Junta de Andalucía

Política de Seguridad de la Información

Empresa Pública para la Gestión del Turismo y del Deporte de Andalucía

Publicado

19 de marzo del 2024

Control de Firmas

HOJA DE CONTROL DE LA DOCUMENTACIÓN					
Código	SI-PSI-01	Edición	2.1	Tipo	Interno
Título	Política de Seguridad de la Información				
Elaborado	CONSTA EN EL ORIGINAL	Consultor Externo			
Revisado	CONSTA EN EL ORIGINAL	Consultor Externo			
Revisión EPTDA	CONSTA EN EL ORIGINAL	Responsable Área de Sistemas			
Conforme	CONSTA EN EL ORIGINAL	COO Directora de Operaciones			
Validado	CONSTA EN EL ORIGINAL	COO Directora de Operaciones			
Aprobado	CONSTA EN EL ORIGINAL	CEO Director Gerente			
Departamento	IT				
Palabras clave	Política Seguridad, ENS				

CAMBIOS RESPECTO A LA REVISIÓN ANTERIOR
Actualización de cargos con nuevo organigrama de Turismo y Deporte de Andalucía

Índice

1. Introducción

Este documento constituye la Política de Seguridad de la Información de la Empresa Pública para la Gestión del Turismo y del Deporte de Andalucía S.A., en lo sucesivo, **Turismo y Deporte de Andalucía**, en cumplimiento del artículo 12 (Política de seguridad y requisitos mínimos de seguridad) 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 y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 12 establece que "Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente".

De acuerdo con este mandato, la Junta de Andalucía aprobó el Decreto 1/2011, de 11 de enero, por el que se establece la Política de seguridad de las TIC de la Junta, que fue modificado por el Decreto 70/2017, de 6 de junio, que incluye a las entidades instrumentales en su ámbito de aplicación. En su artículo 10 señala que "cada Consejería y entidad instrumental debe disponer formalmente de su propio documento de política de seguridad TIC, así como de las disposiciones de desarrollo que adecúen las directrices comunes a sus particularidades". Por ello, se publicó la Orden de 15 de noviembre de 2023, por la que se establece la política de seguridad de la Consejería de Turismo, Cultura y Deporte en los ámbitos de seguridad interior, seguridad de las tecnologías de la información y comunicaciones y de la protección de datos.

Turismo y Deporte de Andalucía, conforme a los requisitos indicados por el Esquema Nacional de Seguridad, y siguiendo las pautas de la política de seguridad de la Consejería de Turismo, Cultura y Deporte, de la que depende, presenta esta política de seguridad.

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805 para la redacción de la Política de Seguridad en el ámbito del Esquema Nacional de Seguridad. La Política de Seguridad de la Información recoge la postura de **Turismo y Deporte de Andalucía** en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad.

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 y reaccionando con presteza a los incidentes.

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, en adelante ENS y la legislación vigente en materia de Protección de Datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Turismo y Deporte de Andalucía, debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida de los sistemas de información, 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.

Turismo y Deporte de Andalucía, debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

2. Objeto

La presente Política de Seguridad de la Información expresa el compromiso de la **Dirección de Turismo y Deporte de Andalucía** con la gestión de la seguridad de la información en general y, particularmente, con la de los sistemas de información.

La Política pretende, en definitiva, dirigir y dar soporte a la gestión de la seguridad de la información mediante el establecimiento de una estructura organizativa en la que se apoyará el gobierno de la seguridad, así como de unas directrices básicas de acuerdo a los requisitos propios de seguridad y a la regulación aplicable, constituyéndose en el marco dentro del que se definirá el conjunto de normas reguladoras, procedimientos y prácticas que determinen el modo en que los activos son gestionados, protegidos y distribuidos.

3. Alcance y Ámbito de Aplicación

Con arreglo a lo expresado en el artículo 1 del Decreto 1/2011, de 11 de enero, y en el Decreto 70/2017, de 6 de junio, que lo modifica, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, y la Orden de 15 de noviembre de 2023, por la que se establece la política de seguridad de la Consejería de Turismo, Cultura y Deporte en los ámbitos de seguridad interior, seguridad de las tecnologías de la información y comunicaciones y de la protección de datos personales, esta política se aplica a todos los sistemas TIC de **Turismo y Deporte de Andalucía** y a todos los miembros de la organización, así como a aquellas personas u organizaciones que presten servicios a la organización, sin excepciones.

