POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

INFORMACIÓN DEL DOCUMENTO

HISTORIA DEL DOCUMENTO			
Nombre del documento	Políticas General de seguridad de la Información		
Preparado por	Comité interno de seguridad REUNA		
Documento base			
Creación del documento	AS/JH	Fecha de creación	Junio 2023
Aprobación	PA/CI/AA/AL	Fecha de aprobación	Agosto 2024

CONTROL DE VERSIONES			
Versión	Fecha de Modificación	Preparada por	Descripción
1.0	10-08-2023	AS/JH	Adaptación a REUNA
1.1	01-08-2024	PA/CI/AA/AL	Revisión y aprobación

Contenido

1. PROPÓSITO

Esta Política General de Gestión de Seguridad de la Información, tiene como propósito establecer los lineamientos para la gestión de la Seguridad de la Información en REUNA.

2. ALCANCE O ÁMBITO DE APLICACIÓN

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencia), personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios a REUNA.

La presente política se aplica sobre todo tipo de información, considerando todo medio de soporte y presentación, documentos, audio o video, que constan en medios digitales, magnéticos, ópticos, electrónicos o fotográficos.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Alcance de Dominios y Controles de Seguridad de la Información (Nch-ISO 27001:2013)		
Nombre del Dominio	ID Control ISO 27001	Nombre del Control
Políticas de seguridad de la información	A.05.01.01	Políticas para la seguridad de la información
	A.05.01.02	Revisión de las políticas de seguridad de la información
Organización de la seguridad de la información	A.06.01.01	Roles y responsabilidades de la seguridad de la información
Cumplimiento	A.18.02.01	Revisión independiente de la seguridad de la información

3. MARCO NORMATIVO Y DOCUMENTOS RELACIONADOS

- Documentos del Sistema de Gestión de Seguridad de la Información (SGSI) de REUNA, disponibles en Plataforma Docs de REUNA.
- Política Nacional de Ciberseguridad (PNCS)
- El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior.

- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad.
- Leyes relacionadas.

- Políticas de Seguridad de la Información de REUNA, disponibles en Plataforma Docs o en formato físico

4. ROLES Y RESPONSABILIDADES

1. Comité Interno de Seguridad de la Información (CISI)

Comité conformado por un miembro de cada área de REUNA, los cuales son designados por los respectivos gerentes. Las responsabilidades de este comité son:

- Supervisar la implementación de la estructura documental del Sistema de Gestión de Seguridad de la Información
- Proponer a las gerencias, estrategias o soluciones específicas para implementar o controlar los componentes de la estructura documental del Sistema de Seguridad de la Información.
- Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones sobre ello.
- Revisar y monitorear los incidentes de seguridad de la información a fin de establecer acciones preventivas y correctivas.
- Coordinarse con los representantes de cada área de la Institución, para mantener estrategias comunes de gestión.
- Apoyar a las distintas áreas, según corresponda, en la implementación de los controles en conjunto con las gerencias, a través del Programa de Mejoramiento de la Gestión de cada año, de acuerdo al indicador transversal definido para la Seguridad de la Información. (Indicador en base a brechas, medidas de mitigación y cambios)
- Revisar los elementos del Sistema de Seguridad de la Información y proponer mejoras a través del Encargado de Seguridad de la Información, definiendo fechas específicas, ej: dos veces al año.
- Difundir los componentes de la estructura documental del Sistema de Seguridad de la Información a través de la plataforma Docs y los medios de comunicación establecidos dentro de REUNA.
- Monitorear cambios significativos que pudieran variar los riesgos presentes en la Institución.
- Establecer acciones y proponer iniciativas para mejorar la seguridad de la información en REUNA.
- Supervisar la realización de auditorías de Seguridad de la Información, internas o externas.

2. Encargado de Ciberseguridad de REUNA (Ing. de Ciberseguridad).

- Actuar como Asesor en materias relativas a seguridad de la información.

- Gestionar internamente el tratamiento de incidentes que estén vinculados a los activos de información en la Institución, identificados y/o reportados tanto por el Ministerio del Interior como por instancias internas, efectuando la reportabilidad y el seguimiento adecuado a dichos eventos.
- Investigar los eventos de seguridad identificados y/o reportados.
- Gestionar la respuesta y priorización del tratamiento de incidentes identificados y/o reportados, que estén vinculados a los activos de información en la Institución.
- Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.
- Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de seguridad.
- Establecer puntos de enlace con especialistas externos que permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- Entregar la información necesaria para que se comunique adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de la Corporación, acerca de las Políticas de Seguridad de la Información vigentes en REUNA, y en particular sobre las obligaciones que les correspondan en relación a la gestión de incidentes de seguridad.

