Gobierno de Chile

Región de Los Ríos
GOBIERNO REGIONAL

**APRUEBA ACTUALIZACIÓN DE POLITICA DE SEGURIDAD DE LA INFORMACIÓN Y DEJA SIN EFECTO RES. EXENTA N° 2420 DEL 2011, N°2203 DEL 2012, N° 2185 DEL 2013, Y N° 1550 DEL 2017.**

**RESOLUCIÓN EXENTA Nº 1676/**

**VALDIVIA, 26 DE OCTUBRE DE 2018.**

**VISTOS:**

Lo dispuesto en la Ley N° 18.575, de Bases Generales de la Administración del Estado, cuyo texto refundido, coordinado y sistematizado se fijó por D.F.L. N° 1 (19.653) de 2000, del Ministerio Secretaría General de la Presidencia; la Ley Orgánica Constitucional N°19.175, sobre Gobierno y Administración Regional; la Ley N° 19.880 de 2003, de Bases de Procedimiento Administrativos que rigen los actos de los órganos de la Administración del Estado; la Ley 20.285, Sobre Transparencia y Acceso a la Información Pública; la Ley 19.553 de 1998 modificada por la Ley 19.618 y 19.882; la Resolución N° 1.600 de 2008, de la Contraloría General de la República y en el Decreto N° 426 del 24 de marzo de 2017 de Ministerio de Interior, que nombra al Intendente Titular del Gobierno Regional de Los Ríos.

**TENIENDO PRESENTE:**

1. Que mediante Resolución N° 2420 de 2011, se aprobó el documento "Política de Seguridad de la Información", indicando que fue elaborada en base a la NCh ISO27002, la que fue complementada por la Resolución Exenta 2.203 de fecha 24 de julio de 2012, que aprobó nuevamente el texto íntegro de la Política.

2. Que el año 2013 la Política fue complementada estableciendo plazos para su revisión, tanto del documento como de su cumplimiento, además de establecer su necesaria modificación siempre que las circunstancias lo ameriten, complementación que fue aprobada mediante Resolución Exenta N° 2185 de 12 de agosto de 2013, la que incluyó el texto íntegro de la política, dejando sin efecto la Resolución Exenta N° 2203 de 2012.

3. Que la Resolución Exenta N° 1550 de 13 de noviembre de 2017, aprobó la actualización de la Política, en conformidad a las recomendaciones de la Red de Expertos y del Comité de Seguridad de la Información del Gobierno Regional, aprobando nuevamente el texto íntegro y dejando sin efecto la resolución 2185 de 2013, para evitar dispersión de resoluciones.

4. Qué de acuerdo a lo establecido en la Política, el plazo para su revisión y actualización es de cada dos años, mismo plazo para la evaluación de su cumplimiento.

5. Qué en reunión de comité de seguridad realizada el 12 de julio de 2018, de acuerdo a ACTA N° 13 SESIÓN COMITÉ DE SEGURIDAD, se acordó incorporar a la figura del Administrador Regional como nuevo integrante, el que debe formar parte de quienes revisan, proponen mejoras y/o validan el documento de Política de Seguridad de la Información, única cuestión que se observó necesario modificar respecto al documento de la Política de Seguridad de la Información dl Gobierno Regional.

6. Que en virtud de lo anterior, mediante Resolución Exenta N°1675 de 26 de octubre de 2018, se designó como integrante del Comité al Administrador Regional, el que aprobará la Política señalada, la que a su vez contempla sus funciones.

7. Que para evitar la dispersión de actos administrativos es necesario dejar sin efecto la Resolución Exenta mencionada en el primer numeral.