Por tanto, será de obligado cumplimiento para todo el personal en la utilización de medios digitales en el ámbito de actuación de la organización, la información en soporte papel que gestione en el ámbito de sus competencias, así como para toda persona que acceda tanto a los Sistemas TIC como a la propia información que sea gestionada por **Turismo y Deporte de Andalucía**, con independencia de cuál sea su destino, adscripción o relación con esta.

4. Misión y Objetivos

Turismo y Deporte de Andalucía asume como misión la realización de actividades y servicios tendentes a la mejora y crecimiento de la industria turística y del deporte, a cuyo fin desarrollará principalmente las siguientes acciones:

- La realización de actuaciones orientadas al crecimiento y desarrollo de la industria turística y del deporte en todos sus aspectos.
- La gestión de las Instalaciones turísticas o deportivas adscritas a la Consejería competente en materia de turismo y deporte, conforme al régimen de encomiendas previsto en el artículo 106 de la Ley 9/2007, de 22 de octubre, así como la elaboración de planes, ejecución de obras y trabajos que resulten necesarios para la mejor explotación de las mismas.
- La elaboración de estudios, planes y proyectos relacionados con las materias de turismo y deporte.

- La realización de todo tipo de actuaciones, obras y trabajos para la conservación y transformación de los recursos e instalaciones turísticas, así como la ejecución de obras de instalaciones y equipamientos deportivos.
- La gestión y explotación de bienes inmuebles y servicios afectos al uso turístico o deportivo.
- La realización de cuantas actividades se estime convenientes para la mejora y crecimiento de la oferta turística en sentido estricto, así como de la oferta complementaria, efectuando campañas publicitarias con los medios y bajo la forma adecuada en cada caso.
- La organización de actividades deportivas y la difusión del deporte en Andalucía.
- La investigación y el análisis de nuevos productos turísticos y deportivos.
- La edición de todo tipo de material promocional, en cualquiera de los soportes que se estimen oportunos.
- La producción y la distribución de la información que favorezca al desarrollo turístico o deportivo andaluz.
- La realización de las acciones promocionales en colaboración y coordinación con otras entidades, públicas o privadas, que tengan análogos fines, en el marco de la política turística o deportiva general.
- La gestión del Fondo de Apoyo a las Pymes turísticas y comerciales y la suscripción y formalización de los acuerdos, convenios y contratos que resulten necesarios para su ejecución, en el marco de las directrices establecidas de conformidad con lo dispuesto en la normativa que sobre el particular resultare de aplicación en cada momento.
- La gestión y explotación, directa o indirecta, de hoteles escuela u otros establecimientos o instalaciones de hostelería o restauración en los que se desarrollen o impartan actividades formativas relacionadas con dicho sector productivo.

En consecuencia, **Turismo y Deporte de Andalucía** asume como misión cuantas actividades contribuyan al desarrollo turístico o del deporte en la Comunidad Autónoma de Andalucía.

5. Legislación y Normativa Aplicable

Para la elaboración del contenido de la presente política de seguridad se ha tenido en consideración entre otras, la siguiente legislación:

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del 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.
- 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.
- Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Decreto 70/2017, de 6 de junio, por el que se modifica el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.
- 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 que traspone la Directiva Europea NIS, Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.
- Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional.

- 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.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.
- 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.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Las normas aplicables a la administración electrónica y seguridad de la información que complementen, desarrollen o sustituyan a las anteriores y que se encuentren dentro del ámbito de aplicación de la política de seguridad de la información de **Turismo y Deporte de Andalucía**.

En materia de protección de datos:

- 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, en adelante RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (en adelante LOPDGDD).
- Dictámenes, informes, guías y recomendaciones de la Agencia Española de Protección de Datos.

También se han tenido en cuenta:

- Normas y estándares sobre Seguridad de la Información, en especial la última versión vigente de las normas ISO/IEC 27001 e ISO 27002.
- Las Guías CCN-STIC y en concreto, la serie 800, que establecen un proceso de construcción de un sistema de gestión basado en la mejora continua (Ciclo de Demming o modelo PDCA) sobre los requisitos específicos del ENS.

