8 de noviembre de 2024

XI LEGISLATURA

Serie C
General
N.º 227

SUMARIO

Boletín Oficial DEL PARLAMENTO DE LA RIOJA

Depósito Legal: LR-37-1999 / ISSN: 1139-8337

RÉGIMEN INTERNO

La Mesa del Parlamento de La Rioja, en su reunión celebrada el día 23 de octubre de 2024, ha adoptado, sobre el asunto de referencia, el acuerdo que se indica.

11L/RI-0148. Documento de Política de Seguridad de la Información del Parlamento de La Rioja.

Acuerdo:

Visto escrito, registrado de entrada con el n.º 12294 en fecha 14 de octubre de 2024, que presenta el letrado mayor del Parlamento de La Rioja, elevando el Documento de Política de Seguridad de la Información del Parlamento de La Rioja, aprobado por el Grupo de Trabajo de Administración Electrónica.

La Mesa de la Cámara, en ejercicio de las competencias que le atribuye el artículo 28 de su Reglamento, acuerda lo siguiente:

1. Aprobar el Documento de Política de Seguridad de la Información del Parlamento de La Rioja.

2. Disponer, de conformidad con lo dispuesto en el artículo 81.1 del Reglamento de la Cámara, la publicación de este acuerdo en el Boletín Oficial de este Parlamento.

Logroño, 28 de octubre de 2024. La presidenta del Parlamento: Marta Fernández Cornago.

Política de Seguridad de la Información

1. Introducción.

El Parlamento de La Rioja está comprometido con proteger la confidencialidad, la integridad, la autenticidad, la trazabilidad y la disponibilidad de la información utilizada en la institución, así como sus canales de transmisión y/o comunicación, para ofrecer al ciudadano un servicio de administración electrónica de confianza, potenciando el uso de las tecnologías de la información y la comunicación (TIC).

Para ello, dispone de un sistema de gestión de seguridad de la información y se establecen las responsabilidades sobre el acceso y utilización de la información.

2. Justificación de la política de 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. La dependencia de los sistemas TIC del Parlamento de La Rioja hace indispensable la necesidad de proteger la información contra amenazas que puedan incidir en la confidencialidad, integridad o disponibilidad de esta. Para ello, se requiere de una estrategia que se adapte a los constantes cambios a los que la sociedad está expuesta para garantizar la prestación de los servicios.

Todas las áreas del Parlamento de La Rioja deben cerciorarse de que la seguridad en los sistemas TIC es una parte integral de cada etapa del ciclo de vida de estos, 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. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

3. Alcance.

Esta política se aplica a todos los sistemas y las tecnologías de la información y la comunicación de los que haga uso el Parlamento de La Rioja.

El presente documento se aplica a cualquier persona que haga uso o tenga acceso a información propiedad del Parlamento de La Rioja gestionada a través de sus sistemas.

Todas las personas que mantienen una relación contractual o estatutaria con el Parlamento de La Rioja, así como sus miembros electos, tienen la obligación de conocer y cumplir esta política y la normativa de seguridad desarrollada a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información (CSI) disponer de los medios necesarios para que la información llegue a las personas y/o servicios afectados.

4. Referencias.

Para el desarrollo del presente documento se ha tenido en consideración el siguiente conjunto de normas que forman el marco normativo de aplicación:

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

5. Principios y objetivos de seguridad.

El Parlamento de La Rioja entiende la seguridad como un concepto integral y, en este sentido, la toma de decisiones en la materia se rige por los principios básicos enunciados en el Esquema Nacional de Seguridad (artículo 5):

a) Seguridad como proceso integral.

b) Gestión de la seguridad basada en los riesgos.

c) Prevención, detección, respuesta y conservación.

d) Existencia de líneas de defensa.

e) Vigilancia continua.

f) Reevaluación periódica.

g) Diferenciación de responsabilidades.

El Parlamento de La Rioja, como soporte de los principios de seguridad de la información establecidos, ofrece, según el ENS, los siguientes objetivos de partida:

Fomentar la relación electrónica del ciudadano con el Parlamento de La Rioja.

Reducir tiempos de espera de atención al ciudadano.

Acortar tiempos de espera en la resolución de trámites solicitados por el ciudadano.

Mejorar el uso interno de los sistemas de información del Parlamento de La Rioja.

Desarrollar un sistema de gestión de información documental que facilite un rápido acceso del personal

del Parlamento de La Rioja a la información solicitada por el ciudadano, garantizando la seguridad de la información en cuanto a su integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad.

