Política de Seguridad de la Información

Índice

1. OBJETIVOS

El Consejo de Relaciones Laborales del País Vasco (en adelante, CRL) ha establecido un marco de gestión de la seguridad de la información según lo establecido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la administración electrónica, reconociendo así como activos estratégicos la información y los sistemas que la soportan.

El citado marco abarca igualmente la protección de datos de carácter personal y tiene en cuenta las disposiciones del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (en adelante RGPD), así como lo contemplado en la legislación de carácter nacional en dicha materia.

Uno de los objetivos fundamentales de la implantación de este marco de referencia es el asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos puedan acceder a los servicios en un entorno de gestión seguro, anticipándonos a sus necesidades, y preservando sus derechos.

Los objetivos generales en materia de seguridad de la información y protección de datos son los siguientes:

- Facilitar el cumplimiento de los objetivos y la misión de la Institución utilizando de forma segura los sistemas de información y las comunicaciones.
- Lograr una protección, proporcional al riesgo, de la información tratada y de los sistemas, dispositivos y elementos que soportan los servicios y procesos de tratamiento, mediante la preservación de las dimensiones de seguridad de la información, es decir, su autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad y conservación.
- Disponer de las medidas de seguridad necesarias para el cumplimiento de los requisitos legales de aplicación, especialmente en el ámbito de la protección de datos de carácter personal y la prestación de servicios a través de medios electrónicos.

La Política de Seguridad de la Información del CRL, en adelante la Política de Seguridad de la Información, es el instrumento en que se apoya el CRL para alcanzar sus objetivos. La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

2. ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para todos las personas que trabajan en el CRL, incluyendo a sus recursos y procesos afectados por el ENS y el RGPD, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

3. MISIÓN DE LA ENTIDAD

El CRL es una Institución pública de la Comunidad Autónoma del País Vasco, constituida como órgano de diálogo y encuentro permanente entre las confederaciones sindicales y empresariales y como órgano consultivo en materia sociolaboral respecto del Gobierno y del Parlamento vascos. Tiene personalidad jurídica propia y actúa con plena independencia en el desarrollo de sus funciones.

EI CRL para ejercer sus competencias hace uso de sistemas de información que deben ser protegidos de una forma efectiva y eficiente.

4. MARCO NORMATIVO

El marco normativo de las actividades del CRL en el ámbito de esta Política de Seguridad de la Información está integrado por las siguientes normas, sin carácter excluyente:

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 25/2007, de 18 de octubre, de Conservación de Datos Relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.
- Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.
- 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.
- 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.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico 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 (en adelante, Reglamento General de Protección de Datos o RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

5. ORGANIZACIÓN DE LA SEGURIDAD

La organización de la seguridad en el CRL queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades en la materia, y la implantación de la infraestructura que las soporte.

Con carácter general, todos y cada uno de los usuarios de los sistemas de información del CRL son responsables de la seguridad de los activos de información mediante un uso adecuado de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

A continuación, se describen las funciones y responsabilidades de los Órganos y Roles implantados en las diferentes escalas de gobierno, ejecutiva y operacional.

5.1. Órganos

5.1.1. Presidencia

En materia de seguridad de la información, el CRL, a través de la Presidencia del CRL o en quien delegue, tiene las siguientes obligaciones:

- Hacer cumplir las disposiciones establecidas en el ENS cuando el sistema de información se encuentre dentro del ámbito de aplicación del mismo y, en su caso, emitir directrices. De igual forma,las disposiciones de la normativa aplicable en materia de protección de datos personales (RGPD,LOPDGDD y otras normas que puedan identificarse)
- Aprobar la Política de Seguridad de la Información del CRL y cualquier otra política sectorial complementaria de la anterior, así como de todas aquellas modificaciones o actualizaciones de las mismas, que el Comité de Seguridad de la Información pueda proponer y permita el cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad, y de la normativa de protección de datos personales.

- Constituir y realizar el nombramiento de los integrantes del Comité de Seguridad de la Información.
- Realizar el nombramiento del Responsable de Seguridad de la Información y del Delegado de Protección de Datos, a propuesta del Comité de Seguridad de la Información.
- Aprobar el desarrollo organizativo propuesto por el Comité de Seguridad de la Información.
- Adoptar las medidas pertinentes, en materia de seguridad de la información, a propuesta del Comité de Seguridad de la Información.