6. Principios Rectores de la Política de Seguridad

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información, y, por tanto, la presente política de seguridad se establece de acuerdo los siguientes principios:

a) **Seguridad como proceso integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

b) **Gestión de la seguridad basada en los riesgos**: De acuerdo con lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 7 del Real Decreto 311/2022, de 3 de mayo, el análisis y gestión de riesgos será parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

c) **Prevención, detección, respuesta y conservación**: La normativa que desarrolla la presente Política de Seguridad, contemplará acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar las vulnerabilidades de la Organización y lograr que las amenazas sobre la misma no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

d) **Existencia de líneas de defensa**: El sistema de información de la Organización dispondrá de una estrategia de protección constituida por múltiples capas de seguridad, constituidas por medidas de naturaleza organizativa, física y lógica.

e) **Vigilancia continua y reevaluación periódica**: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido, dedicado y diferenciado.

f) **Diferenciación de responsabilidades**: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad. En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

7. Requisitos mínimos de seguridad

Esta política de seguridad se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos exigidos en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, cumpliendo con lo establecido en el artículo 28 del ENS:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal.
- Profesionalidad.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Adquisición de productos de seguridad y contratación de servicios de seguridad.
- Mínimo privilegio.
- Integridad y actualización del sistema.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de la actividad y detección del código dañino.
- Incidentes de seguridad.
- Continuidad de la actividad.
- Mejora continua del proceso de seguridad.

8. Estructura normativa y desarrollo de la Política de Seguridad

En cumplimiento con lo dispuesto en la legislación aplicable, esta Política de Seguridad de la Información ha de ser objeto de desarrollo para que queden perfectamente definidas las medidas de seguridad específicas para los distintos ámbitos contemplados en el apartado 'Legislación y Normativa Aplicable' de este documento. En todo caso, las diferentes políticas, normativas y regulaciones específicas que resulten de tal desarrollo deberán respetar lo dispuesto en la presente Política de Seguridad y derivarse de la misma.

De acuerdo con lo anterior, **Turismo y Deporte de Andalucía** establecerá un marco normativo propio en materia de seguridad, estructurado en diferentes niveles, a fin de garantizar que los objetivos y medidas establecidos en el presente documento tengan un desarrollo específico.

La estructura jerárquica de la documentación de seguridad es la siguiente:

Documento	Detalle
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. • Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	• Determina las acciones o tareas a realizar en el desempeño de un proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. • Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad.

Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.
Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. • Deben ser aprobadas por el Responsable de Seguridad.

En la guía CCN-STIC-801 Responsabilidades y Funciones, se detalla el esquema de las principales responsabilidades (quien debe elaborarlo y quién aprobarlo) para cada uno de estos documentos.

La Normativa de Seguridad estará a disposición de todos los miembros de la Institución que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Turismo y Deporte de Andalucía, en cumplimiento con el 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, atenderá, en base a su cuerpo normativo, al cumplimiento de los siguientes artículos:

Artículo 13. Organización e implantación del proceso de seguridad.

La política de seguridad de **Turismo y Deporte de Andalucía** compromete a todos los miembros de la Organización, es conocida por todos e identifica los responsables de velar por su cumplimiento.

Artículo 14. Análisis y gestión de los riesgos.

Turismo y Deporte de Andalucía analiza y gestiona los riesgos por medio del análisis y tratamiento de estos empleando metodología MAGERIT adoptando las medidas necesarias para mitigar o suprimir los riesgos existiendo proporcionalidad entre ellas y estos.

Artículo 15. Gestión de personal.

Turismo y Deporte de Andalucía a través de su personal, y en base a su plan de formación y concienciación, aplica los principios de seguridad en el desempeño de su cometido. Todo el personal relacionado con la información y los sistemas es formado e informado de sus deberes y obligaciones en materia de seguridad a través de su cuerpo normativo, pudiendo supervisar sus acciones y asegurar su cumplimiento.

Artículo 16. Profesionalidad.

Turismo y Deporte de Andalucía garantiza la seguridad de las tecnologías de la información aplicables a los sistemas y servicios prestados en base a personal cualificado, garantizando su supervisión, atención y revisión mediante la ejecución de auditorías periódicas y la evaluación y gestión de los servicios recibidos.