**R E S U E L V O:**

**1° APRUÉBASE** a contar de esta fecha, la Política de Seguridad de la Información que regirá para todas las personas que conformes y presten funciones en este Gobierno Regional de Los Ríos, cuyo texto íntegro es el siguiente:

GOBIERNO REGIONAL DPTO. JURIDICO REGION DE LOS RIOS

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Sistemas de Gestión de Seguridad de la Información
(SGSI- ISO/IEC 27001-27002)

**Versión**

| Versión | Fecha | Responsable | Validado por |
|---|---|---|---|
| 4.0 | 26-10-2018 | Patricio Acum Salinas | Intendente Cesar Asenjo Jerez |

| | | |
|---|---|---|
| Alejandro Paredes Zieballe | Administrador Regional | |
| Carlos Ovando Hernández | Encargado de Seguridad de la Información, Miembro Comité de Seguridad de la Información | |
| Heidi Machmar Hernández | Miembro Comité de Seguridad de la Información | |
| Wilson Monzón Riquelme | Miembro Comité de Seguridad de la Información | |
| Paola Hermosilla B. | Miembro Comité de Seguridad de la Información | |
| Cesar Pérez S. | Miembro Comité de Seguridad de la Información | |
| Rodrigo Aravena B. | Miembro Comité de Seguridad de la Información | |
| Patricio Acum Salinas | Encargado PMG-SSI, encargado Unidad de Informática. | |

GOBIERNO REGIONAL DIVISIÓN ADMINISTRACIÓN Y FINANZAS REGIÓN DE LOS RÍOS
GOBIERNO REGIONAL DIVISION DE PLANIFICACION REGION DE LOS RIOS
GOBIERNO REGIONAL DIVISIÓN DE PRESUPUESTO E INVERSIÓN REGIÓN DE LOS RÍOS
GOBIERNO REGIONAL DEPARTAMENTO FINANZAS REGION DE LOS RIOS
GOBIERNO REGIONAL DPTO. JURIDICO REGION DE LOS RIOS
GOBIERNO REGIONAL UNIDAD DE GESTIÓN ESTRATÉGICA INSTITUCIONAL REGION DE LOS RIOS
GOBIERNO REGIONAL UNIDAD INFORMATICA REGION DE LOS RIOS

GOBIERNO REGIONAL INTENDENTE REGION DE LOS RIOS

**CESAR ASENJO JEREZ**
**INTENDENTE**
**GOBIERNO REGIONAL DE LOS RÍOS**

## Contenido

# DECLARACIÓN INSTITUCIONAL

## OBJETIVO GENERAL.

El Gobierno Regional de Los Ríos, expresa por medio de este documento su total convicción y compromiso de resguardar los activos de información con los que cuenta el Gobierno Regional que dirige, conociendo la importancia de dichos activos en el cumplimiento de la relevante misión que desempeña. Es por ello que se actualiza la **Política de Seguridad de la Información** basada en Sistemas de Gestión de Seguridad de la Información, la que debe garantizar el correcto funcionamiento del servicio, el cumplimiento de metas y la prevención de riesgos y/o amenazas referidas a los Activos de Información.

Por consiguiente, gestionar la seguridad de la información es un imperativo que se debe cumplir en el marco de la normativa gubernamental existente, por medio de todas aquellas actividades y tareas que sean necesarias para establecer los niveles de seguridad que la propia institución determine, basándose para ello en metodologías y técnicas estándares en estas materias, con el firme propósito de lograr introducir un ciclo de mejoramiento continuo y sostenible en el tiempo, que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad, de todos sus activos de información relevantes para la institución, como un principio clave en la gestión de sus procesos.

EI Gobierno Regional de Los Ríos, se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de implantación del tipo "Sistema de Gestión de Seguridad de la Información (SGSI), basado en la Norma Chilena Oficial NCh-IS027001, con el objetivo de preservar los activos de información institucional.

Entendiendo como **Activos de Información**, todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de la información de valor para la Institución, de esta forma se distinguen tres niveles básicos de activos de información:

- ✓ **La Información**: Con la cual se trabaja en sus múltiples formatos, es decir: papel, digital, texto, imagen, audio, video, etc.
- ✓ **Equipos/Sistemas/Infraestructura**: Estos activos son los que soportan la información.
- ✓ **Las Personas**: Representan un componente fundamental de los activos de información ya que utilizan la misma en sus labores diarias, pudiendo: crear, modificar y/o eliminar de acuerdo a las necesidades de la Institución, además de lo anterior, son quienes tienen conocimiento de los procesos institucionales.

