaTIK erakunde autonomoko zuzendaria, informazio-sistemen ardura duten eta barnean kudeatzen diren udal-zerbitzuei dagokienez.
- Segurtasuneko arduraduna kanporatutako udal-informazioko sistemei dagokienez: horiek kontratatzeaz arduratzen diren saileko zuzendariak, hirugarrenen ardura diren informazio-sistemak dituzten udal-zerbitzuei dagokienez.
- Udaleko informazio-sistema korporatiboei buruzko sistemaren arduraduna: DonostiaTIK erakunde autonomoko sistema- eta ustiapen-zerbitzuko burua, udal-sare korporatiboan sartzen diren udal-zerbitzuei eta barnean kudeatzen diren informazio-sistemei dagokienez.

7.2 Comité de Seguridad

El Comité de Seguridad estará constituido por los siguientes cargos y personas:

- Presidencia del Comité: Concejal/a responsable del área de Gobernanza
- Responsable de Servicios: [Director/a de Presidencia]
- Responsable de Información: [Jefe/a de Servicios Generales de Presidencia]
- Responsable de Seguridad respecto a los sistemas de información Municipales corporativos: El/La Director/a del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales cuyos sistemas de información son responsabilidad y se gestionan internamente
- Responsable de Seguridad respecto a los sistemas de información Municipales externalizados: Directores/as de Departamento encargados/as de su contratación, respecto de los servicios municipales cuyos sistemas de información son responsabilidad de terceros.
- Responsable de Sistema respecto a los sistemas de información Municipales corporativos: El/La Jefe/a del servicio de sistemas y explotación del Organismo Autónomo DonostiaTIK, respecto de los servicios municipales que se incluyan en la red corporativa municipal y sobre los sistemas de información que son

- Datuak Babesteko kide anitzeko organo delegatuko lehendakaria, haren ordezkari gisa, edo hark eskuordetutako organo horretako kide den presidentetzako teknikari juridikoa. Hitza izango du, baina botorik ez. Era berean, Batzordeko idazkari gisa jardungo du.

Datuak Babesteko organo ordezkariaren lehendakariak hitzarekin baina botorik gabe parte hartuko du. Era berean, Batzordeko idazkari gisa jardungo du.

Informazioaren Segurtasunerako Batzordearen ohiko bilerak sei hilean behin egingo dira.

Ezohiko bilerak egin ahalko dira premiek edo inguruabarrek hala eskatzen duten bakoitzean.

7.3 Segurtasun Eskema Nazionalarekin lotutako arduradunen eginkizunak

Jarraian, pertsona bakoitzaren funtzioak eta erantzukizunak zehaztu eta ezarriko dira:

Zerbitzuen arduraduna:

- Zerbitzuen segurtasunaren kategoriaren balioespenak egiten ditu, zerbitzuen segurtasunari eragiten dion intzidente batek izango lukeen eraginaren balioespenaren arabera, erabilgarritasunari, egiazkotasunari, osotasunari, konfidentzialtasunari edo trazabilitateari kalte eginez.
- Informazioaren arduradunak informazioaren segurtasun-betekizunak zehazten ditu, maiatzaren 3ko 311/2022 Errege Dekretuaren I. eranskinean ezarritako esparruaren barruan, ENS segurtasun-arduradunak proposatu ondoren.

Informazioaren arduraduna:

- Informazioaren segurtasunaren kategoriaren balioespenak egiten ditu, informazioaren segurtasunari eragiten dion intzidente batek izango lukeen eraginaren balioespenaren arabera, erabilgarritasunari, egiazkotasunari, osotasunari, konfidentzialtasunari edo trazabilitateari kalte eginez.

- Informazioaren segurtasun-betekizunak zehazten ditu, maiatzaren 3ko 311/2022 Errege Dekretuaren I. eranskinean ezarritako

responsabilidad y se gestionan internamente.

- El Presidente o la presidenta del órgano colegiado Delegado de Protección de Datos, en representación del mismo, o el/la técnico/a jurídico/a de Presidencia que forme parte de dicho órgano en quien aquél delegue. Participará con voz pero sin voto. Actuará, a su vez, como Secretario del Comité.

La presidenta del Órgano Delegado de Protección de Datos. Participará con voz pero sin voto. Actuará, a su vez, como Secretario/a del Comité.

Las reuniones ordinarias del Comité de Seguridad de la Información tendrán una periodicidad semestral.

Podrán convocarse reuniones extraordinarias cada vez que las necesidades o las circunstancias así lo exijan.

7.3 Funciones de las Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación se detallan y se establecen las funciones y responsabilidades de cada una de las figuras:

La persona Responsable de Servicios:

- Efectúa las valoraciones de la categoría de seguridad de los servicios en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad

- El Responsable de la Información, determina los requisitos de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad ENS.