Artículo 17. Autorización y control de los accesos.

Turismo y Deporte de Andalucía establece las medidas técnicas y organizativas necesarias para asegurar el control de acceso a sus sistemas de información, controlando y limitado las autorizaciones y el acceso a sus funciones.

Artículo 18. Protección de las instalaciones.

Turismo y Deporte de Andalucía dispone de los medios técnicos y organizativos necesarios de forma que garantiza la debida protección de sus instalaciones.

Artículo 19. Adquisición de productos de seguridad y contratación de servicios de seguridad.

Turismo y Deporte de Andalucía valora positivamente aquellos productos y servicios de seguridad que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

Artículo 20. Mínimo privilegio.

Turismo y Deporte de Andalucía aplica el principio de mínimo privilegio en sus sistemas de forma que proporcionan la mínima funcionalidad requerida en función de los requisitos exigidos en cada caso.

Artículo 21. Integridad y actualización del sistema.

Turismo y Deporte de Andalucía, atendiendo a su cuerpo normativo, requiere la autorización formal para la gestión del cambio y, en caso de ser necesario, para la gestión de la configuración.

Artículo 22. Protección de información almacenada y en tránsito.

Turismo y Deporte de Andalucía establece mediante su normativa los principios de clasificación de la información, así como la gestión, protección y uso de la misma.

Artículo 23. Prevención ante otros sistemas de información interconectados.

Turismo y Deporte de Andalucía mantiene gestionadas las redes de comunicaciones conforme a las especificaciones del servicio analizando en caso de ser necesario los riesgos derivados de la interconexión de sistemas a través de las mismas.

Artículo 24. Registro de actividad y detección de código dañino.

Turismo y Deporte de Andalucía, en cumplimiento con la Ley y la Normativa vigente, dispone de los registros de actividad requeridos por estas de manera que se pueda monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas.

Artículo 25. Incidentes de seguridad.

Turismo y Deporte de Andalucía, a través de su normativa, establece las pautas a seguir para la gestión y resolución de incidentes.

Artículo 26. Continuidad de la actividad.

Turismo y Deporte de Andalucía establece los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

Artículo 27. Mejora continua del proceso de seguridad.

Turismo y Deporte de Andalucía, atendiendo al nivel de compromiso adquirido con la seguridad, se encuentra inmerso en un proceso de mejora continua.

Artículo 28. Cumplimiento de los requisitos mínimos.

Turismo y Deporte de Andalucía adopta las medidas y refuerzos de seguridad que le corresponden según en el Anexo II del ENS.

9. Organización de la Seguridad

9.1 Definición de Roles

Tal como indica el artículo 13 del ENS, la seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.

La Política de Seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 del ENS y según se detalla en la sección 3.1 del anexo II del mismo, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento.

La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

Rol	Funciones
Dirección	Órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.
Comité de Seguridad	Órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos marcados por los órganos de gobierno.
Responsable de la Información	Tiene la responsabilidad de determinar los requisitos de seguridad de la información sobre la que es responsable.
Responsable de Servicio	Tiene la responsabilidad de determinar los requisitos de seguridad de los servicios sobre los que es responsable.
Responsable de Seguridad	Determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisando la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos y reportará sobre estas cuestiones al Comité de Seguridad de la Información.
Responsable del Sistema	Se encarga de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.
Administradores del Sistema	Son las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

9.2 Jerarquía en el proceso de decisiones y mecanismos de coordinación y resolución de conflictos

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el Comité de Seguridad de la Información da instrucciones al Responsable de la Seguridad de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la Organización.

El Responsable del Sistema:

- Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El Responsable de la Seguridad:

- Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad de la Información, como secretario:
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

- Da cuenta a la Junta de Gobierno Local, según lo acordado en el Comité de Seguridad de la Información.
    - Resumen consolidado de actuaciones en materia de seguridad.
    - Resumen consolidado de incidentes relativos a la seguridad de la información.
    - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.

