DOC-SGSI-01 - Politica de Seguridad Información

Control del documento

Clave	Resumen	Versión	Fecha Aprobación	Fecha Revisión	Aprobado Por	Estado	Descripción	Código Documento
DOC-7	Politica de Seguridad Información de la DGAD	8.0	dic 15, 2020	dic 14, 2020		En almacenamiento y distribución	Realizado	DOC-SGSI-01

INDICE

DECLARACION DE LA POLITICA DE SEGURIDAD DE LA INFORMACION DE LA DIRECCIÓN GENERAL PARA EL AVANCE DIGITAL

INTRODUCCIÓN

Este documento refleja la Política de Seguridad de la Información de la Dirección General para el Avance Digital (en adelante DGAD) del Gobierno de La Rioja.
Esta política se alinea tanto con la estrategia y gestión de riesgos de la propia DGAD como, de forma más general, del Gobierno de La Rioja en su conjunto. Describe las líneas maestras de los objetivos a seguir y el compromiso de la dirección por el cumplimiento de los requisitos aplicables de seguridad y de mejora continua del Sistema de Gestión de Seguridad de la Información (en adelante SGSI).
Esta política se alinea con la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja (aprobada por Decreto 96/2020, de 4 de noviembre con las sucesivas modificaciones que se vayan incorporando), conforme a lo establecido en:

- Misión y objetivos.
- Revisión de la Política de Seguridad de la Información.
- Instrumentos de desarrollo.
- Obligaciones del personal.

ALCANCE

El alcance de la presente Política de Seguridad de la Información corresponde a los sistemas de información que dan soporte a los servicios TIC (Sistemas e Infraestructura) del Gobierno de La Rioja.

COMPROMISO CORPORATIVO

Esta Política de Seguridad de la Información asegura el firme compromiso de la DGAD para la difusión y consolidación de una "cultura de la seguridad".
Asimismo, establece el compromiso de comprender las necesidades y expectativas de las partes interesadas que determinen los requisitos a satisfacer por parte del SGSI.
La DGAD expresa su compromiso con la mejora continua, por medio del desarrollo de procedimientos que aseguren una adecuada gestión de acciones correctivas ante no conformidades, así como una revisión periódica del SGSI para asegurar su idoneidad, adecuación y eficacia.

MISIÓN Y OBJETIVOS

La DGAD se alinea con la misión y objetivos establecidos en la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja dentro del alcance identificado en la presente política, persiguiendo ofrecer a todas las partes interesadas un servicio en un entorno seguro y de confianza.
Esta política establece un marco global para la gestión de la seguridad de la información protegiendo los activos de la información,

minimizando los riesgos derivados de un posible fallo de seguridad, y asegurar el cumplimiento de los objetivos establecidos.
Se establecen los siguientes objetivos generales:

- Contribuir desde la gestión de la seguridad al cumplimiento de la misión y objetivos de la DGAD.
- Disponer de las medidas de control necesarias para garantizar el cumplimiento de los requisitos legales que sean de aplicación como consecuencia de la actividad desarrollada.
- Asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.
- Asegurar la prestación continuada de los servicios.
- Proteger los activos de información correspondientes al alcance definido y la tecnología que los soporta de cualquier amenaza, con el fin de asegurar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los mismos.

REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Toda política de seguridad cuyo alcance sea la DGAD o los servicios o áreas de su competencia debe ser aprobada por el Comité de Seguridad de la Información de la DGAD.

INSTRUMENTOS DE DESARROLLO

Siguiendo la estructura definida en la Política de Seguridad de la Información de la Administración de la Comunidad Autónoma de La Rioja, la DGAD ha establecido un marco normativo en materia de seguridad que se encuentra estructurado por diferentes niveles, de forma que los objetivos planteados por el presente documento tengan un desarrollo reglamentario que permita definir y concretar regulaciones y restricciones que sean aplicables sobre los sistemas de información o al personal que gestiona o utiliza dichos sistemas. Estructura su marco normativo en los siguientes tipos de documentos:

- La presente **Política de Seguridad de la Información** que debe establecer los requisitos y criterios de protección y servirá de guía para la creación de normas de seguridad.
- Las **normas de seguridad** definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización. Establecen un conjunto de expectativas y requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Los **procedimientos de seguridad** en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Son documentos que especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

Toda esta documentación será gestionada según un procedimiento de gestión de documentos y registros que tiene como objetivo establecer los criterios para el control de la documentación y registros de seguridad utilizados.