De lo anterior, se desprende la necesidad e importancia de brindar una adecuada protección a los activos de información de la Institución, asegurando a los mismos frente a la amplia gama de amenazas existentes, minimizar los daños que puedan sufrir y maximizar el rol y la finalidad de la administración del estado. Por lo tanto, se deben proteger en cualquiera de las formas o medios en que se creen, almacene o trate, publique, transmita o posiblemente se destruyan.

## MARCO REFERENCIAL

El presente documento se rige por normas jurídicas, de seguridad y procedimientos establecidos por la autoridad que a continuación se detallan; Decreto Supremo N°83 del Ministerio Secretaría General de la Presidencia, el cual "Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los

Documentos Electrónicos"; Sistema de Gestión de Seguridad de la Información (NCh 27001, NCh 27002), perteneciente al Programa de Mejoramiento de la Gestión del Ministerio de Hacienda a través de la Dirección de Presupuestos (DIPRES) y que se rige por la Ley N° 19.553 y sus modificaciones, la cual "Concede Asignación de Modernización y otros Beneficios que se indica" y el documento Política de Seguridad de la Información aprobada por el señor Intendente Regional don Juan Andrés Varas Braun.

El conocimiento, aceptación y uso del presente documento es de responsabilidad de todos los funcionarios y personas que presten algún servicio al Gobierno Regional de Los Ríos cualquiera sea su calidad jurídica, la relación contractual con la institución y el nivel de responsabilidad de cada uno en las distintas divisiones, departamentos y unidades en los que se desempeñen. Igualmente, quienes mantengan contratos y/o presten servicios en forma externa y que tengan acceso a información de la institución que se encuentre en proceso y que además, no se considere como parte de la información públicamente disponible de acuerdo a Ley de Transparencia N°20.285.

## ALCANCE

Esta política se aplica a todos los funcionarios, independiente de su tipo de contrato, que tengan derechos de acceso a la información que puedan afectar los activos de información del Gobierno regional de Los Ríos y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

## NORMATIVA APLICABLE

El marco legal para el Sistema de Gestión de Seguridad de la Información se señala en el documento "Normativa del Sistema de Gestión de Seguridad de la Información"

La **seguridad de la información** se entiende como su preservación y protección en los siguientes aspectos:

- ✓ **Confidencialidad:** Proteger la información para que sólo los usuarios autorizados accedan a ella. (identificación/autenticación – roles – protección de la impresión – controles fotocopiadores, etc.)
- ✓ **Integridad:** Aseguramiento que la información sea exacta, sin que sufra modificaciones, alteraciones o pérdidas en todo el proceso de su construcción, notificación y almacenamiento. (base de datos corruptas – documentos extraviados (office, Word, etc.) – datos no actualizados).
- ✓ **Disponibilidad:** Cerciorar que la información esté disponible para los usuarios autorizados en el momento en que sea necesario acceder a ella y a sus respaldos, evitando incidentes por denegación del servicio.

Adicionalmente se deben considerar los conceptos de:

- ✓ **Autenticidad:** Asegurar la validez de la información en tiempo, forma y distribución, validar emisor para evitar suplantación de identidades.
- ✓ **Auditabilidad:** todos los eventos de un sistema deben poder ser registrados para su control posterior.
- ✓ **Protección de la duplicación:** asegurar que los documentos o información que sean generado por el Gobierno Regional, sólo se realice una vez, a menos que se especifique lo contrario.
- ✓ **No repudio:** evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- ✓ **Legalidad:** referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el organismo.