5.1.2. Comité de Seguridad de la Información

El Comité de Seguridad de la Información tiene como finalidad velar por la seguridad de la servicios y activos de información en el CRL, asegurando y facilitando la correcta coordinación e integración de todas las actuaciones de los diversos órganos afectados en esta materia.

Para el cumplimiento de la finalidad descrita, el Comité de Seguridad de la Información es responsable de las siguientes funciones:

- Elaborar las propuestas de modificación y actualización de la Política de Seguridad de la Información, evaluando su idoneidad con una periodicidad mínima anual y proponiendo a la Presidencia del Consejo, a través del Presidente del Comité de Seguridad de la Información, su aprobación y revisión cuando proceda.
- Elaborar y proponer las políticas sectoriales que complementen a la política de seguridad de la información, así como cambios sobre éstas, con el objetivo de cumplir con los esquemas nacionales de seguridad e interoperabilidad.
- Elaborar y proponer el desarrollo organizativo que permita el cumplimiento de los esquemas nacionales de seguridad e interoperabilidad, en el ámbito de la Institución.
- Proponer las designaciones de Responsable de Seguridad de la Información, y Delegado de Protección de Datos
- Velar por el cumplimiento y difusión de la Política de Seguridad de la Información, promoviendo las actividades de concienciación y formación en materia de seguridad de la información para el personal del CRL.
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- Elevar a la Presidencia a través del Presidente del Comité de Seguridad de la Información, para su aprobación, las resoluciones necesarias para el desarrollo de la Política de Seguridad de la Información.
- Difundir los acuerdos aprobados por el Comité a toda la Institución.
- Resolver los conflictos que pudieran surgir en la interpretación y aplicación de la Política de Seguridad de la Información y su desarrollo entre los diferentes responsables, escalándolos a la Presidencia del Consejo si fuese necesario.
- Proponer a la Presidencia a través del Presidente del Comité de Seguridad de la Información, para su aprobación, las directrices para coordinar la comunicación del CRL con el Centro Criptológico Nacional y la Autoridad de Control de protección de datos.
- Recabar informes regulares del estado de seguridad de la información de la Institución y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la Presidencia a través del Presidente del Comité de Seguridad de la Información, al Responsable de Seguridad y a los diferentes grupos de trabajo que se pudieran crear como apoyo en la gestión de la seguridad de la información.

- Promover inversiones racionales y proporcionadas de carácter horizontal para garantizar la disponibilidad de recursos para atender a las diferentes necesidades de seguridad de la información.
- Definir criterios de valoración para los diferentes tipos de información manejados y los diferentes servicios prestados con el fin de armonizar los análisis de riesgos de los diferentes sistemas de información.
- Proponer a la Presidencia a través del Presidente del Comité de Seguridad de la Información, para su aprobación, la Declaración de Aplicabilidad, establecida en la regulación del ENS, de la información, servicios y sistemas de información del CRL.

5.2. Roles

5.2.1. Presidente del Comité de Seguridad de la Información

La Presidencia del Comité de Seguridad de la Información corresponderá a la persona designada como Responsable de Seguridad de la Información del CRL.

Las funciones del Presidente son las siguientes:

- Ostentar la representación del Comité de Seguridad de la Información.
- Acordar las convocatorias de las sesiones y determinar el orden del día.
- Presidir las sesiones y moderar los debates que pudieran originarse.
- Concluir los empates en la toma de decisiones, si estos se dieran, con su voto de calidad.
- Asegurar el cumplimiento de las leyes.
- Visar las actas y propuestas adoptadas por el Comité de Seguridad de la Información, así como las certificaciones de sus acuerdos.
- Remitir a la Presidencia los acuerdos y resoluciones del Comité de Seguridad de la Información para su aprobación cuando ello fuese procedente.
- Nombrar a los titulares de las Vocalías y de la Secretaría del órgano.
- Ejercer cuantas otras funciones sean inherentes a su condición.

5.2.2. Vocalías del Comité de Seguridad de la Información

Serán titulares de las Vocalías del Comité de Seguridad de la Información las personas con los siguientes roles asignados:

- El Responsable de Sistemas.
- El Delegado de Protección de Datos.

Las vocalías tendrán asignadas las siguientes funciones:

- Asistir a las reuniones, participar en los debates y formular ruegos y preguntas.
- Ejercer su derecho de voto, manifestar el sentido del mismo, así como los motivos que lo justifican.
- Ejercer aquellas funciones que le sean encomendadas expresamente por el Comité o la Presidencia de éste.
- Velar por que la Política de Seguridad de la Información y su desarrollo sea difundida y aplicada en el ámbito en el que ejercen su representación.
- Obtener la información lo más precisa posible para cumplir las funciones asignadas.
- Ejercer cuantas otras funciones sean inherentes a su condición.

