ÍNDICE

1. INTRODUCCIÓN

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. depende de los sistemas de información para alcanzar sus objetivos y prestar sus servicios, en particular aquellos relacionados con la prestación de servicios de marketing digital y comunicación a Administraciones Públicas. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas, en función del riesgo, para protegerlos frente a daños accidentales o deliberados que puedan afectar a la autenticidad, trazabilidad, integridad o confidencialidad de la información tratada o la disponibilidad de los servicios prestados.

El objetivo último de la seguridad de la información es garantizar que la entidad pueda cumplir con sus objetivos estratégicos, desarrollar sus funciones y prestar los servicios para los que ha sido constituida, asegurando la calidad de la información gestionada y la prestación continuada de los servicios. Para ello, la entidad actuará de forma preventiva y supervisará de manera continua la actividad diaria de sus sistemas, reaccionando con diligencia y eficacia ante los incidentes de seguridad.

En el contexto de los servicios de marketing digital prestados a Administraciones Públicas, la protección de la información adquiere una especial relevancia, dado que dichos servicios pueden implicar el tratamiento de información institucional, datos personales y contenidos estratégicos, cuya alteración, pérdida o divulgación no autorizada podría afectar tanto a la imagen pública como al correcto funcionamiento de las entidades clientes.

Los sistemas TIC deben estar protegidos contra amenazas en constante evolución con capacidad de impactar en la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, así como en el uso previsto y valor de la información y los servicios. Para hacer frente a estas amenazas, DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. adoptará una estrategia de seguridad basada en la gestión continua del riesgo, que permita adaptarse a los cambios en el entorno tecnológico, regulatorio y operativo, garantizando en todo momento la continuidad de los servicios prestados a las Administraciones Públicas. En este sentido, la organización aplicará las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, adecuándolas a la naturaleza de los servicios prestados, y llevará a cabo un proceso continuo de monitorización, evaluación y mejora de la seguridad. Esto incluye el seguimiento del estado de los sistemas, la gestión proactiva de vulnerabilidades, la detección y respuesta ante incidentes de seguridad, y la implementación de planes de continuidad y recuperación.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. garantizará que la seguridad de la información sea 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 donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información. La organización promoverá una cultura de seguridad de la información entre todo su personal y colaboradores, asegurando que conozcan sus responsabilidades y actúen de acuerdo con las políticas, normas y procedimientos establecidos.

2. ALCANCE

La presente política es de aplicación a todos los sistemas de información de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L., entendiendo como tales los sistemas, infraestructuras, redes, aplicaciones, servicios y recursos tecnológicos que soportan los procesos de negocio de la organización.

Esta política es igualmente de obligado cumplimiento para todo el personal de la organización, con independencia de su relación contractual, función o ubicación, incluyendo empleados, directivos y colaboradores. Asimismo, será de aplicación a terceros que, de forma directa o indirecta, accedan, gestionen o traten información o sistemas de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L., tales como proveedores, prestadores de servicios, socios tecnológicos o cualquier otra entidad externa.

El alcance de esta política comprende a los sistemas de información que dan soporte a los servicios de análisis, diseño, desarrollo, mantenimiento y soporte técnico de aplicaciones web, plataformas digitales y contenidos interactivos para entidades del Sector Público, en el ámbito del marketing digital.

Esta política se aplicará a todos los procesos de negocio y actividades que impliquen el tratamiento de información o el uso de sistemas TIC, abarcando todo el ciclo de vida de los sistemas de información, desde su planificación y diseño hasta su retirada de servicio.

En particular, esta política será de aplicación a los sistemas que den soporte a servicios prestados a Administraciones Públicas, garantizando el cumplimiento de los requisitos establecidos por el Esquema Nacional de Seguridad y demás normativa aplicable.

3. MISIÓN

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. tiene como misión proporcionar servicios de marketing digital, comunicación y difusión a Administraciones Públicas, contribuyendo a mejorar la visibilidad, accesibilidad y eficacia de la información y los servicios que estas ofrecen a la ciudadanía, mediante el uso de tecnologías digitales y canales online.

En el desarrollo de su actividad, la organización gestiona información de carácter institucional y, en determinados casos, datos personales o contenidos asociados a la comunicación pública, lo que requiere garantizar un tratamiento seguro, fiable y conforme a la normativa vigente, especialmente en aquellos servicios prestados a entidades del sector público.