3. Encargado Seguridad de la Información (CISO).

- Encabezar el CISI, el cual tendrá a su cargo la actualización de políticas de Ciberseguridad y Seguridad de la Información al interior de la organización.
- Organizar las actividades del Comité Interno de Seguridad.
- Alinear los esfuerzos de las distintas áreas de la institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad.
- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la organización y el control de su implementación, velando por su correcta aplicación y cumplimiento, así como mantener coordinación con otras áreas para apoyar los objetivos de seguridad de la información.
- Apoyar el proceso de Sensibilización en Materias de Ciberseguridad al Interior de la Institución.
- Definir las vías de comunicación que se requieran para apoyar en la resolución del incidente de seguridad al interior de la Institución. Sean estas a través del escalamiento al Comité Interno de Seguridad, Gerencias u otra según se requiera.
- Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad.
- Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de REUNA, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes en la Corporación, y en particular

sobre las obligaciones que les correspondan en relación a la gestión de incidentes.

4. Usuarios finales.

- Se debe entender como usuarios finales a todos quienes tienen la responsabilidad de acatar las políticas y normativas definidas, independiente que además tengan otros roles en este ámbito.
- Debe considerar:
  - A todos los funcionarios.
  - Personal contratado a plazo fijo
  - Terceros (proveedores, compra de servicios, tratamiento por encargo, servicios externalizados, etc.),

5. MATERIAS QUE ABORDA LA POLÍTICA

- Políticas para la seguridad de la información.
- Revisión de las políticas de seguridad de la información.
- Roles y responsabilidades de la seguridad de la información.
- Revisión independiente de la seguridad de la información.

6. DIRECTRICES DE LA POLITICA

6.1 Declaración Institucional

REUNA se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, 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. Para estos efectos, REUNA se basará 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.

Para la gestión de la Seguridad de la Información al interior de REUNA se ha decidido contar con un programa de implantación del tipo “Sistema de Gestión de Seguridad de la Información” (SGSI), basado en los requisitos de la Norma NCh-ISO27001:2013, y las prácticas para los controles de seguridad de la Norma NCh-ISO27002:2013, con el objetivo de preservar los activos de información institucional con respecto a:

- **Su Integridad:** la información no puede ser alterada ni eliminada por cambios no autorizados o accidentales. Este principio fundamental de

seguridad busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas del negocio, así como evitar fraudes o irregularidades de cualquier índole que haga que la información sea alterada.

- **Su Confidencialidad:** La información confidencial, privada y sensible sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones. Este principio fundamental de seguridad busca garantizar que toda la información de los ciudadanos, funcionarios y proveedores, y sus medios de procesamiento o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

- **Su Disponibilidad:** La información debe estar disponible para el personal, usuarios y entidades reguladoras de manera oportuna y acorde a sus niveles de autorización. Este principio fundamental de seguridad busca garantizar que los usuarios autorizados tengan acceso a la información cuando ésta es requerida por el proceso institucional. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o dañe las instalaciones, medios de almacenamiento o equipamiento de procesamiento.
  Según lo expuesto anteriormente, las autoridades de REUNA se comprometen a:

  - Apoyar los objetivos y principios de la seguridad de la información, y a proveer los recursos necesarios para la gestión de actividades en seguridad.

  - Promover un plan de acción de mejora continua con el fin de asegurar una adecuada gestión de la seguridad de la información, según lo dispuesto en la NCh-ISO 27001:2013 y otras normativas vigentes que, conforme a lo dispuesto en el número 7 de esta política general, estarán disponibles permanentemente en la plataforma Docs de REUNA.

6.2 Objetivos de la Gestión de Seguridad de la Información en REUNA

6.2.1...Objetivo General

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

6.2.2...Objetivos Específicos

- Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso institucional, abarcando tanto los procesos críticos institucionales, como los de soporte.
- Realizar actividades necesarias de análisis de riesgo, según normativas, técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riesgos que sean identificados, sin perder de vista el enfoque de la gestión por procesos institucionales.
- Proteger la información, sus medios de procesamiento, conservación y transmisión del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.
- Mantener y hacer uso de la estructura y el marco de estándares, políticas y procedimientos en materia de seguridad de la información.
- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.
- Hacer uso de planes de continuidad operacional ante hechos contingentes que interrumpan la operación del servicio.
- Sensibilizar y capacitar a los funcionarios de REUNA acerca de su responsabilidad para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio de REUNA.