La persona Responsable de Información:

- Efectúa las valoraciones de la categoría de seguridad de la información en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

- Determina los requisitos de seguridad de la información dentro del marco establecido en el

esparruaren barruan, ENS segurtasun-arduradunak proposatu ondoren.

ENS segurtasun-arduraduna:

- Sistemaren segurtasun-kategoria zehazten du.
- Aplikagarritasun-adierazpena formalki onartzen du.
- Informazioaren eta zerbitzuen segurtasunaren arloan egin behar dela planifikatzen du, eta egin den ikuskatzen du.
-
- POC (harremanetarako puntua edo pertsona) gisa, zerbitzuen segurtasun-baldintzak, informazioaren segurtasunari buruzko komunikazioak eta zerbitzuen eremuko intzidenteen kudeaketa bideratzen eta gainbegiratzen ditu.
- Sistemaren arduraduna sistemaren eragiketen arduraduna da.

7.4 Informazioaren Segurtasuneko Batzordearen eginkizunak

Segurtasun Batzordeak eginkizun hauek izango ditu:

- Datuak babesteko araudia betetzeko beharrezkoak diren jarduerak egitea.
- Donostiako udalari informazioaren segurtasunaren eremuan dituzten kezkei erantzutea, eta Zuzendaritzari informazioaren segurtasunaren egoeraren berri ematea aldizka.
- Arduradunen eta/edo askotariko segurtasun rolen artean sor daitezkeen erantzukizun gatazkak ebaztea, eta kasuak goragokoei bidaltzea, erabakitzeko behar adinako aginpiderik ez duenean.
- Informazioaren segurtasuna kudeatzeko sistemaren etengabeko hobekuntza sustatzea. Horretarako, ekintza hauek egingo ditu:
  - Arloek informazioaren segurtasunaren eremuan egiten dituzten ahaleginak koordinatzea, eremu horretan erabakitako estrategiarekin bat etorriko

anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad ENS.

La persona Responsable de Seguridad ENS:

- Determina la categoría de seguridad del sistema.
- Aprueba formalmente la Declaración de Aplicabilidad.
- Planifica qué ha de hacerse en materia de seguridad de la información y los servicios y supervisa que se haya realizado.
- Como POC (punto o persona de contacto), canaliza y supervisa el cumplimiento de los requisitos de seguridad de los servicios, las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes en el ámbito de los servicios.
- La persona Responsable del Sistema, es el/la encargado/a de las operaciones del sistema.

7.4 Funciones del Comité de Seguridad de la Información

El Comité de Seguridad tendrá las siguientes funciones:

- Llevar a cabo las actuaciones necesarias para cumplir con la normativa de protección de datos.
- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas, informando regularmente del estado de la Seguridad de la Información a la Entidad.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes Roles de Seguridad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
  - Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la

direla ziurtatzeko eta bikoiztasunak saihesteko.	estrategia decidida en la materia, y evitar duplicidades.
◦ Informazioaren segurtasuna hobetzeko planak proposatzea, dagokion aurrekontu zuzkidurarekin, eta segurtasun arloko jarduerei lehentasuna ematea, baliabideak mugatuak direnean.	◦ Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
◦ Informazioaren segurtasuna proiektu guztietan kontuan hartzen dela zaintzea, hasierako zehaztapenetik hasi eta martxan jarri arte (PrivacybyDesign). Bereziki, bikoiztasunak murrizten dituzten eta IKT sistema guztien funtzionamendu homogeneoa bultzatzen duten zerbitzu horizontalak sortzen eta erabiltzen direla zaindu beharko du.	◦ Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación (PrivacybyDesign). En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
◦ Administrazioak bere gain hartutako hondar arrisku nagusien jarraipena egitea eta arrisku horien inguruan egin daitezkeen jarduerak gomendatzea.	◦ Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
◦ Segurtasun gorabeheren kudeaketaren jarraipena egitea eta horiei dagokienez egin daitezkeen jarduketak gomendatzea.	◦ Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
◦ Informazioaren segurtasun politika prestatu eta berrikustea, onar dadin.	◦ Elaborar y revisar la Política de Seguridad de la Información para su aprobación.
◦ Informazioaren segurtasunari buruzko araudia prestatzea, onar dadin.	◦ Elaborar la normativa de Seguridad de la Información para su aprobación.
◦ Arau Esparrua eguneratuta izatea, barne hartuta Informazioaren Segurtasunerako Politikaren Jarraibide Teknikoak, haren eranskin batean	◦ Mantener actualizado el “Marco Normativo” incluyendo las “Instrucción Técnicas de Seguridad”, de la Política de Seguridad de la Información en un anexo a la misma.
◦ Langileak informazioaren segurtasunaren arloan eta, bereziki, datu pertsonalen babesaren arloan prestatzeko eta sentsibilizatzeko prestakuntza programak prestatzea.	◦ Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información, y en particular en materia de protección de datos de carácter personal.
◦ SENaren eta datuak babesteko araudiaren aldizkako auditoretzak egin daitezen bultzatzea, Administrazioak informazioaren segurtasunaren arloan dituen betebeharrak betetzen direla egiaztatzeko.	◦ Promover la realización de las auditorías periódicas ENS y la normativa de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.
◦ Informazioaren segurtasunaren	◦ Informar del estado de seguridad de la

egoeraren berri ematea Zuzendaritzari.

información a la Dirección. 77

7.5 Izendatzeko prozedurak

Donostiako Udaleko Tokiko Gobernu Batzordeak batzordea osatu, berorren kideak izendatu eta erantzukizunak esleituko ditu. Izendapen guztiak 4 urtean behin edo lanpostuak hutsik geratzen direnean berrikusiko dira.