Para el cumplimiento de sus objetivos, DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. hace uso intensivo de sistemas de información que resultan esenciales para la prestación de sus servicios. Estos sistemas deben ser adecuadamente protegidos,

gestionados y supervisados, asegurando en todo momento la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información tratada.

En este contexto, la seguridad de la información se configura como un elemento clave para garantizar la confianza de las Administraciones Públicas clientes, la continuidad de los servicios prestados y el cumplimiento de los requisitos establecidos por la normativa vigente.

Los objetivos en materia de seguridad que DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. pretende garantizar con la presente política serán:

- Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.
- Implementar medidas de seguridad en función del riesgo.
- Formar y concienciar a los integrantes de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. respecto a la seguridad de la información. Implementar medidas de seguridad que permitan la trazabilidad de los accesos y, respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.
- Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.
- Establecer la seguridad en la gestión de comunicaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de redes de comunicaciones sea adecuadamente protegida.
- Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.
- Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.
- Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.
- Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

4. MARCO NORMATIVO

La presente política de seguridad de la información se desarrolla en el marco de la legislación vigente aplicable a DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L., teniendo en cuenta tanto su condición de entidad privada como su papel como prestador de servicios a Administraciones Públicas.

En particular, las principales normas y referencias que afectan a esta política son las siguientes:

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

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Cualquier otra normativa, regulación o instrucción que resulte de aplicación en función de los servicios prestados.

Asimismo, DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. tendrá en consideración las guías, normas técnicas y recomendaciones emitidas por el Centro Criptológico Nacional (CCN-STIC), como referencia para la adecuada implementación y mejora continua de las medidas de seguridad.

5. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1. Gestión de riesgos.

De conformidad con lo establecido en el Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad, la gestión de riesgos constituye un elemento esencial para garantizar la seguridad de la información y la prestación de los servicios.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. adoptará un enfoque sistemático para la identificación, análisis, evaluación y tratamiento de los riesgos que puedan afectar a sus sistemas de información, especialmente aquellos vinculados a los servicios de marketing digital que se prestan a las Administraciones Públicas.

La gestión de riesgos tendrá como objetivo mantener los riesgos en niveles aceptables para la organización, teniendo en cuenta el impacto que estos puedan tener sobre la confidencialidad, integridad, autenticidad y trazabilidad de la información, así como sobre la disponibilidad de los servicios. La dirección de la organización participará en la toma de decisiones relativas a la aceptación del riesgo residual.

El análisis y tratamiento de riesgos se realizará utilizando metodologías reconocidas y alineadas con las buenas prácticas en el ámbito de la seguridad de la información (Magerit), tomando como referencia las guías y recomendaciones publicadas por el Centro Criptológico Nacional y otros organismos de referencia en materia de ciberseguridad.

Todos los sistemas incluidos en el alcance de esta política deberán someterse a un análisis de riesgos, en el que se identifiquen las amenazas, vulnerabilidades e impactos potenciales. Dicho análisis será revisado de forma periódica, al menos con carácter anual, y siempre que se produzcan cambios relevantes, tales como:

- Modificaciones significativas en la información tratada o en su nivel de sensibilidad.

- Cambios sustanciales en los servicios prestados o en los sistemas que los soportan.
- La ocurrencia de incidentes de seguridad de especial relevancia.
- La identificación de vulnerabilidades críticas que puedan afectar a los sistemas.

La gestión de riesgos estará integrada en todas las fases del ciclo de vida de los sistemas de información. La selección de medidas de seguridad y la evaluación de su eficacia se realizarán teniendo en cuenta los resultados del análisis de riesgos.

5.2. Gestión y protección de la información.

Toda la información gestionada por DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. deberá ser tratada de acuerdo con su nivel de sensibilidad y con las medidas de seguridad que resulten aplicables en cada caso.

El personal de la organización, así como cualquier tercero que acceda a información en el marco de una relación profesional, estará sujeto al deber de confidencialidad respecto a aquella información que no tenga carácter público. Esta obligación se mantendrá vigente incluso una vez finalizada la relación laboral o contractual. A tal efecto, la organización establecerá los compromisos de confidencialidad correspondientes, que deberán ser aceptados de forma expresa.

