DOCUMENTO APROBADO MEDIANTE ACTA DE DIRECTORIO

REGISTROS DE REVISIÓN

Ingryd Soledad Gironda Santelices
Subgerente de Proyectos e Innovación
19/08/2024 16:50

Micaela Marlene Mamani Zuñagua
Supervisor de Riesgos
27/08/2024 16:07

Contenido

1. OBJETIVO

Preservar la confidencialidad, integridad y disponibilidad de la información, así como la protección de ésta, a fin de minimizar el daño y garantizar la continuidad operacional del negocio, a través del establecimiento de criterios y lineamientos para la administración, custodia, uso de la información y de los activos asociados a su tratamiento.

La información es un activo esencial, fundamental y factor estratégico para la gestión, operación y continuidad de los servicios y actividades de la EDV.

2. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de esta política comprende directa o indirectamente a: Accionistas, Directores, Síndicos, Alta Gerencia, todos los Funcionarios de la EDV y todas las personas con las que la EDV mantiene convenios, contratos u otros.

3. MARCO NORMATIVO

La presente Política se alinea a la siguiente normativa:

- Ley del Mercado de Valores Nro. 1834 de 31 de Marzo de 1998
- Recopilación de Normas para el Mercado de Valores, Libro 6°, Título I Reglamento de Entidades de Depósito de Valores, Compensación y Liquidación de Valores, Capítulo III Actividades y Funcionamiento de la Entidad de Deposito de Valores, Sección 1, Artículo 5° Seguridad.
- Recopilación de Normas para el Mercado de Valores, Libro 11°, Título I Requisitos de Seguridad, Capítulo I Reglamento para la Gestión de Seguridad de la Información.
- Norma ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de Gestión de la Seguridad de la Información - Requisitos

4. DEFINICIONES

ACTIVO DE INFORMACIÓN: Son aquellos datos, información, sistemas y elementos relacionados con la tecnología de la información, que tienen valor para la EDV.

ACUERDO DE NIVEL DE SERVICIO (SLA: SERVICE LEVEL AGREEMENT): Contrato en el que se estipulan las condiciones de un servicio en función a parámetros objetivos, establecidos de mutuo acuerdo entre un proveedor de servicio y la EDV.

ANÁLISIS Y EVALUACIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN: Proceso por el cual se identifican los activos de información, las amenazas y vulnerabilidades a las que se encuentran expuestos, con el fin de generar controles que minimicen los efectos de los posibles incidentes de seguridad de la información.

ÁREA DE EXCLUSIÓN: Área de acceso restringido identificada en las instalaciones de la EDV.

CENTRO DE PROCESAMIENTO DE DATOS (CPD): Ambiente físico clasificado como área de exclusión, donde están ubicados los recursos utilizados para el procesamiento de información.

CENTRO DE PROCESAMIENTO DE DATOS ALTERNO: Lugar alternativo provisto de equipos computacionales, equipos de comunicación, estaciones de trabajo, enlaces de comunicaciones, fuentes de energía y accesos seguros que se encuentran instalados en una ubicación geográfica distinta al Centro de Procesamiento de Datos.

CIFRAR: Proceso mediante el cual la información o archivos es alterada, en forma lógica, incluyendo claves en el origen y en el destino, con el objetivo de evitar que personas no autorizadas puedan interpretarla al verla, copiarla o utilizarla para actividades no permitidas.

CONFIDENCIALIDAD: Garantiza que la información se encuentre accesible únicamente para el personal autorizado.

CONTRASEÑA O CLAVE DE ACCESO (PASSWORD): Conjunto de caracteres que una persona debe registrar para ser reconocida como usuario autorizado, para acceder a los recursos de un equipo computacional o red.

CORTAFUEGOS (FIREWALL): Dispositivo o conjunto de dispositivos (software y/o hardware) configurados para permitir, limitar, cifrar, descifrar el tráfico entre los diferentes ámbitos de un sistema, red o redes, sobre la base de un conjunto de normas y otros criterios, de manera que sólo el tráfico autorizado, definido por la política local de seguridad, sea permitido.