- ✓ **Confiabilidad de la información:** que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

La máxima autoridad regional, ha expresado su voluntad de apoyar los objetivos y principios de la Seguridad de la Información, conociendo la importancia de ésta en pos de lograr la eficiencia y eficacia en los procesos relacionados con el cumplimiento de la labor del Gobierno Regional, el cual en su calidad de organismo autónomo con personalidad jurídica de derecho público, debe velar por la correcta administración de la región; impulsar un desarrollo armónico y equitativo en el ámbito económico, social y cultural; concretar acuerdos de trabajo y alianzas estratégicas entre los distintos sectores tanto públicos como privados.
Conociendo que el Sistema de Gestión de Seguridad de la Información está directamente vinculado con todas las materias nombradas y con el fin de asegurar dichos logros, el Intendente Regional ha nombrado al Comité de Seguridad de la Información, el que contará con un encargado de Seguridad, dicho funcionario cuenta con las aptitudes y méritos conforme este nombramiento amerita y además se relacionará de forma directa con la máxima autoridad regional en caso de la ocurrencia de amenazas, o para mantener informado de los avances en esta materia.

La presente Política crea el marco para fijar objetivos de control y controles, con los que se deberá prever posibles amenazas a los activos de información.
Los potenciales riesgos en la Seguridad de la Información significan un impacto negativo en el ejercicio de las funciones de la Administración, considerando la probabilidad y la importancia de ocurrencia. Por lo que en la gestión de riesgos se deberá identificar, evaluar y tomar decisiones para reducirlo a un nivel aceptable, con miras siempre a la perfección.
Los posibles riesgos a la seguridad de la información se encuentran en todo el proceso de ejecución de funciones y labores del Gobierno Regional, y por lo tanto en todos sus funcionarios, es decir, a todas las Divisiones, Departamentos, Unidades y Oficinas del Gobierno Regional, llegando también a los agentes externos vinculados, beneficiarios y la Región en su totalidad.

# DIFUSIÓN DE LA POLITICA

La responsabilidad de salvaguardar los activos de información es tarea de todos los agentes involucrados, tanto internos como externos, por lo cual la Política de Seguridad de la Información y cualquier otro documento de carácter oficial emitido por la institución y que guarde relación con la materia, serán dados a conocer a todos los funcionarios del Gobierno Regional y también a eventuales terceros externos involucrados, mediante correo electrónico y publicado en la intranet del Gobierno Regional, los que estarán obligados a conocer acatar y dar cumplimiento a todo lo dispuesto en este u otros futuros documentos que digan relación a la materia.

Se deberá dar cumplimiento a los principios, normas y requisitos importantes en materia de seguridad de la información que atañen a las funciones del Gobierno Regional, de acuerdo a ello será responsabilidad de los funcionarios y usuarios externos lo siguiente:

- ✓ Conocer y dar cumplimiento a las leyes vigentes, a los instructivos emanados y a las responsabilidades individuales y colectivas en materia de seguridad de la información, así como la obligación de prevenir, proteger y/o informar acerca de cualquier posible amenaza de los activos de información cualquiera sea su origen, causa o consecuencia.
- ✓ Asegurar la continuidad de los procesos del Gobierno Regional, mediante un plan de contingencia que de una rápida respuesta a posibles eventos en que se vea retardado el normal funcionamiento del mismo, este plan deberá ser probado y revisado de forma periódica, además de la constante búsqueda de nuevas metodologías tendientes a estar preparados ante nuevas amenazas.

- ✓ Las prácticas conducentes a la violación de la Política de Seguridad de la Información serán sancionadas de acuerdo a la normativa vigente y de acuerdo al impacto que ello signifique para el buen funcionamiento de las labores del Gobierno Regional.

# ROLES Y RESPONSABILIDADES

La Política de Seguridad deberá, mediante el Sistema de Gestión de Seguridad de la Información, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.
De acuerdo a ello el Intendente Regional ha designado responsabilidades generales y específicas en esta materia, es decir, son responsables, El administrador Regional, jefes de división, departamento, unidades, y cada funcionario sea cual fuere su situación contractual de conocer e implementar la Política de Seguridad, ya sea a modo colectivo o individual.