7.5 Procedimientos de designación

La Junta de Gobierno Local del Ayuntamiento de San Sebastián procederá a la constitución y designación de los miembros del comité y de las distintas responsabilidades. Todos los nombramientos se revisarán cada 4 años o cuando los puestos quedes vacantes.

8. DATU PERTSONALAK

Donostiako Udalak, datu pertsonalak biltzeko orduan, aintzat hartuko du egokiak eta baliagarriak diren, baina ez gehiegizkoak, eta horiek lortzearen xede den arloarekin eta helburuekin lotuta dauden, eta kasu horietan soilik bilduko ditu. Era berean, kasu bakoitzean indarrean dagoen Datuak Babesteko araudia betetzeko beharrezkoak diren neurri teknikoak eta antolakuntzako neurriak hartuko ditu.

8. DATOS DE CARÁCTER PERSONAL

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

9. INFORMAZIOAREN SEGURTASUN POLITIKA GARATZEA

Informazioaren Segurtasunerako Batzordeak kudeaketa sistema bat garatzea onartu beharko du. Sistema hori DonostiaTIKek ezarri, inplementatu, mantendu eta hobetuko du, segurtasun estandarren arabera. Sistema hori Segurtasun Eskema Nazionalera egokituko da eta haren kontrolak kudeatzeko balioko du. Sistema dokumentatu egingo da, eta aukera emango du kontrolen eta Batzordeak ezarritako helburuen betetze mailaren ebidentziak sortzeko. Dokumentuak kudeatzeko prozedura bat egongo da (00-PR), zeinak sistemaren segurtasuneko dokumentazioa egituratzeko, kudeatzeko eta eskuratzeko jarraibideak ezarriko baititu.

Informazioaren Segurtasunerako Batzordeari dagokio politika honen urteko berrikuspena egitea eta, hobetu behar izanez gero, Donostiako Udaleko Tokiko Gobernu Batzordeak onar dezan proposatzea.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información deberá aprobar el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad, mantenido y gestionado por DonostiaTIK. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental, 00-PR que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte de la Junta de Gobierno Local del Ayuntamiento de San Sebastián.

10. HIRUGARRENAK

Donostiako Udalak beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa erabiltzen duenean, Informazioaren Segurtasunerako Politika honen berri emango zaie erakunde horiei. Jakinarazpenetarako eta Informazioaren

10. TERCERAS PARTES

Cuando el Ayuntamiento de San Sebastián preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán canales para el reporte y la coordinación de los respectivos Comités de

Segurtasunerako Batzordeak koordinatzeko bideak ezarriko dira, eta segurtasun gorabeherak daudenean jarduteko prozedurak ezarriko dira.

Donostiako Udalak hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa lagatzen dienean, Segurtasun Politika honen eta zerbitzu edo informazio horiei dagokien Segurtasun Araudiaren berri emango zaie. Hirugarren alderdiak araudi horretan ezarritako betekizunak bete beharko ditu, eta bere prozedura operatiboak garatu ahal izango ditu hura betetzeko. Gorabeherak jakinarazi eta konpontzeko prozedura espezifikoak ezarriko dira. Bermatuko da hirugarrenen langileak informazioaren segurtasunaren arloan behar bezala kontzientziatuta daudela, gutxienez, Segurtasun Politika honetan ezarritako maila berean.

Segurtasun-politika horren alderdiren bat ezin badu bete heren batek aurreko paragrafoetan eskatzen denaren arabera, ENS segurtasun-arduradunaren txosten bat beharko da, arriskuak eta, hala badagokio, horiek tratatzeko modua zehazteko. Informazioaren eta Zerbitzuek arduradunek txosten hori aztertu eta baloratu beharko dute, organo eskudunak onartu baino lehen, hala badagokio.

Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando el Ayuntamiento Donostia / San Sebastián utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha 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 está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad ENS que precise los riesgos en que se incurre y en su caso la forma de tratarlos. Se requerirá el análisis y posterior valoración de este informe por parte de las personas responsables de Información y Servicios antes de su aprobación en su caso por el órgano competente.

GOBERNANTZA IREKI, DIGITAL ETA KOLABORATIBOKO ZINEGOTZI ORDEZKARIA

Ana López Loyarte