DISPONIBILIDAD: Permite el acceso a la información en el tiempo y la forma que esta sea requerida.

EQUIPO CRÍTICO: Equipo de procesamiento de datos que soporta las principales operaciones de la EDV.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Suceso o serie de sucesos inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la EDV, amenazar la seguridad de la información y/o los recursos tecnológicos.

INTEGRIDAD: Busca mantener con exactitud la información completa, tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

INTERNET: Red de redes de alcance mundial que opera bajo estándares y protocolos internacionales.

INTERNET DE LAS COSAS (IoT): Sistema de dispositivos electrónicos interconectados que puede recopilar y transferir datos a través de una red inalámbrica sin intervención de personas.

INTRANET: Red interna de computadoras que haciendo uso de tecnología de internet, permite compartir información o programas.

INFRAESTRUCTURA DE TECNOLOGÍA DE LA INFORMACIÓN: Es el conjunto de hardware, software, redes de comunicación, multimedia y otros, así como el sitio y ambiente que los soporta, que es establecido para el procesamiento de las aplicaciones.

MEDIOS DE ACCESO A LA INFORMACIÓN: Son equipos servidores, computadores personales, teléfonos inteligentes, terminales tipo cajero automático, las redes de comunicación, Intranet, Internet y telefonía.

PLAN DE CONTINGENCIAS TECNOLÓGICAS: Documento que contempla un conjunto de procedimientos y acciones que deben entrar en funcionamiento al ocurrir un evento que dañe parte o la totalidad de los recursos tecnológicos de la EDV.

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP: BUSINESS CONTINUITY PLANNING): Documento que contempla la logística que debe seguir la EDV a objeto de restaurar los servicios y aplicaciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado, después de una interrupción o desastre.

PRINCIPIO DE MENOR PRIVILEGIO: Establece que cada programa y cada usuario del sistema de información debe operar utilizando los privilegios estrictamente necesarios para completar el trabajo.

PROCESO CRÍTICO: Proceso o sistema de información que al dejar de funcionar, afecta la continuidad operativa de la EDV.

PROCEDIMIENTO DE ENMASCARAMIENTO DE DATOS: Mecanismo que modifica los datos de un determinado sistema en ambientes de desarrollo y pruebas, con el fin de garantizar la confidencialidad de la información del ambiente de producción.

PROPIETARIO DE LA INFORMACIÓN: Es el responsable formalmente designado para controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos de información.

PROTECCIÓN FÍSICA Y AMBIENTAL: Conjunto de acciones y recursos implementados para proteger y permitir el adecuado funcionamiento de los equipos e instalaciones del Centro de Procesamiento de Datos y del Centro de Procesamiento de Datos Alterno, dada su condición de áreas de exclusión.

PRUEBAS DE INTRUSIÓN: Son pruebas controladas que permiten identificar posibles debilidades de los recursos tecnológicos de la EDV, que un intruso podría llegar a explotar para obtener el control de sus sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores y/o dispositivos de red. Las pruebas de intrusión pueden ser realizadas a través de la red interna, desde Internet, accesos remotos o cualquier otro medio.

RESPALDO O COPIA DE SEGURIDAD (BACKUP): Copia de información almacenada en un medio digital, que se genera en forma periódica, con el propósito de utilizar dicha información, en casos de emergencia o contingencia.

SEGURIDAD DE LA INFORMACIÓN: Conjunto de medidas y recursos destinados a resguardar y proteger la información, buscando mantener la confidencialidad, confiabilidad, disponibilidad e integridad de la misma.

SISTEMA DE INFORMACIÓN: Conjunto organizado e interrelacionado de procedimientos de recopilación, procesamiento, transmisión y difusión de información que interactúan entre sí para lograr un objetivo.

SITIO EXTERNO DE RESGUARDO: Ambiente externo al Centro de Procesamiento de Datos, donde se almacenan todos los medios de respaldo, documentación y otros recursos de tecnología de información catalogados como críticos, necesarios para soportar los planes de continuidad del negocio y contingencias tecnológicas.

