PROPIEDADES DEL DOCUMENTO

FECHA DE CREACIÓN:	04/10/19	**CLASIFICACIÓN DOCUMENTO:**	Uso oficial - Interno

CONTROL DE FIRMAS

	FECHA	FIRMA
ELABORADO POR: Responsable de Seguridad	19/04/24	
APROBADO POR: Comité de Seguridad	15/07/24	

HISTORIAL DE VERSIONES

VERSIÓN	FECHA	AUTOR	CAMBIOS
1.0	04/10/19	Responsable de Seguridad	Versión inicial del documento
1.1	27/01/22	Responsable de Seguridad	Inclusión de la “Oficina de CiberSeguridad y Cumplimiento Normativo” Cambio en la periodicidad de las reuniones. Actualización del marco normativo Otros cambios
1.2	19/04/24	Responsable de Seguridad	Adaptación al RD 311/2022, del 3 de mayo, por el que se regula el ENS.

Índice

1. APROBACIÓN Y ENTRADA EN VIGOR....3
2. INTRODUCCIÓN....3
3. MISIÓN DE DONOSTIATIK....4
4. ALCANCE....4
5. MARCO NORMATIVO....5
6. CUMPLIMIENTO DE ARTÍCULOS....8
7. ORGANIZACIÓN DE LA SEGURIDAD....13
7.1 Roles de Seguridad de la Información....13
7.2 Comité de Seguridad de la Información....13
7.3 Oficina de CiberSeguridad y Cumplimiento Normativo....14
7.4 Funciones de las Responsabilidades asociadas al Esquema Nacional de Seguridad....14
7.5 Funciones del Comité de Seguridad de la Información....17
7.6 Procedimientos de designación....18
8. ESTRUCTURA DE LA DOCUMENTACIÓN....19
9. DATOS DE CARÁCTER PERSONAL....19
10. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN....19
11. TERCERAS PARTES....19
12. COORDINACIÓN E INTERPRETACIÓN....20

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 09 de Octubre de 2019 por la Dirección de DonostiaTIK.

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 DonostiaTIK un Organismo Autónomo Local 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, DonostiaTIK, 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 DonostiaTIK, 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 DonostiaTIK, 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 8 del ENS.

3. MISIÓN DE DONOSTIATIK

El objetivo de DonostiaTIK es ofrecer servicios tecnológicos de calidad: informáticos, de telecomunicaciones o cualquiera otros, mediante soluciones integrales y homogéneas tanto a la organización municipal para mejorar los servicios que se prestan a la ciudadanía, como a la ciudadanía donostiarra.

Para conseguir estos objetivos, DonostiaTIK asume la gestión y realización de los siguientes servicios y actividades al Ayuntamiento de Donostia – San Sebastián, y a los Organismos Públicos y Sociedades dependientes del mismo:

- Aplicación de los procedimientos informáticos.
- Gestión integral de las comunicaciones de voz y datos.
- Creación y explotación del Centro de Proceso de Datos, con las debidas garantías de independencia, custodia de datos y cualificación.
- Contratación de servicios de telecomunicaciones y aplicaciones informáticas completas, programas, equipos, asesores y cualquier elemento, material y humano, necesario para completar la capacidad del CPD o mejorar su efectividad.
- Implantación de servicios de telecomunicaciones e informáticos.
- Celebración de convenios de colaboración o de prestación de servicios.
- Investigación, asesoramiento y formación en diversos aspectos que presten las telecomunicaciones y la informática aplicadas a la actividad municipal.
- Cualquier servicio o actividad relacionado con los anteriores.

4. ALCANCE

Esta Política se aplicará a los sistemas de información municipales gestionados por DonostiaTIK, que proporciona servicios y actividades al Ayuntamiento de Donostia/San Sebastián, sus Organismos Autónomos y Sociedades dependientes, en cumplimiento de los fines con lo que ha sido creado el organismo según consta en el artículo 7 de sus estatutos, y relacionadas con sus funciones del apartado 2. "MISIÓN DE DONOSTIATIK".

Todos los miembros de DonostiaTIK 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 DonostiaTIK y, en particular, la prestación de sus servicios electrónicos, está integrado por las siguientes normas:

- 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.
- 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.
- 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-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- 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.
- 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.
- Ley 2/2016, de 7 de abril, de Instituciones Locales de Euskadi.
- Norma Foral 4/2019, de 11 de marzo, de Buen Gobierno en el marco de la gobernanza pública foral.
- 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.
- 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.
- 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 Esquema Nacional de Seguridad.

