Índice

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN 3
3. MISIÓN DE DONOSTIA KULTURA 4
4. ALCANCE 4
5. MARCO NORMATIVO 4
6. CUMPLIMIENTO DE ARTÍCULOS 7
7. ORGANIZACIÓN DE LA SEGURIDAD 12
   7.1 Roles de Seguridad de la Información 12
   7.2 Comité de Seguridad de la Información 12
   7.3 Funciones de las Responsabilidades asociadas al Esquema Nacional de Seguridad 13
   7.4 Funciones del Comité de Seguridad de la Información 15
   7.5 Procedimientos de designación 17
8. DATOS DE CARÁCTER PERSONAL 17
9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 17
10. TERCERAS PARTES 18
11. COORDINACIÓN E INTERPRETACIÓN 18

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 3 noviembre de 2026 por la Dirección de Donostia Kultura.

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

Esta Política se enmarca en integra con la Política de Seguridad de la Información del Ayuntamiento de Donostia/San Sebastián, al ser Donostia Kultura una Entidad Pública Empresarial dependiente del Ayuntamiento, por lo que su regulación se adapta a lo allí recogido con las pertinentes adaptaciones singulares propias del Organismo.

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 311/2022 de 3 de mayo, 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, Donostia Kultura, de acuerdo con los fines que le han sido atribuidos en los Estatutos del organismo y 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 de Donostia Kultura, 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 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 Donostia Kultura 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, acorde a lo establecido en el Artículo 7 del ENS.

3. MISIÓN DE DONOSTIA KULTURA

Desarrollar de forma directa y descentralizada las competencias municipales en materia de Cultura y Festejos. Le compete en consecuencia la planificación, construcción y gestión del ámbito cultural de competencia del Ayuntamiento de Donostia-San Sebastián, así como la promoción y organización de actividades festivas.

4. ALCANCE

Esta Política se aplicará a los sistemas de información municipales, relacionados con las funciones del apartado 3. MISIÓN DE DONOSTIA KULTURA".

Todos los miembros de Donostia Kultura 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. MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de Donostia Kultura y, en particular, la prestación de sus servicios electrónicos, está integrado por las siguientes normas:

- Real Decreto 311/2022 Real, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad 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.
- 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.
- 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.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Artículo 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- 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).
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- 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.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- 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.
- 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.

- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- 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.
- 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.
- Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.
- 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.
- 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.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza en la materia.
- Real Decreto-ley 24/2021: modificación de la Ley 9/2017 y del Real Decreto-ley 3/2020.
- 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.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- 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.
- Ley 2/2016, de 7 de abril, de Instituciones Locales de Euskadi.
- DECRETO 55/2020, de 21 de abril, de segunda modificación del Decreto de Administración Electrónica., - Boletín Oficial del Pais Vasco, de 30-04-2020.
- 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.

- 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.

- REGLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial)

- Y por toda la demás legislación que resulte de aplicación, como la Ley de Patrimonio Histórico, de Protección de la Propiedad Intelectual etc.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica derivadas de las anteriores y publicadas en las sedes electrónica comprendidas dentro del ámbito de aplicación de de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad de la Información, será coherente con las modificaciones de la Política de Seguridad de la Información del Ayuntamiento de Donostia y se mantendrá en un Anexo a este documento, hasta que proceda a la actualización de la Política de Seguridad. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento publicadas por el órgano con competencias en la materia, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad”.

Así mismo, el Comité también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. CUMPLIMIENTO DE ARTÍCULOS

Donostia Kultura 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 en el ámbito de la administración electrónica, que recoge 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.

Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, 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 no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) 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.

Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 20)

Donostia Kultura ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de seguridad de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 14) y profesionalidad (artículo 15)

Todos los miembros de Donostia Kultura, que se encuentran dentro del ámbito del ENS, recibirán acciones de concienciación en materia de seguridad. Se establecerá un programa de concienciación continua para atender a todos los miembros de Donostia Kultura, en particular al de nueva incorporación.

