



Política de Seguridad de la información

Este documento es confidencial. Ni la totalidad ni ninguna parte de este documento pueden ser reveladas a terceros sin el consentimiento previo por JRI LABORATORIO DE SISTEMAS, S. L. Los derechos de autor de este documento recaen en JRI, S. A. Todos los derechos reservados. Ni la totalidad ni ninguna parte de este documento pueden ser reproducidos, almacenados en ningún sistema de recuperación o transmitidos en cualquier forma o por cualquier medio (electrónico, mecánico, reprográfico, de grabación o de otro tipo) sin el consentimiento previo por escrito de los dueños de los derechos de autor.

Las impresiones son consideradas COPIAS NO CONTROLADAS

| | |
|----------------------------------|--|
| Título del documento | Política de Seguridad de la Información |
| Versión | 1.0 |
| Referencia de control | 3.1 ENS |
| Propietario del documento | Comité de Seguridad de la Información |
| Estado | Aprobado |
| Aprobado por | Dirección |
| Fecha de lanzamiento | 01/04/2023 |
| Autor del documento | Responsable de Seguridad de la Información |

Política de Seguridad de la Información

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 1 de abril de 2023, por la dirección.

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

2. INTRODUCCIÓN

Esta política cumple con el Control 3.1 del Esquema Nacional de Seguridad habiendo sido establecida por el Comité de Seguridad de la Información e incluyendo todos los requisitos que la norma exige. Este documento sienta las bases para la gestión de la Seguridad de la Información de JRI LABORATORIO DE SISTEMAS, S. L., en adelante JRI.

Esta política se encuentra disponible como información documentada a todo el personal de JRI.

JRI depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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

Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos de la organización deben cerciorarse de que la seguridad TIC es 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 de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

Política de Seguridad de la Información

La presente política de seguridad se establece de acuerdo con los principios básicos señalados en el capítulo II del RD 311.2022 y se desarrollará aplicando los siguientes requisitos mínimos:

- a) Organización e implantación del proceso de seguridad.
- b) Análisis y gestión de los riesgos.
- c) Gestión de personal.
- d) Profesionalidad.
- e) Autorización y control de los accesos.
- f) Protección de las instalaciones.
- g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- o) Mejora continua del proceso de seguridad.

Estos requisitos mínimos se exigen en proporción a los riesgos identificados en nuestro sistema, de conformidad con lo dispuesto en el artículo 28 del RD 311.2022.

Esta política se encuentra disponible como información documentada a todo el personal de JRI.

3. MISIÓN

JRI depende de los sistemas TIC para alcanzar sus objetivos de prestación de servicios de desarrollo de software y soluciones IT.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los servicios prestados consiguen obtener una mejora en el rendimiento de la infraestructura, mejorar la productividad del personal técnico y reducir significativamente el coste de las inversiones. Es decir, se busca maximizar el tiempo útil

Política de Seguridad de la Información

y la seguridad de los sistemas de información, sin tener que realizar inversiones en equipamiento, software o formación de recursos humanos.

4. OBJETIVOS GENERALES

La Política de Seguridad proporciona las bases para definir y delimitar los objetivos y responsabilidades para las diversas actuaciones técnicas, legales y organizativas que se requieran para garantizar la seguridad de la información y la privacidad, cumpliendo el marco legal de aplicación y las políticas globales y específicas de firma, así como los procedimientos definidos.

Estas actuaciones desde el punto de vista de la seguridad y privacidad son seleccionadas e implantadas basándose en el análisis de riesgos y el equilibrio entre riesgo aceptable y coste de las medidas.

El objetivo de la Política de Seguridad es fijar el marco de actuación necesario para proteger los recursos de información y datos frente a amenazas, internas o externas, deliberadas o accidentales.

La información y datos pueden existir en una variedad de formatos, con soportes tanto electrónicos como el papel u otros medios, e incluye a veces datos críticos acerca de las operaciones, estrategias o actividades de JRI y de sus clientes e incluso, en su caso, datos de carácter sensible que establece la normativa de protección de datos de carácter personal. La pérdida, corrupción, o sustracción de información o de los sistemas que la gestionan tiene un impacto elevado en nuestra Firma.

JRI está convencida de que una gestión eficaz de la Seguridad de la Información y de la Privacidad es un elemento habilitador para que la organización comprenda completamente y actúe de modo adecuado a los riesgos a los que la información es expuesta, así como para poder responder y adaptarse de manera eficiente a los crecientes requerimientos de organismos reguladores, leyes, y por supuesto sus clientes.

5. DECLARACIÓN DE PRINCIPIOS

En JRI asumimos valores que consideramos esenciales para la consecución de nuestros objetivos, como es la preservación de la Información y los datos personales, tanto propios como del resto de partes interesadas y el desarrollo profesional y personal de todos los componentes de su equipo de trabajo.