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

6. CUMPLIMIENTO DE ARTÍCULOS

DonostiaTIK para lograr el cumplimiento de los artículos del Real Decreto 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 y mínimo privilegio

La seguridad se entenderá 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 a DonostiaTIK, estará presidida por este principio, que 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.

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

La vigilancia continua por parte de DonostiaTIK 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 de DonostiaTIK, que se encuentran 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 dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

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.

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.

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

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

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.

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.

Incidentes de seguridad, prevención, detección, reacción y recuperación

DonostiaTIK dispone de procedimientos de gestión de incidentes de seguridad y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

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 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

DonostiaTIK 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 de las capas 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 de la entidad 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.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

DonostiaTIK 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.

Autorización y control de los accesos

DonostiaTIK ha implementado mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

DonostiaTIK 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

Para la adquisición de productos o contratación de servicios de seguridad DonostiaTIK 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.

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

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

DonostiaTIK 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.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

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.

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.

Registros de actividad y detección de código dañino

DonostiaTIK 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 usuarios, 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.

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, la entidad 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.

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.

Infraestructura y servicios comunes

DonostiaTIK 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.

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

DonostiaTIK tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos que sean de aplicación.

7. ORGANIZACIÓN DE LA SEGURIDAD

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

7.1 Roles de Seguridad de la Información

DonostiaTIK 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 el Comité de Seguridad de la Información.
- Responsable de Seguridad de la Información: Jefe de Servicios de DonostiaTIK.
- Responsable del Sistema: Jefa de Producción del DonostiaTIK.
- POC (punto o persona de contacto) : Jefe de Servicios de DonostiaTIK

7.2 Comité de Seguridad de la Información

DonostiaTIK ha constituido un Comité de Seguridad de la Información, como órgano resolutorio, de coordinación y cooperación con el Comité de Seguridad de la Información del Ayuntamiento de Donostia/San Sebastián, con la siguiente composición:

- Presidente: Director-Gerente de DonostiaTIK.
- Secretaria: Interlocutora del Delegado/a de Protección de Datos

Miembros:

- Responsable de Seguridad de la Información: Jefe de Servicios de DonostiaTIK.
- Responsable del Sistema: Jefa de Producción del DonostiaTIK.
- Interlocutora del Delegado/a de Protección de Datos: Secretaría Técnico de DonostiaTIK.

Esta interlocutora 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.

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 Oficina de CiberSeguridad y Cumplimiento Normativo

DonostiaTIK ha constituido una Oficina de CiberSeguridad y Cumplimiento Normativo, funcionando una comisión asesora y de trabajo con el objeto de servir de apoyo para el desempeño de las funciones y responsabilidades de los diferentes roles de seguridad, que estará compuesta por los siguientes:

- Responsable de Seguridad de la Información
- Responsable del Sistema
- Dos Técnicos de Sistemas en Ciberseguridad.
- Un Técnico de Gestión y Desarrollo de Proyectos Informáticos, Seguridad y Calidad.

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

Esta Oficina se reunirá al menos semestralmente. Los acuerdos adoptados, se plasmarán en actas que serán trasladados al Presidente del Comité de Seguridad de la Información para su conocimiento.

7.4 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:
  - Efectuar las valoraciones de la categoría de seguridad en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

- 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:
  - Determinar la categoría de seguridad del sistema
  - 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.
  - Como POC (punto o persona de contacto):
    - Canalizar y supervisar tanto el cumplimiento de los requisitos de seguridad de los servicios que presta, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes en el ámbito de dichos servicios.
  - 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 AVPD.
    - 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.

7.5 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 DonostiaTIK 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.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Mantener actualizado el “Marco Normativo” de la Política de Seguridad de la Información.
- 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.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- 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.
- Renovación

7.6 Procedimientos de designación

La Dirección de DonostiaTIK 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. ESTRUCTURA DE LA DOCUMENTACIÓN

DonostiaTIK dispone de un procedimiento documentado en el que se establecer el método de elaboración, revisión, aprobación, actualización, identificación, distribución, control y archivo de los documentos del Sistema de Gestión que dan cumplimiento al ENS (SGENS), en el Ayuntamiento de Donostia-San Sebastián y DonostiaTIK.

9. DATOS DE CARÁCTER PERSONAL

DonostiaTIK 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.

10. 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 DonostiaTIK, 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 DonostiaTIK.

11. TERCERAS PARTES

Cuando DonostiaTIK 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 DonostiaTIK 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.

De igual modo, los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

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.

12. COORDINACIÓN E INTERPRETACIÓN

En el desarrollo de las actuaciones contenidas en la Política, DonostiaTIK 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.