5.2.3. Secretaria del Comité de Seguridad de la Información

La Secretaría del Comité de Seguridad de la Información será designada por la Presidencia de éste entre el personal funcionario adscrito al CRL, y no ostentará la condición de vocal.

Las funciones del Secretario son las siguientes:

- Asistir a las reuniones con voz pero sin voto.
- Gestionar las convocatorias de las sesiones por orden de la Presidencia del Comité.
- Preparar el salón destinado a las sesiones.
- Redactar las actas de las sesiones, autorizándolas con su firma y el visto bueno de la Presidencia del Comité.
- Expedir certificaciones de las consultas, dictámenes y acuerdos aprobados con el visto bueno de la Presidencia del Comité.
- Recibir las comunicaciones de cada miembro del órgano y, por tanto, las notificaciones, peticiones de datos, rectificaciones o cualquier otra clase de escritos de los que deba tener conocimiento.
- Ejercer cuantas otras funciones sean inherentes a su condición.

5.2.4. Otros asistentes del Comité de Seguridad de la Información

Quienes por razones de su función, conocimiento o especialización hayan sido convocados a alguna sesión del Comité de Seguridad de la Información podrán asistir con voz, no así voto.

5.2.5. Responsable de Seguridad de la Información

El Responsable de Seguridad de la Información es el encargado de determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Se designa como Responsable de Seguridad de la Información al Secretario General del Consejo de Relaciones Laborales.

Las funciones del Responsable de Seguridad de la Información son las siguientes:

- Determinar las decisiones necesarias para satisfacer los requisitos de seguridad de la información y de los servicios establecidos por sus respectivos responsables.
- Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
- Analizar y elevar al Comité de Seguridad de la Información toda la documentación relacionada con la seguridad de los sistemas de información para su aprobación.
- Realizar el seguimiento y control del estado de seguridad de los sistemas de información, verificando que las medidas de seguridad son adecuadas a través del análisis de riesgos.
- Establecer el conjunto de proyectos y actuaciones que conformarán el plan director de seguridad que permitirá implantar las medidas de seguridad propuestas y elevarlo al responsable del sistema de Información.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar informes periódicos de seguridad para el Comité de Seguridad de la Información, que incluirán los incidentes más relevantes de cada periodo.
- Realizar o promover auditorias periódicas para garantizar la correcta aplicación de las medidas de seguridad y el cumplimiento de las normas y procedimientos vigentes en la organización en materia de seguridad de la información. El informe resultante de las mismas se enviará a los

responsables de los sistemas de Información y al responsable de la prestación del servicio para subsanar las deficiencias encontradas.

- Determinar y establecer la metodología y herramientas para llevar a cabo el análisis de riesgos.
- Redactar cuando sea necesario las declaraciones de aplicabilidad de los sistemas de Información respecto al ENS.
- Elaborar, junto los responsables de los servicios y sistemas, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

5.2.6. Responsable del Servicio y de la Información

El Responsable del Servicio y de la Información, es el titular del servicio con competencia suficiente para decidir sobre la finalidad y prestación del correspondiente servicio, así como sobre la finalidad, contenido y uso de la información tratada. De igual manera, es el responsable de determinar los requisitos de seguridad dentro del marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

Las funciones del Responsable del Servicio y de la Información son las siguientes:

- Determinar y mantener actualizados los niveles de seguridad del servicio e información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del ENS.
- Realizar, junto al Responsable de Seguridad de la Información, los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se han de implantar.
- Aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.
- Realizar, junto al Responsable de Seguridad de la Información, el seguimiento y control de los riesgos.
- Suspender, de acuerdo con el Responsable de Seguridad de la Información, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.
- Elaborar, junto con el Responsable de Seguridad de la Información, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

5.2.7. Responsable de Sistemas

El Responsable de Sistemas es un puesto operativo designado por el Comité de Seguridad de la Información entre el personal funcionario adscrito al CRL, encargado de la explotación de los sistemas de la Institución. Este rol es el equivalente al “Responsable del Sistema” enunciado en el ENS.