**El comité de Seguridad de la Información tendrá la labor de:**

- ✓ Definir una metodología de gestión y tratamiento del riesgo.
- ✓ Monitorear cambios significativos de los riesgos que afecten a los activos de información frente a las amenazas más importantes.
- ✓ Identificar los Activos de Información desde un punto de vista de la importancia de cada uno.
- ✓ Identificar a quienes son los responsables del manejo de los Activos de Información.
- ✓ Establecer vulnerabilidades o riesgos de los activos según el impacto que pudieran producir para la institución en caso de concretarse amenazas a la seguridad de los mismos.
- ✓ Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad de la información.
- ✓ Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área y a cada funcionario del Gobierno Regional.
- ✓ Acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información.
- ✓ Garantizar que la seguridad sea parte del proceso de planificación de la información.
- ✓ Evaluar y coordinar la implementación de controles específicos de seguridad para nuevos sistemas o servicios.
- ✓ Promover la difusión y apoyo a la seguridad de la información dentro del Gobierno Regional.

**El Administrador Regional y Jefes de Divisiones deberán:**

- ✓ Conocer al detalle el presente documento.
- ✓ Participar activamente de las reuniones del Comité de Seguridad de la Información.
- ✓ Fomentar el cumplimiento de los procedimientos establecidos por el Comité de Seguridad de la Información por parte de los funcionarios bajo su dependencia.
- ✓ Generar instancias de revisión de temas de seguridad de la información con sus respectivas divisiones.

**El Encargado de Seguridad de la Información deberá:**

- ✓ Coordinar las acciones del comité de seguridad de la información.
- ✓ Fijar calendario de reuniones semestrales para evaluar el cumplimiento de la Política de Seguridad, sin que ello impida realizar reuniones extraordinarias en caso necesario.

- ✓ Impulsar la implementación y cumplimiento de la presente política.
- ✓ Estar en contacto directo e informar cuando sea necesario de situaciones de riesgo que afecten a la seguridad de los activos de información a la máxima autoridad regional.
- ✓ Gestionar los recursos necesarios para cumplir con la normativa respecto de seguridad de la información, por ejemplo, la adquisición de Normas ISO, adquisición de sistemas que cumplan con estas normas, servicios de capacitación relacionados con seguridad de la información, entre otros.

**El responsable de Seguridad Informática tendrá la misión de:**

- ✓ Cumplir funciones relativas a la seguridad de los sistemas de información del Gobierno Regional, además de supervisar todos los aspectos inherentes a los temas tratados en la Política de Seguridad.
- ✓ Administración y comunicación de los sistemas y recursos de tecnologías de información del Gobierno Regional.
- ✓ Mantenimiento de sistemas siguiendo una metodología de ciclo de vida de sistemas apropiada.
- ✓ Velar porque en la adquisición de sistemas se contemple la inclusión de normas y medidas de seguridad establecidas en la normativa vigente.

**Los funcionarios que mantengan información en su poder necesaria para sus labores diarias, serán responsables de:**

- ✓ Clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada.
- ✓ Definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencias.
- ✓ Serán responsables de mantener la información fuera del alcance de terceros no relacionados con la misma, no dejar información crítica visible o en lugares no seguros.
- ✓ Mantener siempre sus equipos computacionales, en los que mantenga y trabaje con información reservada, con acceso restringido mediante contraseña única, además mantener cerrados los lugares donde se guarde información impresa.

**El Jefe de Recursos Humanos deberá:**

- ✓ Notificar a todo el personal que ingrese de la existencia y de la obligación de dar cumplimiento a la Política de Seguridad de la Información, así como de todas las normas, procedimientos y prácticas que de ella surjan.
- ✓ Tendrá a su cargo la notificación de la presente Política de Seguridad a todo el personal, de los cambios que en ella se produzcan, así como los documentos que se anexen.
- ✓ Coordinar las tareas de capacitación continua en materia de seguridad.