9.3 Procedimiento de designación

La Dirección de la Organización nombrará formalmente mediante acta al efecto:

- A los Responsables de la Información.
- A los Responsables de los Servicios.
- Al Responsable de la Seguridad.
- Al Responsable del Sistema.
- A los Administradores del Sistema, a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

9.4 Roles: Funciones y Responsabilidades

9.4.1 Dirección

La Dirección de **Turismo y Deporte de Andalucía**. se ha comprometido con la implantación y el mantenimiento del Sistema de Gestión de la Seguridad de la Información y como evidencia de ello se encarga de la aprobación de la Política de Seguridad de la Información, además de formar parte del Comité de Seguridad de la Información.

La función de Dirección la desempeñará el CEO Director Gerente quien entiende la misión de la organización, determina los objetivos que se propone alcanzar y responde que se alcancen.

Función	Detalle
Nombrar	• Designar los diferentes roles encargados de la gestión de la seguridad.
Objetivos	• Fijar y aprobar anualmente unos objetivos de nivel de riesgo aceptable. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de la Organización, ser medibles o

	estimables y coherentes con las presentes Directrices. El Comité de Seguridad seguirá y reportará anualmente la evolución de dichos objetivos.
Aprobar	• Aprobar la Política de Seguridad, así como las revisiones de la misma. • Aprobar, tras cada proceso de Apreciación del Riesgo que se realice, el Plan de Tratamiento del Riesgo que se elabore, que puede incluir la aplicación de controles, la transferencia a terceros, evitar riesgos – lo que deriva generalmente en la realización de cambios en procesos -, o bien la asunción de determinados riesgos.
Recursos	• Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

9.4.2 Comité de Seguridad de la Información

Se ha creado el Comité de Seguridad de la Información que estará compuesto por los siguientes miembros:

Perfil	Responsable
Presidencia	Dirección Gerencia
Vocales	• Dirección de Operaciones ○ Dirección de Marca/Dirección de Innovación ○ Jefatura de Departamento de Marketing Digital ○ Oficina del dato ○ Subdirección de Patrocinios y Promoción Deportiva ○ Subdirección de Instalaciones Deportivas ○ Subdirección de Servicios Jurídicos y Documentación ○ Dirección de Operaciones / Recursos Humanos ○ Dirección de Marca/Patrocinios ○ Dirección de Operaciones / Subdirección Económico Financiera ○ Subdirección de Servicios Jurídicos y Documentación
Asesores	Delegado De Protección De Datos Responsable de Área de Sistemas
Secretaría	Subdirección de Coordinación

Funciones del Comité. Corresponde al Comité de Seguridad de la Información:

Función	Detalle
Informar	• Atender las inquietudes de la Alta Dirección y de los diferentes departamentos/áreas. • Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
Promover	• Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información. • Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
Coordinar	• Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades. • Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.
Elaborar	• Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección. • Elaborar la estrategia de evolución de la Organización en lo que respecta a la seguridad de la información.
Aprobar	• Aprobar la normativa de seguridad de la información. • Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información • Aprobar planes de mejora de la seguridad de la información de la Organización. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
Controlar	• Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. • Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. 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.

Funciones del Secretario. Corresponde al Secretario/a del Comité de Seguridad de la Información:

- Convocar las reuniones del Comité de Seguridad de la información
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones de los Vocales. Corresponde a los vocales del Comité de Seguridad de la Información:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán como mínimo, el voto de la mayoría simple de sus miembros.

9.4.3 Responsable de la Información

El Responsable de la Información debe ser una persona que ocupa un alto cargo en la dirección de la organización.

Compatibilidades. Este rol únicamente podrá coincidir con la del Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Seguridad, Responsable del Sistema y el de Administrador del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Se ha designado responsable de la Información a:

Perfil	Responsable
Responsable de la Información	Dirección de Innovación

9.4.4 Responsable del Servicio

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa.

Compatibilidades. Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Seguridad, Responsable del Sistema y el de Administrador del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Se ha designado como Responsables de Servicio a las Dirección de Operaciones, como representante de los siguientes servicios prestados y sus responsables técnicos.