Las funciones del Responsable de Sistemas son las siguientes:

- Desarrollar, operar y mantener los Sistemas de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión de los Sistemas de Información estableciendo los criterios de uso y los servicios disponibles en los mismos.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes de los sistemas durante las etapas de desarrollo, instalación y prueba de los mismos, cerciorándose de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- El Responsable de Sistemas puede 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 del servicio y la información afectados y el Responsable de la Seguridad, antes de ser ejecutada.

- Elaborar, junto con el Responsable de Seguridad de la Información, los procedimientos operativos de seguridad, así como los planes de continuidad y respuesta a incidentes.

5.2.8. Administrador del Sistema

El Administrador del Sistema es un puesto operativo designado por el Comité de Seguridad de la Información entre el personal funcionario adscrito al CRL y el personal ajeno a la entidad que presta servicios de Tecnologías de Información y Comunicación, encargado de las labores de soporte y mantenimiento del sistema.

Las funciones del Administrador del Sistema son las siguientes:

- Implementar y controlar las medidas de seguridad aplicables al Sistema de Información, asegurándose de su cumplimiento.
- Gestionar el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información, llevando un control sobre su configuración y actualización para mantener un nivel de seguridad adecuado.
- Aplicar los procedimientos operativos de seguridad aprobados, así como asegurar su aplicación.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de Seguridad de la Información y al Responsable de Sistemas 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.

5.2.9. Responsable del Tratamiento

De acuerdo a las disposiciones del RGPD, el Responsable del Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Este rol, que recae sobre el Consejo de Relaciones Laborales, será desempeñado por el correspondiente Responsable del Servicio y de la Información o, en su ausencia, por la Presidencia del Consejo.

Las funciones y obligaciones del Responsable de Tratamiento son:

- Aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.
- Cumplir con el deber de información a los interesados, recoger su consentimiento cuando sea preciso y velar por sus derechos y libertades.
- Mantener un registro de actividades de tratamiento (artículo 30 del RGPD) que constará por escrito, inclusive en formato electrónico.
- Elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.
- Subscribir un contrato u acto jurídico con el responsable (artículo 28 del RGPD) que constará por escrito, inclusive en formato electrónico. Este contrato deberá establecer el objeto, la duración,

la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

- Comunicar las violaciones de seguridad a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.
- Designar a un Delegado de Protección de Datos en los casos previstos en el artículo 37 RGPD y en el artículo 34 de la LOPDGDD.

5.2.10. Delegado de Protección de Datos

De acuerdo a las disposiciones del RGPD, el Delegado de Protección de Datos es el encargado de garantizar el cumplimiento de la normativa de protección de datos. Este rol es designado por el Comité de Seguridad de la Información entre el personal funcionario adscrito al CRL y el personal ajeno a la entidad que presta servicios de asesoramiento especializado, y podrá ser compartido por diversas personas físicas o jurídicas.

Las funciones del Delegado de Protección de Datos son las siguientes:

- 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 presente 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 del RGPD.
- 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.

5.2.11. Encargado de Tratamiento

De acuerdo a las disposiciones del RGPD, el Encargado de Tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, trate datos personales por cuenta del Responsable del Tratamiento.

Las funciones y obligaciones del Encargado de Tratamiento son las siguientes:

- Subscribir un contrato u acto jurídico con el responsable (artículo 28 del RGPD) que constará por escrito, inclusive en formato electrónico. Este contrato deberá establecer el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.
- Cumplir con los establecido en el contrato, tratando los datos personales únicamente para las finalidades acordadas con el responsable; siguiendo sus instrucciones documentadas, y asistiéndole para el cumplimiento de sus obligaciones.
- Mantener un registro de actividades de tratamiento (artículo 30 del RGPD) que constará por escrito, inclusive en formato electrónico.

- Cooperar con la autoridad de control (artículo 31 del RGPD), facilitando la información que esta le solicite y cumpliendo lo que esta ordene en el desempeño de sus funciones.
- Determinar las medidas de seguridad aplicables a los tratamientos que lleven a cabo (artículos 32 y 33 del RGPD), para garantizar un nivel de seguridad adecuado al riesgo y el cumplimiento por parte del personal de las limitaciones del contrato y de la legislación aplicable.
- Comunicar las violaciones de seguridad, de las que tenga conocimiento, al responsable (artículo 33.2 del RGPD) sin dilación indebida.
- Designar a un Delegado de Protección de Datos en los casos previstos en el artículo 37 RGPD y en el artículo 34 de la LOPDGDD.