**El Departamento Jurídico será responsable de:**

- ✓ Verificar el cumplimiento de la presente Política de Seguridad de la Información en la información que diga relación con las labores del departamento o que emane de la misma.
- ✓ Asesorar en materia legal al Gobierno Regional en lo referido a la Seguridad de la Información.

**Los Usuarios de la información y de los sistemas son responsables de:**

- ✓ Conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente, así como de informar al Encargado de Seguridad acerca del mal uso o no cumplimiento de esta por parte de terceros.

**La Unidad de Auditoría deberá:**

- ✓ Practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la Tecnología de la Información.
- ✓ Informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas en la Política de Seguridad de la Información, así como de todo documento emanado de ella y de los procedimientos y prácticas que de ella surjan.

El Comité de Seguridad de la Información realizará una revisión de la presente Política de Seguridad cada dos años con el propósito de mantenerla actualizada, sin perjuicio de efectuar cambios en ella toda vez que sea necesario en función de posibles modificaciones que puedan afectar su definición, por ejemplo, cambios tecnológicos, variación de costos de controles, impactos de los incidentes de seguridad, etc.

El Intendente del Gobierno Regional asumirá su total compromiso en la labor de resguardar los activos de información del Gobierno Regional y velar porque se cumplan las normas establecidas en la Política de Seguridad de la Información por parte de todos los actores, tanto internos como externos vinculados a la institución.

# REVISIÓN DE LA POLITICA

El Comité de Seguridad de la Información del Gobierno Regional constituido mediante Resolución Exenta N°1804 de 08 de julio de 2013, ha establecido lo siguiente:

- ➢ La fecha de revisión del documento Política de Seguridad de la Información será una vez cada dos años considerando como primera revisión la efectuada el día 02 de agosto de 2013, ocasión en la que se decide mantener vigente el documento hasta la nueva revisión y que consta en Acta N° 7 de Reunión de Comité de Seguridad, sin perjuicio de realizar actualizaciones antes de transcurrido un año siempre que las circunstancias lo ameriten.

- ➢ La fecha de revisión del cumplimiento del documento Política de Seguridad de la Información será cada año a partir del año 2014, ocasión en la que se decidirá la forma más apropiada de realizar dicha revisión, acuerdo que consta en Acta N° 7 de Reunión de Comité de Seguridad de la Información.

# GLOSARIO DE TÉRMINOS

Definiciones. Para los propósitos de esta Política, se entenderá por:

- **Acceso a la información**: El acceso a la información es el derecho que tiene toda persona de buscar, recibir y difundir información en poder del Estado.

- **Derechos de accesos**: Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.

- **Restringir el acceso:** Delimitar el acceso de los funcionarios y terceras partes a determinados recursos.

- **Sanción:** Puede ser definida como consecuencia administrativa, civil, jurídica o penal por el incumplimiento del deber que produce en relación con el obligado.

- **Sistema informático:** uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

- **Usuario:** persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por la Unidad de Informática del Gobierno Regional de Los Ríos, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de ésta o del estatuto que lo rija.

- **Documento electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

- **Documento público:** aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.

- **Documento reservado**: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano que sean remitidos.

- **Documento electrónico institucional:** Documento electrónico creado, enviado, comunicado o recibido, por los usuarios del Gobierno Regional de Los Ríos, en ejercicio de las funciones propias de la institución.

- **Unidad de Informática**: Unidad de Informática del Gobierno Regional de Los Ríos.

- **Área de Soporte:** Área de Soporte de la Unidad de Informática del Gobierno Regional de Los Ríos.

- **Activos de información:** Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional.

- **Riesgo:** Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.