SOFTWARE: Equipamiento o soporte lógico de un sistema de información que comprende el conjunto de los componentes lógicos que hacen posible la realización de tareas específicas. El software incluye: software de sistema, software de programación y software de aplicación.

TRANSFERENCIA ELECTRÓNICA DE INFORMACIÓN: Forma de enviar y/o recibir en forma electrónica, datos, información, archivos y mensajes, entre otros.

TECNOLOGÍA DE INFORMACIÓN (TI): Conjunto de procesos y productos derivados de herramientas (hardware y software), soportes de la información y canales de comunicación relacionados con el almacenamiento, procesamiento y transmisión de la información.

USUARIO DEL SISTEMA DE INFORMACIÓN: Persona identificada, autenticada y autorizada para utilizar un sistema de información. Ésta puede ser Funcionario de la EDV (Usuario Interno del sistema de información) o cliente (Usuario Externo del sistema de información).

5. ROLES Y RESPONSABILIDADES

ACCIONISTAS, DIRECTORES, SINDICOS, ALTA GERENCIA Y FUNCIONARIOS DE LA EDV

Los Accionistas, Directores, Síndicos, Alta Gerencia y todos los Funcionarios de la EDV deben:

a. Preservar la integridad, confidencialidad y disponibilidad de la información.
b. Contribuir en la gestión de riesgos mediante el cumplimiento de los lineamientos y principios de la presente Política y de las políticas que se desprendan de la misma.
c. Reportar todo incidente de seguridad de la información que sea de su conocimiento.

AUDITORÍA INTERNA

Auditoría Interna es la responsable de verificar que la Gestión de Seguridad de la Información, esté operando de acuerdo a los alcances y objetivos definidos en la presente política.

COMITÉ DE GESTIÓN INTEGRAL DE RIESGOS

El Comité de Gestión Integral de Riesgos revisa y propone para aprobación del Directorio la estrategia, políticas para la gestión de la Seguridad de la Información.

DIRECTORIO

Órgano de gobierno que aprueba y realiza seguimiento a los lineamientos, estrategia, políticas para la gestión de la Seguridad de la Información.

GERENCIA DE GESTIÓN INTEGRAL DE RIESGOS

Es la responsable de evaluar, diseñar, proponer y sustentar ante el Directorio a través del Comité de Gestión Integral de Riesgos, la estrategia y políticas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información y garantizar la continuidad operacional del negocio, así como identificar, medir, monitorear, controlar y divulgar los riesgos relacionados a la Seguridad de la Información, que no se encuentren de acuerdo a las políticas vigentes.

GERENCIA GENERAL

La Gerencia General es la responsable de proponer a los órganos que establezca el Directorio, la estrategia y políticas necesarias para salvaguardar la confidencialidad, integridad y disponibilidad de la información y garantizar la continuidad operacional del negocio.

GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN

Es la gerencia responsable de implantar los lineamientos de la Política de Seguridad de la Información, para la protección de los activos de información y la gestión de adquisición de programas, sistemas, aplicaciones e infraestructura tecnológica relacionados a Tecnología de la Información, a través del Plan Estratégico de Tecnología de la Información.

SUPERVISOR DE SEGURIDAD DE LA INFORMACIÓN

Gestionar con las instancias que correspondan en la EDV, la implementación, revisión, actualización y difusión de la Política de Seguridad de la Información, así como la normativa que se desprende de la misma.

Establecer los mecanismos para la administración y el control de la seguridad sobre el acceso lógico y físico a los distintos ambientes tecnológicos y recursos de información.

Debe asegurarse que los Accionistas, Directores, Síndicos, miembros independientes del Comité de Auditoría (no Directores), Consejeros, Alta Gerencia, todos los Funcionarios de la EDV y todas las personas con las que la EDV mantiene convenios, contratos u otros, tengan conocimiento de la presente política y sus procedimientos.