Debido a nuestra actividad, en JRI somos conscientes de que la información es un activo con un elevado valor para nuestra organización y requiere, por lo tanto, una protección y gestión adecuadas con el fin de dar continuidad a nuestra línea de negocio y minimizar los posibles daños ocasionados por fallos a la integridad, disponibilidad y confidencialidad de la información. Así mismo, tanto la legislación vigente relativa a la protección de datos personales (RGPD y LOPDGDD), como el compromiso de JRI con nuestros clientes nos hace especialmente sensibles al tratamiento de los datos personales a los que tenemos acceso en el ejercicio de nuestra actividad.

Política de Seguridad de la Información

Para ello, JRI establece un conjunto de actividades de gestión que tienen como objetivo preservar los principios de Confidencialidad, Integridad, Disponibilidad, autenticidad, trazabilidad y Conformidad Regulatoria de la información. A su vez, estos principios se definen de la siguiente manera:

- **Confidencialidad:** es la propiedad que permite garantizar que el acceso a la información solamente puede ser ejercido por las personas autorizadas para ello.
- **Integridad:** es la propiedad de salvaguardar la exactitud y completitud de los activos de información.
- **Disponibilidad:** es la cualidad que garantiza que las personas autorizadas pueden acceder a la información y procesarla en cualquier momento en que sea necesario.
- **Autenticidad:** es la propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Trazabilidad:** es la propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
- **Conformidad Regulatoria:** es la propiedad que asegura que la información es gestionada de acuerdo a los principios éticos, profesionales y legales establecidos por las regulaciones que son aplicables en cada contexto.

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

Esto implica que los diferentes departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos de la organización deben cerciorarse de que la seguridad es 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 de TIC.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 8 del ENS.

Dentro del amparo de lo anterior, se encuentra embebida la protección de la privacidad. Nuestros sistemas tratan datos personales sensibles y por ello, la protección de la privacidad se erige como un pilar esencial en el marco de SGSI y se constituye como una necesidad social que las empresas deben respetar y proteger, así como objeto de legislación y/o regulación específica en todo el mundo.

Política de Seguridad de la Información

6. COMPROMISO DE LA DIRECCIÓN

El propósito del Sistema de Gestión de Seguridad de la Información es garantizar que los riesgos de la seguridad de la información y privacidad sean conocidos, asumidos, gestionados o minimizados de una forma documentada, sistemática, estructurada, repetible, asumible y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En lo que respecta de manera específica a la protección de los datos personales, JRI se compromete a cumplir con los principios indicados en la legislación de referencia. Estos son:

- Principio de “licitud, transparencia y lealtad”. Los datos deben ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de “finalidad”. Los datos deben ser tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otro lado, se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de “minimización de datos”. Aplicar medidas técnicas y organizativas para garantizar que sean objeto de tratamiento los datos que únicamente sean precisos para cada uno de los fines específicos del tratamiento reduciendo, la extensión del tratamiento, limitando a lo necesario el plazo de conservación y su accesibilidad.
- Principio de “exactitud”. Disponer de medidas razonables para que los datos se encuentren actualizados, se supriman o modifiquen sin dilación cuando sean inexactos con respecto a los fines para los que se tratan.
- Principio de “limitación del plazo de conservación”. La conservación de los datos debe limitarse en el tiempo al logro de los fines que persigue el tratamiento.
- Principio de “seguridad” Realizar un análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales que traten.
- Principio de “responsabilidad activa” o “responsabilidad demostrada”. Mantener diligencia debida de manera permanente para proteger y garantizar los derechos y libertades de las personas físicas cuyos datos son tratados en base a un análisis de los riesgos que el tratamiento representa para esos derechos y libertades, de modo que podamos garantizar y demostrar que el tratamiento se ajusta a las previsiones del RGPD y la LOPDGD.
- Dirigir, apoyar y supervisar el sistema de gestión de la seguridad de la información, según lo establecido en el RD 311.2022 y posteriores modificaciones y buscar se alcancen los objetivos del mismo.

La dirección de JRI se compromete a apoyar y promover los principios establecidos en esta Política, para lo que pide al personal de la empresa que asuma y se atenga a las previsiones del sistema de gestión documentado para el ENS.

Política de Seguridad de la Información

6.1. MARCO NORMATIVO

Esta Política de Seguridad complementa las políticas de seguridad de JRI en diferentes materias. La documentación relativa a la Seguridad de la Información estará clasificada en tres niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

- Primer nivel: Política de seguridad.
- Segundo nivel: Normativas y procedimientos de seguridad.
- Tercer nivel: Informes, registros y evidencias electrónicas

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones

6.2. Datos de carácter personal

En el ámbito de los datos de carácter personal, aplica:

- 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.

6.3. Esquema nacional de seguridad

En el ámbito del Esquema Nacional de Seguridad, esta política está integrada por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que desarrolla las leyes 39 y 40 de 2015.
- Ley 39/2015 de 1 de octubre del procedimiento administrativo común.
- ley 40/2015 de procedimiento administrativo común de las administraciones públicas.
- Instrucciones Técnicas del CCN (CCN-STIC).

7. TERCERAS PARTES

Cuando JRI utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones

Política de Seguridad de la Información

establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.