La información será protegida con independencia de su soporte, garantizando un nivel de seguridad equivalente, tanto para la información en formato electrónico, como para aquella contenida en documentos físicos. En este sentido, se adoptarán medidas adecuadas para su almacenamiento, acceso y conservación, minimizando los riesgos de pérdida, deterioro o acceso no autorizado.

En relación con la documentación en soporte físico, se deberán aplicar prácticas que aseguren su adecuada custodia, evitando su exposición innecesaria y almacenándola en ubicaciones seguras. Asimismo, se procurará mantener espacios de trabajo ordenados que reduzcan el riesgo de accesos indebidos o divulgaciones accidentales de información.

La eliminación de la información, tanto en formato electrónico como en soporte papel, se realizará mediante procedimientos que garanticen su destrucción segura, impidiendo la recuperación posterior de los datos. Cuando se recurra a proveedores externos para la gestión o destrucción de información, se deberá asegurar que estos cumplen con las garantías adecuadas en materia de seguridad y confidencialidad, incorporando las correspondientes cláusulas contractuales.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. promoverá, además, la concienciación de su personal en materia de protección de la información, fomentando buenas prácticas en su tratamiento y reforzando la responsabilidad individual en la salvaguarda de los activos de información.

5.3. Control de accesos y uso de los sistemas.

El acceso a los sistemas de información de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. estará restringido exclusivamente a usuarios autorizados, quienes deberán identificarse mediante credenciales individuales, únicas e intransferibles. La organización establecerá los mecanismos necesarios para garantizar una correcta gestión de identidades y accesos.

Los permisos concedidos a cada usuario se ajustarán al principio de mínimo privilegio, de forma que cada persona únicamente disponga de los accesos necesarios para el desempeño de sus funciones. Dichos permisos serán revisados periódicamente y adaptados cuando se produzcan cambios en las responsabilidades o en la relación con la entidad.

Con el fin de garantizar la seguridad de la información y el cumplimiento de las obligaciones legales y contractuales, la actividad realizada sobre los sistemas podrá ser objeto de registro y supervisión. Estos registros permitirán la detección de accesos indebidos, la investigación de incidentes y la verificación del cumplimiento de esta política, respetando en todo caso la normativa vigente en materia de protección de datos.

En particular, las acciones que impliquen acceso a información sensible o la modificación de datos deberán quedar registradas con el nivel de detalle suficiente para asegurar la trazabilidad de las operaciones realizadas.

Los sistemas y medios tecnológicos puestos a disposición del personal están destinados prioritariamente al desarrollo de la actividad profesional. Cualquier uso distinto deberá ser limitado, responsable y conforme a las directrices internas de la organización. En caso de autorizarse el uso de dispositivos personales o el acceso desde entornos externos, se deberán aplicar las medidas de seguridad necesarias para garantizar la protección de la información.

5.4. Protección de los sistemas e infraestructuras.

Los sistemas de información, infraestructuras tecnológicas y redes de comunicaciones de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. deberán ubicarse en entornos adecuados que garanticen su protección frente a accesos no autorizados, daños físicos o interferencias. El acceso a estos entornos estará limitado exclusivamente a personal autorizado.

Los sistemas deberán configurarse y mantenerse conforme al principio de funcionalidad mínima necesaria, de manera que únicamente dispongan de aquellas capacidades, servicios y componentes imprescindibles para cumplir con los fines para los que fueron diseñados o adquiridos. Dichos fines deberán estar definidos y alineados con las necesidades de la organización y de los servicios prestados.

Las actividades relacionadas con la operación, administración, mantenimiento y supervisión de los sistemas deberán estar definidas y organizadas de manera que se garantice su correcto funcionamiento y seguridad. Estas actividades estarán sujetas a control y seguimiento, asegurando la aplicación coherente de las medidas de seguridad establecidas por la organización.

5.5. Gestión de la actividad y monitorización.

Las actividades realizadas sobre los sistemas de información de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. serán registradas con el fin de garantizar la trazabilidad de las operaciones, verificar el cumplimiento de la presente política y dar respuesta a las obligaciones legales, contractuales y de seguridad aplicables.

Los registros generados permitirán la monitorización, análisis y, en su caso, la investigación de eventos e incidentes de seguridad, contribuyendo a la detección temprana de accesos no autorizados o usos indebidos de los sistemas. La

información contenida en dichos registros será tratada con las debidas garantías de confidencialidad e integridad.