Servicio	Responsable
https://regalos.andalucía.org	Dirección de Marca/Dirección de Innovación
http://www.andalucía.org	Jefatura de Departamento de Marketing Digital
https://www.andalucíalab.org	Oficina del dato
http://www.andaluciaesdeporte.org	Subdirección de Patrocinios y Promoción Deportiva
www.turismoandaluz.com	Dirección de Operaciones
Registro Usuario Instalaciones deportivas	Subdirección de Instalaciones Deportivas
Registro de Entrada/Salida documentos	Subdirección de Servicios Jurídicos y Documentación
Servicios Internos (Intranet)	Dirección de Operaciones / Recursos Humanos
Servicio de Patrocinio y Colaboraciones	Dirección de Marca/Patrocinios
Servicio gestión de encomiendas	Dirección de Operaciones / Subdirección Económico Financiera
Tratamientos relativos a datos personales	Subdirección de Servicios Jurídicos y Documentación

Las funciones del Responsable del Servicio son las siguientes:

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al

Función	Detalle
	Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
Riesgos	Aprobar el riesgo residual (el resultante una vez aplicado los controles de seguridad).

Consideraciones. El Responsable del Servicio deberá tener en cuenta las siguientes consideraciones:

- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.
- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

9.4.5 Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información.

Se ha designado como Responsable de Seguridad de la Información al **Responsable del Área de Sistemas.**

Las funciones del Responsable de Seguridad son las siguientes:

Función	Detalle
Política, Normativa y Procedimientos	• Participará en la elaboración, en el marco del Comité de Seguridad de la Información, de la Política y Normativa de Seguridad de la Información, para su aprobación por Dirección. • Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
Documento de Seguridad	• Coordinará y controlará las medidas definidas en el Documento de Seguridad y en general se encargará del cumplimiento de las medidas de seguridad que detalla el reglamento de desarrollo de la LOPDGDD. • Coordinará la elaboración de la Documentación de Seguridad del Sistema.

Función	Detalle
Formación y concienciación	• Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información
Gestión de la Seguridad	• Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Organización. • Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema. • Realizará el Análisis de Riesgos. • Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. • Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos. • Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información. • Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por el Responsable de Sistemas. • Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios. • Elaborar la memoria anual sobre el estado de la seguridad de la información, con el progreso de los proyectos de los planes de mejora, resumen de las actuaciones en materia de seguridad, de los incidentes relativos a seguridad de la información, del estado de la seguridad del sistema, y en particular del

Función	Detalle
	nivel de riesgo residual al que está expuesto el sistema.
Monitorizar	• Monitorizará los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos. • Monitorizará el desempeño de los procesos de gestión de incidentes de seguridad y recomendará posibles actuaciones respecto de ellos. En particular, velará por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
Asesoramiento	• Asesorará a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo del ámbito de la empresa
Comité de Seguridad.	• Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable de la Seguridad, se podrá designar cuantos Responsables de Seguridad Delegados se consideren necesarios.

La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

9.4.6 Responsable del Sistema

Se ha designado como Responsable del Sistema el área de Sistemas**.**

Compatibilidades. Este rol podrá coincidir con el de Administrador del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad de la Información.

Las funciones del Responsable del Sistema son las siguientes:

Función	Detalle
Gestionar el Sistema	• Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • Acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
Establecer directrices y medidas	• Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema. • Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. • Determinar la configuración autorizada de hardware y software a utilizar en el Sistema. • Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
Elaborar	• Elaborar procedimientos operativos de seguridad. • Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
Aprobar	• Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.

Función	Detalle
	• Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
Monitorizar	• Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información.

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, se podrá designar cuantos Responsables de Sistema Delegados considere necesarios.

La designación corresponde al Responsable del Sistema. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información.

Función	Detalle
Responsable de Sistemas de Málaga	Responsable de Sistemas en Málaga
Responsable de Sistemas de Sevilla	Responsable de Sistemas en Sevilla

9.4.7 Administrador del Sistema

El Administrador del sistema es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Las funciones del Administrador del Sistema son las siguientes:

Función	Detalle
Implementar, gestionar y mantener la seguridad	• La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

Función	Detalle
	• Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • Informar a los Responsables de la Seguridad y del Sistema 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.
Gestión, configuración y actualización	• 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. • Aprobar los cambios en la configuración vigente del 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.
Gestión de las autorizaciones	• La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
Aplicar los procedimientos	• La aplicación de los Procedimientos Operativos de Seguridad. • Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	• 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.