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 realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad de la Información ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

- El proceso de gestión de riesgos comprenderá las siguientes fases:
- Categorización de los sistemas.
- Análisis de riesgos.

El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)

Donostia Kultura ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas

y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, Donostia Kultura implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.

Donostia Kultura establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente.
- Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Para garantizar la disponibilidad de los servicios, Donostia Kultura dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)

El Donostia Kultura ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.

a) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)

Donostia Kultura ha organizado su seguridad comprometiendo a todos los miembros de 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.

Autorización y control de los accesos (artículo 16)

Donostia Kultura ha implementado mecanismos de control de acceso al sistema de información, limitándoos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 17)

Donostia Kultura ha implementado mecanismo 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.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)

Donostia Kultura tendrá en cuenta, para la adquisición de productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)

Donostia Kultura ha implementado mecanismos para proteger la información almacenado o en tránsito especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

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

También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias. De igual modo, se han implementado mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren, para garantizar que toda información en soporte no electrónico relacionada, estará protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 23)

Donostia Kultura habilitará los registros de la actividad de los usuarios, que se consideren necesarios, reteniendo la información necesaria para monitorizar, analizar,

investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente 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.

¬ **Mejora continua del proceso de seguridad (artículo 26)**

Donostia Kultura actualizará y mejorará de forma continua el proceso de seguridad integral implantado, aplicando los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de las tecnologías de la información.

7. ORGANIZACIÓN DE LA SEGURIDAD

La estructura organizativa de la Seguridad de la Información en Donostia Kultura se establece en la forma que se indica a continuación.

7.1 Roles de Seguridad de la Información

Donostia Kultura ha organizado la seguridad mediante la designación de los siguientes roles de seguridad.

- ¬ Responsable de Información y Responsable de los Servicios: responsabilidades que serán asumidas por la Dirección-Gerencia.
- ¬ Responsable de Seguridad de la Información: El / la Director/a del Área de Administración y Recursos de la Entidad Pública Empresarial Donostia Kultura.
- ¬ Responsable del Sistema: El / la Informático/a de Administración y Recursos.

7.2 Comité de Seguridad de la Información

Se constituye el órgano colegiado Comité de Seguridad de la Información, como órgano resolutivo, de Donostia Kultura, que estará formado por los siguientes:

¬ Presidente/a: El / la Director-Gerente de la Entidad Pública Empresarial Donostia Kultura.
¬ Secretario/a: El / la Director/a del Área de Administración y Recursos de la Entidad Pública Empresarial Donostia Kultura.
¬ Responsable de Seguridad de la Información: El / la Director/a del Área de Administración y Recursos de la Entidad Pública Empresarial Donostia Kultura.
¬ Responsable del Sistema: El / la Informático/a de Administración y Recursos.
¬ Interlocutor/a del Delegado/a de Protección de Datos: El / la técnico/a jurídico de la Entidad Públioca Empresarial Donostia Kultura.

Este interlocutor/a del Delegado de Protección de Datos participará con voz, pero sin voto en las reuniones del Comité de seguridad de la información cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un

asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

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:

- **Responsable de la Información y de los Servicios,** sus funciones serán:
  - Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, pudiéndose recabar un propuesta al Responsable de Seguridad ENS, y escuchando la opinión del Responsable del Sistema.
  - Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- **Responsable de Seguridad de la Información,** determina las decisiones para satisfacer los requisitos de seguridad de la Información y Servicios. Sus principales funciones son:
  - Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.
  - Promover la formación y concienciación en materia de seguridad de la información.
  - Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
  - Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
  - Promover la realización del análisis de riesgos.