6.3 Gestión de la Política y otros documentos del sistema de Gestión de Seguridad de la información

La estructura documental de ese sistema está compuesta por una Política General de Seguridad de la Información, políticas específicas de seguridad de la información, procedimientos de operación, instructivos y registros.
La referida estructura documental deberá ser aprobada por las respectivas gerencias y será revisada (a lo menos cada dos años) por el Encargado de Seguridad y el Comité Interno de Seguridad.

Las versiones vigentes de la normativa del SGSI y los documentos de apoyo, serán publicados en el sitio intranet de REUNA http://intranet.reuna.cl, además de otros sitios o lugares de fácil acceso a los funcionarios.

6.4 Identificación de riesgos

- A lo menos cada dos años el Comité Interno de Seguridad, debe gestionar la actualización de los riesgos de seguridad de la información, que debe ser construido a partir del análisis de las amenazas y vulnerabilidades a los que se encuentran expuestos los activos de la información relevantes. –Norma NCh-ISO 31000:2012 – Principios y directrices para la Gestión de Riesgos.
- Marco COSO ERM – www.coso.org.
- CSIRT de Gobierno de Chile

En el caso de los riesgos residuales, deben ser relevados por el Comité de Seguridad de la Información a las gerencias de REUNA en primera instancia para las acciones a seguir.

6.5 Revisión y medición

A lo menos una vez al año, el Comité Interno de Seguridad debe evaluar el estado del Sistema de Gestión de Seguridad de la Información e informar a Gerencias los resultados, considerando cambios que surjan en el transcurso de este período que podrían afectar el enfoque de la organización a la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, circunstancias del negocio, disponibilidad de recursos, condiciones contractuales, reguladoras, y legales, o cambios al ambiente técnico. Para ello debe considerar los siguientes aspectos:

- Retroalimentación de las partes interesadas.
- Resultados de las revisiones efectuadas por terceras partes.
- Estado de acciones preventivas y correctivas.
- Cambios en los procesos institucionales, nueva legislación, tecnología etc.
- Alertas ante amenazas y vulnerabilidades.
- Información relacionada a incidentes de seguridad.
- Recomendaciones provistas por autoridades relevantes.
- Medición de los indicadores del Sistema.

Revisión independiente de la seguridad de la información: a lo menos cada dos años se deberá revisar la Política General de Seguridad de la Información, y el estado del SGSI mediante auditorías internas o externas.

6.6 Cumplimiento

Todos los usuarios de REUNA, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deberán dar cumplimiento, en lo que les corresponda, a esta Política General de Seguridad de la Información, las políticas específicas y los procedimientos relacionados que se aprueben al efecto.

6.7 Sanciones

El incumplimiento de las obligaciones emanadas de esta Política, de las Políticas específicas del Sistema, Procedimientos u otros documentos que se deriven de éstos, serán sancionadas en los términos de las leyes vigentes y aplicables bajo el Reglamento Interno para los funcionarios de REUNA. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

7. MECANISMO DE DIFUSIÓN

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Plataforma Docs de REUNA
- Correo informativo. Con acuse de recibo obligatorio (Documento PDF con firma digital)
- Inducción a nuevos colaboradores
- Capacitación continua
- Reuniones informativas

8. PERÍODO DE REVISIÓN

La revisión del contenido de esta Política se efectuará a lo menos cada dos años por el Comité Interno de Seguridad, o atendiendo necesidades de cambios para garantizar su idoneidad, adecuación y efectividad.

9. EXCEPCIONES AL CUMPLIMIENTO DE LA POLÍTICA

Frente a casos especiales, se informará al Comité Interno de Seguridad con un plazo máximo de resolución de 5 días, para que evalúe y pueda establecer condiciones puntuales de excepción en el cumplimiento de las presentes directrices, siempre que no infrinja la legislación vigente. Toda excepción debe ser documentada y generar un proceso de revisión de la política, que determine si se deben agregar directrices en lo particular.

****