9.4.8 Delegado de Protección de Datos (DPD)

Se ha designado como delegado de protección de datos al Ascêndia Reingeniería + Consultoría 2024, que tendrá como mínimo las siguientes funciones (contempladas en el art. 39 del Reglamento General de Protección de Datos.):

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

9.5 Designación y renovación de los cargos

Anualmente, la dirección designará los distintos cargos de seguridad. Presentándolos en una reunión del comité de seguridad. En caso de no recogerse nuevas designaciones, se entenderán renovados los cargos actuales por un periodo de un año.

9.6 Matriz RACI

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un equipo. Las siglas se explican en el Anexo 1.

	Rol	Descripción
R	**Responsable**	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RACI. Es quien debe ejecutar las tareas.
A	**Administrador**	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las

		tareas.
C	**Consultor**	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).
I	**Informado**	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea	CD	RINFO	RSERV	RSEG	DPD	RSIS	ASS
Niveles de seguridad requeridos por la información		A	I	R	C	C	
Niveles de seguridad requeridos por el servicio		I	A	R	C	C	
Determinación de la categoría del sistema		I	I	A/R	I	I	
Establecimiento y gestión de los registros de actividades de tratamiento.					A/R		
Análisis de riesgos		I	I	A/R	R	C	
Declaración de aplicabilidad		I	I	A/R	I	C	
Medidas de seguridad adicionales				A/R	I	C	
Configuración de seguridad		I	I	A	C	C	R
Aceptación del riesgo residual (1)		A	A	R	I	I	
Documentación de seguridad (3)				A	C	C	I
Política de seguridad	A			R	I	C	
Normativa de seguridad (3)				A	I	C	I
Procedimientos de seguridad (3)				C	I	A	I
Implantación de las medidas de seguridad		I	I	C	I	A	R
Supervisión de las medidas de seguridad (2)				A	C	C	R
Estado de seguridad del Sistema	I	I	I	A	I	I	R
Planes de mejora de la seguridad (3)				A	C	C	
Planes de concienciación y formación (3)				A	C	C	

1.- Aparecen dos A porque la aceptación del riesgo residual debe ser coordinada entre ambas responsabilidades. Esta coordinación es muy sencilla si las responsabilidades se aúnan en el Comité de Seguridad.
2.- Las tareas que realiza el ASS involucran al Responsable del Sistema y de la Seguridad. Uno deberá ser el responsable (A) y el otro deberá ser consultado (C). La determinación de quién hace cada papel dependerá de a quién reporta el ASS, pudiendo existir diferentes ASS para diferentes funciones, pero siempre con una línea clara de dependencia de uno u otro responsable.

3.- Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

10. Datos de carácter personal

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal.

Turismo y Deporte de Andalucía solo recabará 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 vigente de Protección de Datos.

La garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las áreas de **Turismo y Deporte de Andalucía,** que se rige por los siguientes principios:

a) Licitud, lealtad y transparencia.

b) Limitación de la finalidad.

c) Minimización de datos.

d) Exactitud.

e) Limitación del plazo de conservación.

f) Integridad y confidencialidad.

g) Responsabilidad proactiva.

La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento, aplicándose para ello las medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado en función del correspondiente análisis de riesgos, tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre. Dicho análisis de riesgos se realizará teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

La garantía del cumplimiento de lo previsto en el apartado anterior, se articulará a través del marco organizativo establecido en la presente Política de Seguridad y se llevará a cabo de conformidad con la normativa aplicable en materia de protección referida en el artículo 3 de esta Orden y en el Real Decreto 311/2022, de 3 de mayo, prevaleciendo las medidas derivadas de la aplicación de la normativa de protección de datos cuando, tras un análisis de riesgos, se estime que las mismas son superiores a las previstas en el ENS.

La observación del principio de seguridad del tratamiento de los datos personales cobrará especial relevancia cuando sea probable que un determinado tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas, en cuyo caso el Responsable del tratamiento recabará el asesoramiento del DPD al realizar la preceptiva evaluación de impacto relativa a la protección de datos.

11. Gestión de riesgos

11.1 Justificación

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

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 7 del ENS.

11.2 Criterios de Evaluación de Riesgos

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados se especificarán en la metodología de evaluación de riesgos que elaborará la organización, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la organización de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los ciudadanos.

