



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

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.

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.

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.

Política de Seguridad de la Información

- 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.

1.1. Alcance

Su alcance comprende todos los sistemas TIC y la información que dan soporte a los servicios de soluciones en captura, digitalización de documentación impresa, procesamiento y plataformas de apoyo en todos los centros de datos de JRI.

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

Política de Seguridad de la Información

1.3. 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.

1.4. 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.

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:

Política de Seguridad de la Información

- **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.

1.5. 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,

Política de Seguridad de la Información

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.

2. POLÍTICA

2.1. Prevención

Todos los departamentos deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para

Política de Seguridad de la Información

ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 8 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. Respuesta

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4. Recuperación

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

JRI se compromete a prestar sus servicios de forma gestionada y cumpliendo con los requisitos establecidos en su Sistema Integrado de Gestión de modo que se garantice un servicio ininterrumpido conforme a los requisitos de disponibilidad, seguridad y calidad hacia los clientes.

Política de Seguridad de la Información

3. 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

3.1. 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.

3.2. 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).

Política de Seguridad de la Información

4. ORGANIZACIÓN DE LA SEGURIDAD

4.1. Comités: funciones y responsabilidades

El Comité de Seguridad de la Información estará formado por:

- Responsable de Seguridad:
- Responsable de Sistemas (o Responsable de IT):
- Responsable de la Información:
- Responsable del Servicio de Desarrollo de Producto:

El Comité de Seguridad de la Información tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información.
- Coordinar todas las funciones de seguridad de la organización.
- Velar por el cumplimiento de la normativa legal y sectorial de aplicación.
- Velar por el alineamiento de las actividades de seguridad a los objetivos de la organización.
- Coordinar los Planes de Continuidad de las diferentes áreas, para asegurar una actuación sin fisuras en caso de que deban ser activados.
- Coordinar y aprobar, en su caso, las propuestas de proyectos recibidas de los diferentes ámbitos de seguridad, encargándose gestionar un control y presentación regular del progreso de los proyectos y anuncio de las posibles desviaciones.
- Recibir las inquietudes en materia de seguridad de la Dirección de la entidad y transmitir las a los responsables departamentales pertinentes, recabando de ellos las correspondientes respuestas y soluciones que, una vez coordinadas, habrán de ser comunicadas a la Dirección.

Política de Seguridad de la Información

- Recabar de los responsables de seguridad departamentales informes regulares del estado de la seguridad de la organización y de los posibles incidentes. Estos informes, se consolidan y resumen para su comunicación a la Dirección de la entidad.
- Coordinar y dar respuesta a las inquietudes transmitidas a través de los responsables de seguridad departamentales.
- Definir, dentro de la Política de Seguridad Corporativa, la asignación de roles y los criterios para alcanzar las garantías pertinentes en lo relativo a segregación de funciones
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización.

Política de Seguridad de la Información

4.2. Roles: funciones y responsabilidades

Se detallarán a continuación las funciones de los responsables de la organización:

Responsable de la Información

- Responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- Responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Establecer los requisitos de la información en materia de seguridad.
- Determinar y aprobar los niveles de seguridad de la información.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad.
- Determinar los niveles de seguridad de los servicios.

Responsable de la Seguridad.

Sus funciones serán las siguientes

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El responsable de la Seguridad será el secretario (o presidente) del Comité de Seguridad de la Información con las funciones indicadas en este documento.

Política de Seguridad de la Información

Responsable del Sistema.

Sus funciones serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.
- Potestad para proponer la suspensión del tratamiento de una cierta información o la prestación de un determinado servicio si aprecia deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Responsable de Privacidad

Sus funciones serán las siguientes:

- Coordinar todos los aspectos relacionados con la adecuación de las actuaciones de JRI en materia de protección de datos de carácter personal.
- Coordinar, junto con el responsable de Seguridad, el cumplimiento del ENS con respecto a la protección de datos de carácter personal.

4.3. Procedimientos de designación

El responsable de Seguridad de la Información es nombrado por el Comité de Seguridad de la Información. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Igualmente, el resto de los cargos indicados en el apartado anterior será designado por el Comité de Seguridad de la Información mediante acta de reunión.

4.4. Difusión, actualización y revisión de la política de seguridad de la información

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.

La Política será aprobada por el Órgano de Gobierno y difundida para que la conozcan todas las partes afectadas.

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.

Política de Seguridad de la Información

4.5. Datos de carácter personal

El Documento de Seguridad al que tendrán acceso sólo las personas autorizadas, recoge los registros de actividad de tratamiento de datos afectados y los responsables correspondientes. Todos los sistemas de información de JRI se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

4.6. Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis 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 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.

5. OBLIGACIONES DEL PERSONAL

Todos los miembros de JRI tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de JRI atenderán a una sesión de concienciación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de JRI en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para 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.

Política de Seguridad de la Información

6. 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 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.