En particular, las acciones que impliquen el acceso a información sensible, así como aquellas que supongan la modificación, eliminación o transferencia de datos, deberán quedar registradas con el nivel de detalle suficiente para asegurar la trazabilidad de las actuaciones realizadas y facilitar su posterior análisis.

La organización establecerá mecanismos de supervisión continua que permitan identificar comportamientos anómalos, vulnerabilidades o amenazas que puedan afectar a la seguridad de los sistemas y de la información.

Asimismo, se definirán criterios para la conservación de los registros durante el tiempo necesario para cumplir con los requisitos legales, contractuales y operativos, garantizando su protección frente a accesos no autorizados, alteraciones o pérdidas.

La gestión de la actividad y la monitorización se integrarán en los procesos de gestión de incidentes de seguridad, permitiendo una respuesta eficaz ante cualquier evento que pueda comprometer la seguridad de la información o la continuidad de los servicios.

5.6. Seguridad en la gestión de servicios y proveedores.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. podrá apoyarse en terceros para la prestación de determinados servicios, el suministro de soluciones tecnológicas o la gestión de infraestructuras necesarias para el desarrollo de su actividad.

La contratación y gestión de proveedores que tengan acceso a información de la entidad o que participen en la prestación de servicios TIC se realizará bajo criterios de seguridad, asegurando que dichos terceros cumplen con niveles adecuados de protección de la información y con la normativa vigente que les resulte de aplicación.

En estos casos, se deberá establecer las condiciones de seguridad aplicables en los acuerdos contractuales, incluyendo, cuando corresponda, cláusulas específicas sobre confidencialidad, protección de datos, gestión de incidentes de seguridad, continuidad del servicio y obligaciones de notificación ante brechas de seguridad.

Los proveedores que traten información de la organización o den soporte a sistemas deberán ser evaluados previamente en función de su capacidad para garantizar la seguridad de los servicios prestados, pudiendo requerirse evidencias de cumplimiento, certificaciones o garantías equivalentes.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. mantendrá un control adecuado sobre los servicios externalizados, asegurando su seguimiento, supervisión y revisión periódica, con el fin de verificar el cumplimiento de los requisitos de seguridad establecidos y minimizar los riesgos asociados a la dependencia de terceros.

5.7. Continuidad del servicio y gestión de incidentes.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. adoptará las medidas necesarias para garantizar la continuidad de los servicios prestados, minimizando el impacto que puedan tener posibles interrupciones en los sistemas de información.

La entidad definirá y mantendrá las estrategias y medidas de continuidad que permitan asegurar la disponibilidad de los servicios, contemplando escenarios de interrupción, degradación del servicio o indisponibilidad de los sistemas. Estas medidas deberán ser proporcionales al nivel de riesgo identificado y a la criticidad de los servicios prestados.

En caso de producirse una incidencia de seguridad que afecte o pueda afectar a la disponibilidad del servicio o a la confidencialidad, integridad, autenticidad y trazabilidad de la información, esta será gestionada de forma estructurada y coordinada, con el objetivo de minimizar su impacto, restaurar el servicio en el menor tiempo posible y evitar su repetición.

La organización establecerá mecanismos para la detección, notificación, análisis, respuesta y seguimiento de los incidentes de seguridad, asegurando que estos sean gestionados de manera eficaz y conforme a los procedimientos internos definidos. Asimismo, se mantendrá la trazabilidad de los incidentes relevantes para su análisis posterior y la mejora continua del sistema de seguridad.

Cuando los incidentes afecten a servicios prestados a Administraciones Públicas, se adoptarán las medidas de comunicación y notificación que resulten obligatorias conforme a la normativa vigente, incluyendo, en su caso, las derivadas del Esquema Nacional de Seguridad y de la normativa de protección de datos.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. promoverá la mejora continua de sus capacidades de respuesta ante incidentes y de continuidad del servicio, revisando periódicamente las medidas implantadas y adaptándolas a la evolución de los riesgos, la tecnología y los servicios prestados.

5.8. Organización de la seguridad y mejora continua.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. establece un marco organizativo para la gestión de la seguridad de la información que asegura la adecuada definición de responsabilidades, la coordinación de las actuaciones en materia de seguridad y la integración de la seguridad en los procesos de la organización.

La seguridad de la información se configura como una responsabilidad compartida en todos los niveles de la organización, promoviendo la implicación activa de la dirección, del personal y de los terceros que intervengan en la prestación de servicios o en la gestión de sistemas de información.