5.3. Procedimiento de designación

Corresponde a la Presidencia del CRL el nombramiento y el cese de los componentes del Comité de Seguridad de la Información, para el ejercicio de las competencias definidas en la presente política. De igual forma, será la Presidencia quien realice los nombramientos del Responsable de Seguridad de la Información, y del Delegado de Protección de Datos.

Dada su relevancia, los nombramientos de los miembros del Comité de Seguridad de la Información, del Responsable de Seguridad de la Información, y del Delegado de Protección de Datos serán revisados cada 4 años, o cuando haya algún cambio en la Organización o algún puesto quede vacante.

6. SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

El CRL establecerá medidas de seguridad para todo el personal desde el proceso de inicio de la relación hasta el cese de ésta. Dichas medidas se compartirán con todas las personas y terceras entidades que colaboren directa o indirectamente con el CRL.

En particular, se llevarán a cabo actividades de formación y concienciación para que el personal sea plenamente consciente de su responsabilidad con la seguridad de la información que afecta a todas las actividades y miembros de la entidad, así como tengan una sensibilidad hacia los riesgos que se corren.

El objetivo es lograr la plena conciencia respecto a que la seguridad de la información esta repartida y distribuida entre todos los usuarios y las actividades de la Institución, de acuerdo al principio de Seguridad Integral recogido en el Artículo 5 del ENS, así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

7. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán ser sometidos a un proceso de gestión de riesgos, evaluando los riesgos a los que están expuestos y tratándolos con las contramedidas que sean necesarias para mitigarlos. El análisis comprendido en el proceso se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves

Para el análisis y gestión del riesgo se sigue la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) elaborada por el Consejo Superior de Administración Electrónica y enfocada a las Administraciones Públicas.

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. 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.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información se desarrollará por medio de una Normativa de Seguridad que afronte aspectos específicos del CRL.

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

9. OBLIGACIONES DEL PERSONAL

Tanto el personal perteneciente al CRL, como aquellas personas que dispongan de alguna vinculación profesional directa o indirecta con el mismo, deberán cumplir con la presente Política de Seguridad de la Información y su normativa de desarrollo (la cual comprende la Normativa de Uso de Sistemas e Información), en su ámbito de actuación. Es responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros del CRL atenderán a sesiones de concienciación en materia de seguridad con una periodicidad acordada por el Comité de Seguridad de la Información, y reflejada en el plan de formación y concienciación.

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.

10. TERCERAS PARTES

Cuando el CRL preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes 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 el CRL utilice servicios de terceros, facilite acceso a sus sistemas o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que corresponda. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos para el reporte y resolución de incidencias, y el intercambio de información confidencial, entre otros.

Será obligación de las terceras partes el poner en conocimiento de su personal la Política de Seguridad y de la Normativa de Seguridad que corresponda, y trasladar de forma expresa al CRL que se conoce y se comprometen a respetarla, así como asumir las responsabilidades que deriven de su incumplimiento. De igual manera 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 de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11. CONFIDENCIALIDAD DE LA INFORMACIÓN

11.1. Definición de información confidencial

Tendrá la consideración de información confidencial cualquier información no divulgada o publicada oficialmente por el CRL o en cumplimiento de la legalidad vigente.

La información confidencial puede estar recogida en forma oral, visual, escrita, grabada en medios magnéticos o en cualquier otro medio o soporte, tangible o intangible, marcada o no como “confidencial”, e incluir información generada por personal del CRL o facilitada por terceras partes con las que el CRL tenga algún tipo de relación establecida. La información confidencial incluye asimismo los datos de carácter personal.

No podrá ser considerada como confidencial la información que sea susceptible de ser conocida mediante la utilización de canales regulares y legales de información, ni la información que sea de público conocimiento.

11.2. Compromiso

Toda persona, y desde este momento todos los empleados, sin perjuicio de que el compromiso esté establecido en su contrato o no, que acceda a información confidencial en el CRL debe firmar un acuerdo de confidencialidad que recoja de forma explícita e inequívoca la obligación de utilización restrictiva de la información confidencial y la obligación de mantenerla en secreto, limitando su acceso y divulgación.

La presente obligación será exigida al personal del CRL con independencia de que hayan firmado o no la correspondiente cláusula de confidencialidad en sus respectivos contratos. Esta obligación continuará vigente tras la extinción de la relación laboral que le una con la Institución.

11.3. No revelación

La información confidencial no puede ser revelada, salvo que exista autorización previa que lo permita. Dicha autorización debe ser otorgada de forma expresa y por escrito, debe limitarse a los términos estrictamente necesarios, y en todo caso, debe ser interpretada de la forma más restrictiva.