- **Amenaza:** Causa potencial de un incidente no-deseado por el cual puede resultar dañado un sistema u organización. A modo de ejemplo, terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

- **Seguridad de la Información:** es el proceso encargado de asegurar que los recursos de un sistema de información sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

- **Proceso:** Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

- **Incidente de Seguridad:** Se define incidente como cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y confidencialidad de la información, junto con la plataforma tecnológica, proceso y aplicativos que permitan acceder a ésta en forma oportuna. En general, es una violación de una política, estándar o procedimiento de seguridad, que no permite prestar un servicio computacional. Como ejemplos de incidentes de seguridad podemos enumerar:
    - Acceso no autorizado.
    - Robo de contraseñas.
    - Robo de información.
    - Denegación de servicio.

- Robo y extravío de un medio de procesamiento de la información.

- **Confidencialidad:** Es la propiedad de un documento o mensaje, que está autorizado para ser leído o entendido, únicamente, por algunas personas o entidades.

- **Integridad:** Se entiende por la corrección y completitud de los datos o de la información manejada.

- **Disponibilidad:** es la certeza de que sólo los usuarios autorizados tienen acceso a la información y a los activos asociados cuando es requerido.

- **Medios de procesamiento de información:** Los dispositivos internos y/o externos que tenga la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario.

  Como ejemplos de medios de procesamiento de información, podemos enumerar:
  - Servidores de aplicaciones: de correo, de impresión, aplicaciones web.
  - Servidores de Almacenamientos.
  - Computadores personales.
  - Discos duros externos.
  - Pendrives.
  - Teléfonos móviles.

- **Operaciones informáticas:** Todas las actividades que estén relacionadas con un sistema informático y/o procesamiento de la información.

  - Como ejemplos de operaciones informáticas podemos enumerar:
  - Configuración de servidores y estaciones de trabajo.
  - Configuración de equipos de comunicación que conectan a los usuarios a la red.
  - Creación y/o retiro de acceso a los medios de procesamiento de información.
  - Mantención de base de datos de los sistemas.
  - Respaldo de la información de servidores y estaciones de trabajo.

- **Terceras partes:** Persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión. Para este procedimiento, se entenderá como terceras partes a:
  - Proveedores de servicios y de red.
  - Proveedores de productos de software y servicios de información.
  - Outsourcing de instalaciones y operaciones.
  - Servicios de asesoría de seguridad.
  - Auditores externos.

- **Estación de Trabajo:** En una red de computadores, una estación de trabajo es un computador que facilita a los usuarios el acceso a los servidores y periféricos de la red.

- **Programa malicioso:** Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

- **Virus:** Se usa para designar un programa que, al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora.

- **Malware:** El término malware es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto.
  El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.

- **SPAM:** Se llama spam al correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor). La acción de enviar dichos mensajes se denomina spamming.

**2°** **DÉJASE SIN EFECTO** a contar de esta fecha, la Resolución Exenta N° 1550 de 13 de noviembre de 2017.

**3°** **DIFÚNDASE,** a todos los funcionarios del Gobierno Regional de Los Ríos la política de Seguridad de la Información complementada y aprobada en el resuelvo anterior, mediante los medios electrónicos intranet y correo electrónico.

**ANÓTESE, COMUNÍQUESE, PUBLÍQUESE EN LA PÁGINA DE INTRANET DEL GOBIERNO REGIONAL Y ARCHÍVESE.**

GOBIERNO REGIONAL INTENDENTE REGION DE LOS RIOS

**CESAR ASENJO JEREZ**
**INTENDENTE**
**GOBIERNO REGIONAL DE LOS RÍOS**

GOBIERNO REGIONAL DPTO. JURIDICO REGION DE LOS RIOS

**COH/CMZ/PAS/SRG**
**DISTRIBUCION:**
- Funcionarios Gobierno Regional de Los Ríos.
- División de Administración y Finanzas.
- Departamento Jurídico.
- Arch. Encargado de Seguridad de la Información.
- Archivo Oficina de Partes Gob. Regional.