OBLIGACIONES DEL PERSONAL

Todos los miembros de la DGAD tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y el marco normativo de desarrollo, siendo responsabilidad de la DGAD disponer los medios necesarios para que la información llegue a los afectados. Para ello, estará accesible por parte de todo el personal de la DGAD y externos que se vean involucrados en cualquiera de las actividades de la DGAD.
El personal de la DGAD deberá acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones y cuyo acceso haya sido autorizado. La utilizará exclusivamente para la realización de las distintas funciones operativas que desempeña para la organización. Cualquier acceso o utilización para finalidades distintas a las establecidas se considerará una infracción de la Política de Seguridad de la Información.
En conformidad con el 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), todo el personal que intervenga en cualquier fase del tratamiento de los datos de carácter personal está obligado a todos los requerimientos establecidos a tal efecto por la organización, incluyendo el secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el responsable de tratamiento o, en su caso, con el responsable del mismo. Por consiguiente, se comprometerá a guardar secreto sobre los datos personales a los que pudiera tener acceso por razones de su responsabilidad laboral, contractual o de cualquier otro tipo y a no vulnerar la normativa establecida al respecto.
Todo el personal de la DGAD será responsable de notificar cualquier tipo de incidencia o no conformidad que pudiera comprometer la seguridad de la información. Asimismo, deberá participar de forma activa en una cultura de prevención y protección de activos. Deberá para ello actuar de acuerdo a la presente política y aquellas normas y procedimientos de seguridad elaborados y comunicados por la organización.
Las violaciones o infracciones de la presente Política de Seguridad de la Información se sancionarán según el régimen disciplinario establecido por la propia organización, así como los derivados del "Estatuto Básico del Empleado Público" y del "Estatuto de los Trabajadores".

RELACIONES CON TERCEROS

Todo el personal externo que tenga acceso los recursos activos de información de la DGAD identificados en el capítulo de "Alcance" tiene la obligación de conocer y cumplir esta política y la normativa de seguridad derivada.
Para aquellas terceras partes a las que sean aplicables requisitos de seguridad, el contrato correspondiente incluirá la obligación del

cumplimiento de todos los requerimientos establecidos en la Política de Seguridad de la Información, Reglamento general de protección de datos y en general, todos aquellos que la DGAD considere de aplicación.
Los empleados de las compañías y terceros que presten servicios de cualquier índole a DGAD que tengan acceso a los recursos informáticos y telemáticos, así como a información de la organización, estarán obligados a cumplir con los requisitos de seguridad que se establezcan en la Política de Seguridad de la Información y en los documentos derivados de ella.
Serán responsables de notificar cualquier tipo de incidencia o no conformidad que pudiera comprometer la seguridad de la información.
Asimismo, deberán acceder exclusivamente a aquella información que sea estrictamente necesaria para el desempeño de sus funciones y cuyo acceso haya sido autorizado. La utilizarán exclusivamente para la realización de las distintas funciones operativas que desempeñan para la organización. Cualquier acceso o utilización para finalidades distintas a las establecidas se considerará una infracción de la Política de Seguridad de la Información.

ORGANIZACIÓN DE LA SEGURIDAD

Para el cumplimiento de la organización interna de la seguridad en la DGAD se emprenden las acciones siguientes:

1. Se dispondrá de un documento con las funciones y responsabilidades en materia de gestión de la seguridad de la información.
2. Establecer y aprobar las responsabilidades de la supervisión y el cumplimiento de las medidas de seguridad. Para ello, se asignarán diferentes responsables a las labores de seguimiento y cumplimiento de las mismas:

    - **Comité de Seguridad**
    - Política de Seguridad de la Información: Comité de Seguridad.
    - **Recursos Humanos**
    - Organización de la seguridad y contratación de terceros: Dirección General de Función Pública y la DGAD.
    - Recursos Humanos: Dirección General de Función Pública, DGAD, Servicio Riojano de Salud, Fundación Riojasalud.
    - **Área de Sistemas de Información**
    - Gestión de activos: DGAD.
    - Control de acceso: DGAD.
    - Criptografía: DGAD.
    - Gestión de comunicaciones y operaciones: DGAD.
    - Adquisición, desarrollo y mantenimiento de los sistemas de información: DGAD.
    - **Área de Seguridad Física**
    - Seguridad física y ambiental: Servicio Riojano de Salud y DGAD.
    - **Proveedores**
    - Gestión de proveedores: DGAD.
    - **Área de Seguridad de la Información**
    - Gestión de incidentes: DGAD.
    - Gestión de la continuidad de negocio: DGAD.
    - **Área jurídica**
    - Cumplimiento normativo: Gobierno de la Rioja y DGAD.

Estas áreas tendrán personal asignado y responsable de su gestión. La DGAD se encargará del procedimiento y renovación de las personas responsables. Igualmente, existirá un procedimiento que recoja el funcionamiento del Comité de Seguridad.
El personal de la DGAD recibirá formación de buenas prácticas en materia de seguridad de la información con la periodicidad adecuada para que puedan concienciarse adecuadamente y aplicar los conocimientos adquiridos. En particular, se tendrá en cuenta a las nuevas incorporaciones.

MARCO LEGAL Y REGULATORIO

Por su naturaleza, la DGAD está sometida a toda la normativa aplicable de la Unión Europea, española y de la Comunidad Autónoma de La Rioja.
La DGAD dispondrá de un listado de la legislación aplicable en el ámbito de la seguridad de la información que actualizará periódicamente. Entre otras, recogerá la siguiente legislación, que resulta de aplicación:

- Reglamento 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 derechos digitales.
- Real Decreto 3/2010, de 8 de enero, por la que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- 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.