La organización dispondrá de los roles y funciones necesarios para la adecuada gestión de la seguridad, garantizando la supervisión de las medidas implantadas, la coherencia en su aplicación y la adecuada toma de decisiones en materia de seguridad de la información.

Asimismo, DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. impulsará la mejora continua del Sistema de Gestión de la Seguridad de la Información (SGSI), mediante la revisión periódica de la presente política, la evaluación de la eficacia de las medidas implantadas y la adaptación de estas a la evolución de los riesgos, la tecnología y los requisitos legales, contractuales y operativos.

La organización fomentará la formación y concienciación en materia de seguridad de la información, con el objeto de reforzar una cultura organizativa orientada a la protección de los activos de información y al cumplimiento de las obligaciones establecidas en el Esquema Nacional de Seguridad.

6. ORGANIZACIÓN DE LA SEGURIDAD

El Esquema Nacional de Seguridad prevé que en los sistemas de información existan varios roles diferenciados:

- El responsable de la información, que determinará los requisitos de la información tratada.
- El responsable de los servicios, que determinará los requisitos de los servicios prestados.
- El responsable de seguridad, que tomará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- El responsable del sistema, que se encargará 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.

La responsabilidad de la seguridad de los sistemas de información debe estar diferenciada de la responsabilidad sobre la prestación de los servicios y la política de seguridad de la entidad es la que debe detallar las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

Debido a la estructura de la organización, se ha decidido agrupar el responsable de la información y el responsable de los servicios en una misma persona, que ostenta cargo directivo en la entidad. Asimismo, se ha nombrado a dos personas distintas para los roles de responsable de seguridad y responsable del sistema, con el objeto de que exista independencia jerárquica y que puedan desempeñar sus funciones con plenas garantías.

Los roles serán designados por la Alta Dirección de la entidad y los nombramientos podrán ser revisados cada dos años, pudiendo realizarse antes cuando el puesto quede vacante o por un incumplimiento reiterado de sus funciones, previo apercibimiento. DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. dispondrá de un mecanismo que permita la sustitución de los responsables designados en caso de ausencias de larga duración o aquellas de menor duración pero que puedan provocar ineficiencias en las funciones de cada uno de ellos que afecten al sistema.

6.1. Funciones y responsabilidades del responsable de la información.

La función del responsable de la información será asumida por la dirección de la entidad. En relación con la seguridad de la información, tendrá las siguientes competencias:

- Asumir la responsabilidad última del uso que se haga de la información, así como de la disponibilidad, accesibilidad e interoperabilidad de los servicios.
- Asumir la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad de la información, o bien de disponibilidad del servicio.
- Determinar los niveles de seguridad de la información y la categoría de los servicios.

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I del ENS y las guías CCN-STIC.
- Informar sobre los derechos de acceso a la información.
- Aceptar los niveles de riesgo residual que afectan a la información.
- Poner en comunicación del responsable de seguridad cualquier variación respecto a la información de los que es responsable, especialmente la incorporación de nueva información a su cargo.

6.2. Funciones y responsabilidades del responsable del servicio.

La función del responsable del servicio la ejercerá también la dirección de la entidad. Las funciones se concretan en las siguientes:

- Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del ENS y las guías CCN-STIC, previa propuesta al responsable de seguridad.
- Informar sobre los derechos de acceso al servicio.
- Aceptar los niveles de riesgo residual que afecten al servicio.
- Poner en comunicación del responsable de seguridad, cualquier variación respecto a los servicios de los que es responsable, especialmente la incorporación de nuevos servicios a su cargo.

6.3. Funciones y responsabilidades del responsable de seguridad.

Las funciones del responsable de seguridad de la información se concretan en las siguientes:

- 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.
- Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable del sistema.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema.
- Gestionar los procesos de certificación.

6.4. Funciones y responsabilidades del responsable del sistema.

Las funciones del responsable del sistema serán las siguientes:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene conocimiento de que estos presentan deficiencias graves de seguridad.
- 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.
- Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el responsable de seguridad.
- Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

6.5. Funciones y responsabilidades derivadas de la aplicación de la normativa en materia de protección de datos personales.