Facilitar el acceso a los documentos custodiados en el Archivo de la Cámara con sujeción a las normas que apliquen en cada caso, relativas a la seguridad de la información y a la protección de datos personales.

Cumplir con los requisitos exigidos por la normativa vigente de protección de datos de carácter personal y de impulso de las administraciones públicas.

Mantener, operar y evolucionar un sistema de gestión de la seguridad.

6. Requisitos mínimos de seguridad.

Atendiendo al cumplimiento del Esquema Nacional de Seguridad, se garantizará el cumplimiento de los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad: detallada en el apartado 7 del presente documento.

b) Análisis y gestión de los riesgos de seguridad: se realizarán periódicamente análisis de los riesgos a los que se encuentren expuestos la información y los servicios. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

c) Gestión de personal: el personal del Parlamento de La Rioja será formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad.

d) 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 incidentes y desmantelamiento). El personal técnico del Parlamento de La Rioja recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la institución. Asimismo, solo prestarán servicios al Parlamento de La Rioja aquellas entidades que cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

e) Autorización y control de los accesos: el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

f) Protección de las instalaciones: los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

g) Adquisición de productos de seguridad y contratación de servicios de seguridad: se utilizarán de forma proporcionada a la categoría del sistema y del nivel de seguridad aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo que un riesgo superior lo justifique a juicio de la persona responsable de seguridad.

h) Mínimo privilegio: se otorgarán a los usuarios de los sistemas los mínimos privilegios necesarios para el correcto desempeño de su actividad profesional, incluyendo las funciones de operación y administración, en su caso.

i) Integridad y actualización del sistema: todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

j) Protección de la información almacenada y en tránsito: se prestará especial atención a la información almacenada o en tránsito a través de entornos potencialmente inseguros (equipos portátiles, dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil). Toda información en soporte no electrónico que haya sido causa o consecuencia directa de información electrónica deberá estar protegida con el mismo grado de seguridad que esta.

k) Prevención ante otros sistemas de información interconectados: se establecerá un sistema de

seguridad perimetral para restringir el acceso a los sistemas internos, bloquear la entrada de contenido malicioso a la red privada y evitar la filtración de datos y el uso no autorizado de los sistemas corporativos, en particular, si se establecen conexiones a redes públicas.

l) Registro de actividad y detección de código dañino: se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa con el fin único de dar cumplimiento al objeto del Esquema Nacional de Seguridad y con plena garantía de derecho al honor e intimidad de la persona, incluyendo el cumplimiento de la normativa en materia de protección de datos personales.

m) Incidentes de seguridad: atención y gestión de eventos de seguridad para garantizar la continuidad de los servicios.

n) Continuidad de la actividad: se establecerán mecanismos para garantizar la disponibilidad de los servicios en caso de incidente de seguridad que afecte a la disponibilidad de los sistemas.

ñ) Mejora continua del proceso de seguridad. el proceso integral de seguridad implantado será actualizado y mejorado de forma continua.

7. Definición de roles.

Tal como indica el artículo 13 del Esquema Nacional de Seguridad, la seguridad deberá comprometer a todos los miembros de la organización. La organización de la seguridad de la información en el Parlamento de La Rioja queda establecida mediante la identificación y definición de las diferentes actividades y responsabilidades. No se identifican responsables de servicio ya que quedan embebidos en la composición del Comité de Seguridad de la Información.

7.1. Responsable de la información.

Se designa al Comité de Seguridad de la Información, que tendrá las siguientes funciones:

Adoptar las medidas técnicas y organizativas necesarias que garanticen la seguridad de los tratamientos de datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

Responsabilidad última del uso de la información, así como de su protección.

Responsabilidad última sobre cualquier error o negligencia que implique un incidente de seguridad.

Establecer los niveles de seguridad de la información.

Determinar los niveles de seguridad en cada dimensión dentro del marco establecido en el anexo I del Esquema Nacional de Seguridad.

Aunque la aprobación formal de los niveles corresponda a quien sea responsable de la información, podrá recabar una propuesta de la persona responsable de la seguridad, oída aquella que tenga el rol de responsable del sistema.

El Comité de Seguridad de la Información del Parlamento de La Rioja tendrá la siguiente composición:

Presidente/presidenta: la persona que ostente el cargo de letrado mayor del Parlamento de La Rioja.

Vocales: una persona representante por cada una de las áreas establecidas en el artículo 5 del Reglamento de régimen interno y gobierno interior de la Secretaría del Parlamento de La Rioja que tenga vinculación con la seguridad de la información o los datos personales.