Esta prohibición incluye la revelación de información confidencial del CRL a través de redes sociales personales o formas de comunicación análogas que utilicen empleados del CRL o personal colaborador.

11.4. Utilización

La utilización de la información confidencial debe ser restringida a lo estrictamente necesario para el desarrollo de la actividad laboral o profesional, debe respetar las leyes y normativas aplicables, los contratos de confidencialidad suscritos y las políticas y códigos internos, particularmente la presente política de confidencialidad.

No está permitido el archivo, recopilación, manipulación o tratamiento en cualquier forma de la información confidencial a menos que existan razones laborales o profesionales que lo justifiquen. En todo caso se establecerán las medidas necesarias para garantizar su confidencialidad.

11.5. Devolución o destrucción

Las personas que posean información confidencial del CRL, bajo cualquier tipo de soporte, documentación o fichero deberán entender que dicha posesión es estrictamente temporal, y sin que ello les arrogue derecho alguno de propiedad o copia sobre la misma.

Asimismo, deberán devolver dichos materiales a la Institución inmediatamente después de la finalización de las tareas que han motivado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación contractual. En caso de que dichos materiales ya no sean necesarios y se disponga de autorización para ello, deberán destruirlos de acuerdo a las disposiciones de la normativa una vez finalizadas las tareas.

12. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

El CRL, en el desarrollo de sus funciones, requiere hacer uso de datos de carácter personal. Por ello, se garantizarán los derechos y libertades de los interesados, así como la seguridad de la información, de las comunicaciones y de los sistemas de información que soportan los tratamientos de acuerdo con las medidas previstas en la legislación vigente.

Para lograr las necesarias garantías se realizarán todas las acciones pertinentes de las siguientes:

- La realización de análisis de riesgos sobre los tratamientos, y evaluaciones del impacto en la privacidad cuando sea probable que los tratamientos entrañen un alto riesgo para los derechos y libertades de los afectados.
- El diseño e implantación de medidas técnicas y organizativas para mitigar los riesgos relativos a los tratamientos de datos de carácter personal por defecto y desde el diseño.
- El rediseño de los procesos para mitigar los riesgos que no puedan mitigarse y asumirse.
- La elaboración de toda la documentación necesaria para soportar los procesos y garantizar los derechos y libertades de los afectados, cumpliendo con los principios establecidos por la normativa vigente.
- El traslado de las obligaciones a todo el personal que tenga acceso a los datos de carácter personal.
- La gestión de las relaciones con encargados de tratamiento en base a unos criterios establecidos, incluyendo la regulación a través de contratos que formalicen las obligaciones y los requisitos de seguridad.
- El mantenimiento de un registro de actividades de tratamiento.
- La información en los plazos requeridos, en base a las disposiciones de las leyes aplicables, a la correspondiente autoridad competente de protección de datos de lo siguiente:
  - Los tratamientos realizados.
  - Los resultados de las evaluaciones de impacto realizadas.
  - Las transferencias internacionales fuera de la Unión Europea (UE) que se vayan a llevar a cabo.
  - El nombramiento y datos de contacto de la figura de Delegado de Protección de Datos (DPD).
  - Las violaciones de seguridad que conlleven una probabilidad de riesgo contra los derechos y libertades de los interesados, dentro de las 72h siguientes a su detección.
  - Cualquier otra información que sea requerida por una ley o por indicaciones de la citada autoridad competente de protección de datos.
- La información por capas sobre los tratamientos a los afectados por los mismos, de forma concisa, transparente, inteligible y de fácil acceso.
- La recogida del consentimiento de los afectados de forma expresa e inequívoca, y previamente al inicio de los tratamientos y/o establecimiento de cesiones.

- La notificación a los afectados de violaciones de seguridad que supongan un alto riesgo contra sus derechos y libertades, dentro de las 72h siguientes a su detección.

13. PROCEDIMIENTO DE REVISIÓN

Será misión del Comité de Seguridad de la Información, la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma.

Si procediera la elaboración y propuesta de una modificación y/o actualización, la Política será remitida por el Comité de Seguridad de la Información y tras su aprobación será difundida por el Comité de Seguridad de la Información para que la conozcan todas las partes afectadas.

14. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 6 de mayo de 2019 por el Presidente.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

15. HISTORIAL DE MODIFICACIONES

HISTORIAL DE CAMBIOS		
Versión	Fecha	Descripción del Cambio
001	08/4/2019	Primera versión del documento