- Aprobar formalmente la Declaración de Aplicabilidad.
- Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue. Estas herramientas se analizarán y desplegarán en coordinación con el ayuntamiento de San Sebastián.
- En lo que respecta a las incidentes de seguridad:
  - Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia, en particular con el CCN y la AEPD.
  - Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
  - Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
  - Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

- **Responsable del Sistema**, sus funciones serán:
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
  - Elaborando los procedimientos operativos necesarios.
  - Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
  - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
  - Proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. La decisión final, que será tomada por la dirección de la entidad, debe ser acordada con los responsables de la información y los servicios afectados y el Responsable de la Seguridad de la Información.
  - Determinará y aprobará formalmente la categorización del sistema o sistemas, en base a la valoración de los Servicios e Información ENS, tal y como se establece en el anexo I del Real Decreto ENS, realizada por los Responsables de Información ENS y Responsables de Servicios ENS.
  - Llevará a cabo las funciones del administrador de la seguridad del sistema:

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- La gestión de las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- La aplicación de los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son adecuadamente observados.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

  Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

  En la gestión de incidentes de seguridad (ciberincidentes) podrá, de acuerdo con el Responsable de la Seguridad, suspender de forma cautelar y urgente el tratamiento de la información y la prestación de los servicios como medida de contención. Dicha suspensión deberá ser comunicada al Titular de la entidad y a los responsables de la información y del servicio y, en caso de afección a datos personales al Delegado de Protección de Datos y si afecta a la tramitación administrativa, a los (servicios jurídicos del ayuntamiento) de la organización, en su caso, proceder a la suspensión de los plazos.

7.4 Funciones del Comité de Seguridad de la Información

Serán funciones del Comité de Seguridad de la Información:

- 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 Dirección.
- 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.
- Asumir las funciones del Responsable de la Información y del Responsable del Servicio.
- Coordinarse con el Comité de Seguridad de la Información del Ayuntamiento de Donostia/San Sebastián en la consecución de los objetivos y fines definidos en los Estatutos de Donostia Kultura y en la actualización y mantenimiento de esta Política, así como en la emisión de los criterios comunes de aplicación de la misma que pudiesen incidir en la seguridad de la información municipal.
- 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 estrategia decidida en la materia, y evitar duplicidades.
    - 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.
    - 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.
    - Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - Elaborar y revisar la Política de Seguridad de la Información para su aprobación.
    - Elaborar la normativa de Seguridad de la Información para su aprobación.

- Mantener actualizado el “Marco Normativo” incluido las “Instrucción Técnicas de Seguridad”, de la Política de Seguridad de la Información en un anexo a la
- Identificar las Guías de seguridad CCN que son de aplicación al sistema.
- 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.
- 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.
- Informar del estado de seguridad de la información a la Dirección.

7.5 Procedimientos de designación

La Dirección de Donostia Kultura procederá a la constitución del comité y a la designación de las distintas responsabilidades y roles de seguridad. Todos los nombramientos se revisarán cada 4 años o cuando los puestos quedes vacantes.

8. DATOS DE CARÁCTER PERSONAL

Donostia Kultura 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. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles de seguridad del Esquema Nacional de Seguridad que son de aplicación a Donostia Kultura, así como al Ayuntamiento de Donostia/San Sebastián. 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 “Procedimiento de Gestión de la Documentación”, 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 al menos, anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte de la Dirección de Donostia Kultura.

10. TERCERAS PARTES

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

Cuando Donostia Kultura 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 la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11. COORDINACIÓN E INTERPRETACIÓN

En el desarrollo de las actuaciones contenidas en la Política, Donostia Kultura a través de su Comité de Seguridad de la Información, actuará coordinadamente con el Ayuntamiento de Donostia/San Sebastián, en el ejercicio de sus funciones.

El Comité de Seguridad de la Información podrá dictar criterios interpretativos sobre la aplicación de la misma. En el supuesto de que estos criterios de aplicación fuesen contradictorios con los de la Política del Ayuntamiento, prevalecerán estos últimos para una correcta aplicación coordinada de ambas Políticas, en la consecución de los fines del organismo.

Esta Política, así como sus sucesivas modificaciones se comunicarán al Ayuntamiento, por medio de sus Comités de Seguridad de la Información, al efecto de evitar una aplicación incongruente con la establecida en la Política de Seguridad del Ayuntamiento, como marco general de la seguridad de la información municipal.