Secretario/secretaria: asumido por un letrado o una letrada del Parlamento de La Rioja, que se encargará de coordinar las actuaciones necesarias para el desarrollo de las sesiones del comité y supervisará

las actas de las sesiones que redactará el prestador de servicios de protección de datos y ENS del Parlamento de La Rioja.

El Comité de Seguridad de la Información deberá reunirse al menos una vez al año y, de forma extraordinaria, cuando lo requiera la persona responsable de seguridad, o a petición de la persona responsable del sistema.

Podrán acudir a requerimiento del Comité de Seguridad de la Información cualesquiera otros jefes o jefas de servicio o área y responsables cuya intervención sea precisa.

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

a) Atender las cuestiones en materia de seguridad que se planteen.

b) Garantizar el cumplimiento de la legislación en materia de seguridad que sea aplicable.

c) Informar regularmente del estado de la seguridad de la información a la Mesa de la Cámara.

d) Promover la realización de análisis de riesgos a la persona responsable de seguridad en el ámbito del ENS y del RGPD.

e) Aprobar y revisar la idoneidad de las medidas de seguridad aplicadas en el ámbito del Parlamento de La Rioja, priorizándolas cuando los recursos sean limitados.

f) Aprobar planes y programas de concienciación y/o formación del personal en materia de seguridad de la información y protección de datos personales.

g) Divulgar entre el personal del Parlamento de La Rioja la normativa e instrucciones de seguridad de la información aprobadas.

h) Velar por que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en producción.

i) Supervisar la gestión de incidentes de seguridad, velando por que sean registrados, resueltos y evaluados.

j) Proponer planes de mejora de la seguridad de la información y la protección de datos personales en la institución.

7.2. Responsable de seguridad.

Se designa a quien ostente el cargo de letrado mayor del Parlamento de La Rioja, a quien le corresponden las siguientes funciones:

Reportar directamente al Comité de Seguridad de la Información.

Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.

Promover la formación y la concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad y participar en la elaboración de una planificación al respecto.

Recopilar los requisitos de seguridad de las personas responsables de la información y determinar la categoría del sistema.

Realizar el análisis de riesgos.

Elaborar 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.

Facilitar, a la persona responsable de la información, la información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos.

Participar en la elaboración y aprobación, en el marco del Comité de Seguridad de la Información, de la normativa de seguridad de la información.

Facilitar periódicamente al Comité de Seguridad de la Información un resumen de actuaciones en

materia de seguridad, de incidentes relativos a la seguridad de la información y del estado de la seguridad del sistema.

Elaborar, junto a la persona responsable del sistema, planes de mejora para su aprobación por el Comité de Seguridad de la Información.

Validar los planes de continuidad de los sistemas que elabore la persona responsable del sistema, que deberán ser aprobados por el Comité de Seguridad de la Información y probados periódicamente por la persona responsable del sistema.

7.3. Responsable del sistema.

Se designa como responsable del sistema al Servicio de Sistemas de Información y Archivo, al que le corresponden las siguientes funciones:

Desarrollar, operar y mantener las medidas de seguridad de carácter técnico del sistema de información durante todo su ciclo de vida, de sus especificaciones técnicas, instalación y verificación de su correcto funcionamiento.

Gestionar, configurar y actualizar, según corresponda, el *hardware* y el *software* en los que se basan los mecanismos y los servicios de seguridad del sistema de información.

Definir la topología y la gestión del sistema de información. Para ello, establecer y gestionar las autorizaciones de acceso a la información de los usuarios del sistema, en particular, los privilegios concedidos y los criterios de uso de acuerdo con dichos privilegios.

Garantizar las medidas de seguridad de carácter técnico y que se integren adecuadamente dentro del marco general de seguridad establecido.

Acordar, en su caso, la suspensión del acceso a determinada información o la prestación de un servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la aplicación de los requisitos establecidos. Esta decisión debe ser acordada con la persona responsable de la seguridad y con el Comité de Seguridad de la Información antes de ser ejecutada.

Aplicar los procedimientos operativos de seguridad elaborados y aprobados por la persona responsable de seguridad.

Monitorizar el estado de la seguridad del sistema de información y reportarlo periódicamente o ante incidentes de seguridad relevantes a la persona responsable de seguridad.

Elaborar los planes de continuidad del sistema para que sean validados por la persona responsable de seguridad y coordinados y aprobados por el Comité de Seguridad de la Información.

Supervisar la instalación del *hardware* y del *software* que conforman el sistema de información. Realizar ejercicios y pruebas periódicas de los planes de continuidad del sistema para mantenerlos actualizados y verificar que son efectivos.