11.3 Directrices de Tratamiento

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

11.4 Proceso de Aceptación del Riesgo Residual

Los riesgos residuales serán determinados por el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por el Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán ser aceptados previamente por el Responsable de ese Servicio.

Los niveles de riesgo residuales serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

11.5 Necesidad de realizar o actualizar las evaluaciones de riesgos

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 10 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

12. Gestión de incidentes de seguridad

12.1 Prevención de incidentes

Los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 20 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 18 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

12.2 Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la Organización, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

12.3 Respuesta ante incidentes

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar 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).

12.4 Recuperación ante incidentes y planes de continuidad

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

13. Obligaciones del personal

Los miembros de la organización 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 a los afectados.

Los miembros de la organización atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de la organización, en particular a los 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.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la organización, constituyendo su incumplimiento infracción grave a efectos laborales.

13.1 Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Se hace necesario que, de manera objetiva y no discriminatoria, las organizaciones que presten servicios a **Turismo y Deporte de Andalucía** cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados a nivel de seguridad.

14. Terceras partes

Cuando se presten servicios o se gestione información desde otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad 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.

14.1 Revisión y aprobación de la política de seguridad

La Política de Seguridad de la Información será revisada por el Comité de Seguridad de la Información a intervalos planificados, que no podrán exceder el año de duración, o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

15. Glosario de términos

Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Gestión de incidentes: Plan de acción para atender a las incidencias que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad: Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

Política de seguridad: Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.

Principios básicos de seguridad: Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información: Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad: El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio: Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema: Persona que se encarga de la explotación del sistema de información.

Servicio: Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir

16. Anexo 1. Tareas

En la tabla se usan las siguientes abreviaturas:

- CS - Comité de Seguridad
- CD - Comité de Dirección
- RINFO - Responsable de la Información
- RSERV - Responsable del Servicio
- RSEG - Responsable de Seguridad
- RSIS - Responsable del Sistema
- ASS - Administrador del Sistema
- DPD - Delegado de Protección de Datos

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CS
Determinación de la categoría del sistema	RSEG
Establecimiento y gestión de los registros de actividades de tratamiento.	DPD
Análisis de riesgos (incluido el análisis de riesgo de los tratamientos realizados)	RSEG + DPD
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de Seguridad (incluidas medidas de	elabora: RSEG+DPD

Tarea	Responsable
seguridad adecuadas a los riesgos y naturaleza de los tratamientos)	aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG+DPD
Política de seguridad	elabora: CS aprueba: CD
Normativa de seguridad	elabora: RSEG aprueba: CS
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.	Elabora: RSEG + DPO aplica: RSIS + ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CS
Planes de concienciación y formación	elabora: RSEG+DPD aprueba: CS
Evaluaciones de Impacto: • Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos • Realización de evaluaciones de impacto sobre la protección de datos	DPD
Planes de continuidad	elabora: RSIS valida: RSEG+DPD coordina y aprueba: CS ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG+DPD
Protección de datos personales	DPD

Tarea	Responsable
Respuesta a incidentes de seguridad de la información: • Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad. • Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo. • Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deben estar procedimentadas). • Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deben estar procedimentadas). • Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados. • Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.	RS + DPO+ ASS

Respuesta a incidentes de seguridad de la información:

- ASS: Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.
- ASS: Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.
- ASS: Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- ASS: Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).
- ASS: Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.
- ASS: Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.

- RSEG: Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.
- RSIS: Planificar la implantación de las salvaguardas en el sistema.
- Comité de Seguridad: Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.
- RSIS: Ejecutar el plan de seguridad aprobado.
- DPD: encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales.

El presente documento de Política de Seguridad de la Empresa Pública para la Gestión del Turismo y del Deporte de Andalucía queda aprobado el 22 de mayo de 2024, a la firma de los integrantes de su Comité de Seguridad

Presidente *Fdo. CEO Director Gerente*	***Secretaria*** *Fdo. COO Directora de Operaciones*
Responsable de la Información *Fdo. CIO Director de Innovación*	***Responsable de los Servicios*** *Fdo. COO Directora de Operaciones*
Responsable de Seguridad *Fdo. Responsable de Sistemas*	***Responsable de Sistemas*** *Fdo. Administradora de Sistemas*
Delegado de Protección de Datos *Fdo. Consultor de Protección de Datos*	