La normativa en materia de protección de datos personales, en particular el Reglamento (UE) 2016/679 (RGPD) y la Ley Orgánica 3/2018 (LOPDGDD), establece obligaciones que guardan una estrecha relación con los principios de seguridad de la información recogidos en el Esquema Nacional de Seguridad, especialmente en lo relativo a la definición de responsabilidades sobre los tratamientos de los datos y la adopción de medidas de seguridad adecuadas.

DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L., en su condición de responsable de determinados tratamientos de datos personales derivados de su actividad, asume la responsabilidad de garantizar que dichos tratamientos se realizan conforme a la normativa vigente, aplicando las medidas técnicas y organizativas necesarias para proteger los derechos y libertades de las personas físicas.

En relación con la figura de la persona Delegada de Protección de Datos (DPD), la organización no está obligada a designar a esta figura conforme a los requisitos señalados en el RGPD. No obstante, se cuenta con el apoyo de un servicio externo especializado que actúa como asesor en materia de protección de datos personales, proporcionando orientación, supervisión y recomendaciones para el adecuado cumplimiento de la normativa aplicable.

Dicha función de asesoramiento se ejerce de forma independiente, evitando cualquier conflicto de intereses con la determinación de los fines y medios de los

tratamientos de datos, responsabilidades que corresponden a la dirección de la entidad o a los responsables designados dentro de la misma.

El servicio externo de asesoramiento en protección de datos podrá colaborar en el mantenimiento y revisión del Registro de Actividades de Tratamiento, así como en la evaluación de riesgos asociados al tratamiento de datos personales y en la definición de medidas de cumplimiento normativo, sin perjuicio de que la responsabilidad última sobre los tratamientos recaiga en DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L.

Asimismo, la entidad garantizará que las decisiones relevantes en materia de protección de datos se adopten teniendo en cuenta las recomendaciones y evaluaciones emitidas por el servicio especializado, integrando dichos criterios en el marco del Sistema de Gestión de la Seguridad de la Información.

7. RESOLUCIÓN DE CONFLICTOS

En caso de conflicto entre las personas designadas como responsables, de conformidad con lo previsto en la presente política, corresponderá la resolución del mismo a la dirección de la entidad. En caso de que exista una votación para resolver el conflicto, el voto de la Alta Dirección tendrá un valor doble.

8. OBLIGACIONES DEL PERSONAL

El personal de DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. tiene la obligación de conocer y cumplir esta política de seguridad de la información y la normativa de seguridad que de ella se derive, siendo responsabilidad de la entidad disponer los medios necesarios para hacerla llegar a los afectados. Se establecerá un programa de concienciación continua para atender a todos los miembros de la entidad, 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 llevar a cabo sus funciones. Estas acciones formativas tendrán carácter obligatorio.

9. TERCEROS

Cuando DDINTERACTIVA DESARROLLO Y DIFUSIÓN, S.L. preste servicios a otras entidades o maneje información de otras, se les hará partícipes de esta política de seguridad de la información, sin perjuicio de respetar las obligaciones de la normativa de protección de datos si actúa como encargado de tratamiento en la prestación de los citados servicios.

Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla, de modo que la entidad pueda supervisarlos o solicitar evidencias del cumplimiento de estos, incluso auditorías de segunda o tercera parte. Los terceros

garantizarán que su personal está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política o el que específicamente se pueda exigir en el contrato.

Cuando algún aspecto de la política no pueda ser satisfecho por un tercero según se requiere en los párrafos anteriores, el responsable de la seguridad emitirá un informe 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 del inicio de la contratación. El informe se trasladará al representante de la entidad que deberá autorizar la continuación con la tramitación de contratación del tercero, asumiendo los riesgos detectados.

Cuando la entidad adquiera, desarrolle o implante un sistema de Inteligencia Artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del responsable de la seguridad, que consultará al responsable de la información y del servicio y, cuando sea necesario, al del sistema.

10. APROBACIÓN Y REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Las modificaciones de la presente política que supongan cambios o adaptaciones ante ineficiencias las realizará la dirección de la entidad, que deberá revisarla anualmente.

En caso de que los cambios supongan una modificación sustancial o de los principios o responsabilidades designadas, la dirección propondrá los cambios que deberán ser aprobados, en su caso, por la persona u órgano con las debidas competencias.

La sustitución de la política será instada por la dirección de la entidad y ratificada por la persona u órgano con las debidas competencias, de lo que se informará adecuadamente a los interesados por los mismos canales usados para su difusión.