Elaborar las directrices necesarias para tener en cuenta la seguridad de la información durante todo el ciclo de vida de los activos y procesos (especificación, arquitectura, desarrollo, operación y cambios). Además, deberá facilitar dichas directrices a la persona responsable de seguridad de la información para su aprobación.

7.4. Delegado de Protección de Datos.

El Parlamento de La Rioja cuenta con un servicio externo de Delegado de Protección de Datos (DPD). A continuación, sin perjuicio de las que legalmente le corresponden, se establecen las siguientes responsabilidades:

Supervisar el cumplimiento de los principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.

Identificar las bases jurídicas de los tratamientos.

Supervisar el cumplimiento de lo dispuesto en la normativa vigente en materia de protección de datos de la Unión Europea o de los Estados miembros, así como de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales. Supervisión del diseño e implantación de medidas de información a los afectados por el tratamiento de datos personales.

Establecer mecanismos de recepción y atención de las solicitudes de ejercicio de derechos por parte de los interesados.

Colaborar con el Parlamento de La Rioja en la valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

Revisar los documentos relativos a la contratación de los encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.

Identificar los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.

Supervisar del diseño e implantación de políticas de protección de datos y asignación de responsabilidades.

Coordinar las auditorías de protección de datos.

Revisar el establecimiento y gestión de los registros de actividades de tratamiento.

Supervisar los análisis de riesgos de los tratamientos realizados.

Revisar y proponer la implantación de las medidas de protección de datos desde el diseño y, por defecto, adecuadas a los riesgos y naturaleza de los tratamientos realizados sobre los datos personales.

Revisar y proponer la implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.

Establecer procedimientos de gestión de brechas de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.

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 las autoridades de control y atención a los requerimientos que pudieran ser emitidos por estas.

Implantar programas de formación y sensibilización del personal en materia de protección de datos.

Resolver las consultas que realicen los miembros de Comité de Seguridad de la Información o el personal del Parlamento de La Rioja encargado del tratamiento de datos personales.

7.5. Funciones y obligaciones de los usuarios con acceso a datos.

El Parlamento de La Rioja facilitará las pautas y directrices a los usuarios sobre el tratamiento de la información, el acceso a la misma y el mantenimiento de su confidencialidad. Los usuarios notificarán cualquier circunstancia que pueda provocar potencialmente un incidente o brecha de seguridad.

8. Revisión y auditoría de los sistemas.

Los sistemas de información comprendidos en el ámbito de aplicación del ENS y del RGPD serán susceptibles de auditoría y evaluación a intervalos planificados, con el objetivo de garantizar su continuidad en los niveles adecuados de calidad en cuanto a la protección de la información y en el ejercicio de los servicios a la ciudadanía.

Las auditorías deberán realizarse al menos cada dos años, si bien siempre se realizarán en caso de cambios significativos, a fin de asegurar que se mantenga la idoneidad, adecuación y eficacia de lo descrito.

Los cambios introducidos tras las auditorías deberán ser aprobados posteriormente por la Mesa de la Cámara. Dichos cambios deberán ser difundidos por los canales de comunicación dispuestos al efecto.

9. Terceras partes.

Cuando se presten servicios o se gestione información de otras organizaciones, 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 se utilicen servicios de terceros o se ceda información a terceros, se les hará partícipes de esta política de seguridad y de la normativa de seguridad que ataña a dichos servicios y/o información. Esta tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Cuando algún aspecto de esta política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe de la persona responsable de seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por el Comité de Seguridad de la Información.

10. 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 en la política de seguridad de la información deberán ser aprobados por la Mesa de la Cámara.

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

11. Documentación complementaria.

La política de seguridad de la información se cumplimentará con documentos más precisos que ayudarán a llevar a cabo lo propuesto. Todos los documentos estarán al alcance de los usuarios de los sistemas de información del Parlamento de La Rioja cuando les sean de aplicación.

12. Disposición derogatoria y entrada en vigor.

Queda sin efecto el Documento de Política de Seguridad de la Información aprobado por la Mesa de la Cámara con fecha 6 de septiembre de 2021.

La presente política de seguridad de la información entrará en vigor el día siguiente al de su publicación en el *Boletín Oficial del Parlamento de La Rioja*.

ANEXO

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.

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 detalladas en documento escrito que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

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

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.

BOLETÍN OFICIAL DEL PARLAMENTO DE LA RIOJA

Edita: Servicio de Publicaciones

C/ Marqués de San Nicolás 111, 26001 Logroño

Tfno. (+34) 941 20 40 33 – Ext. 2310

Fax (+34) 941 21 00 40