6. CONTENIDO

6.1. LINEAMIENTOS APLICABLES A LA SEGURIDAD DE LA INFORMACIÓN

Los lineamientos de la EDV en relación a Seguridad de la Información son los siguientes:

a. Proteger la información propia y de sus participantes, reduciendo el impacto de fugas de información, accesos no autorizados, fraude, divulgación, modificación no autorizada y destrucción o deterioro de la misma.

b. Los accesos lógicos y físicos asignados a los usuarios internos y externos deberán basarse en el principio del mínimo privilegio de acuerdo a la segregación de funciones, evitando conflicto de intereses.
c. El acceso a los datos deberá ser otorgado de acuerdo con la segregación de funciones, definiendo los privilegios para crear, leer, actualizar, ejecutar y borrar los mismos.
d. Usuarios y contraseñas como medios de acceso, son personales e intransferibles porque son la identidad que previenen accesos no autorizados.
e. Todos los incidentes o debilidades de Seguridad de la Información deben ser informados de acuerdo al *Plan de Respuesta a Incidentes de Seguridad de la Información (RGS04.GR.PL01)*.
f. Difundir la cultura de Seguridad de la Información a todos los órganos de gobierno de la EDV, así como la Alta Gerencia y los Funcionarios de la EDV.
g. Realizar el análisis y evaluación de riesgos en Seguridad de la Información que permita identificar los activos de información, amenazas y vulnerabilidades a los cuales se encuentran expuestos a fin de generar controles que minimicen los efectos de los posibles incidentes de Seguridad de la Información.
h. La EDV proporcionará los medios para que la información esté disponible para los participantes y usuarios externos e internos, conforme a los acuerdos de niveles de servicios.
i. Otros lineamientos que disponga la normativa aplicable y/o el Directorio.

La presente Política de Seguridad de la Información y el conjunto de políticas en materias específicas que se desprendan de la misma, regirán sin importar como se represente, almacene y transmita la información, los sistemas que la procesen o los métodos de transporte utilizados (Ejemplo: Bases de datos, respaldos magnéticos, información impresa, internet, etc.).

6.2. CLASIFICACIÓN DE INFORMACIÓN

Para establecer los adecuados derechos de acceso a los datos administrados en sus sistemas de información, así como la información física, la información deberá ser clasificada acuerdo a lo siguiente:

1. Sensibilidad y criticidad de la información: Según el mayor riesgo calculado para cada elemento de información durante la evaluación de riesgos.

2. Valor de la información: Según los impactos evaluados durante la evaluación de riesgos considerando la importancia que posee para la EDV.

3. Obligaciones legales y contractuales: Según Ley del Mercado de Valores Nro. 1834 de 31 de Marzo de 1998, la Recopilación de Normas para el Mercado de Valores Libro 6°, Título I, Reglamento de Entidades de Depósito de Valores, Compensación y Liquidación de Valores y Libro 11°, Título I, Capítulo I Reglamento para la Gestión de la Seguridad de la Información.

La *Política de Gestión de Activos de Información (RSG03.GR.PO02)*, debe dar los lineamientos de protección de información Reservada y Privilegiada establecida en la Ley del Mercado de Valores Nro. 1834 de 31 de Marzo de 1998, además de los lineamientos para el tratamiento de la información propia de la EDV.

6.3. SEGURIDAD DE LA INFORMACIÓN PARA PROVEEDORES

Las compras o adquisiciones de programas, sistemas, aplicaciones e infraestructura tecnológica en forma previa a la adquisición se deberá realizar un análisis, conforme a lo descrito en la *Norma de Compras y Contrataciones (ADM04.AF.NR01)*, que considera lo siguiente:

- Análisis de riesgo tecnológico y costo beneficio
- Dependencia aceptable
- Disponibilidad de Código Fuente
- Acuerdos de Niveles de Servicio
- Acuerdos de Confidencialidad

Las cláusulas de seguridad incluidas en el contrato con el proveedor deben basarse en los resultados de la evaluación y tratamiento de riesgos; sin embargo, las cláusulas que establecen la confidencialidad y la devolución de activos una vez finalizado el acuerdo son obligatorias. Además, los contratos deben garantizar la entrega confiable y segura de productos y servicios.

6.4. SEGURIDAD PARA INTERNET DE LAS COSAS

Todo dispositivo (IoT) que sea conectado a la red interna de la Entidad debe contar previamente con la aprobación del Supervisor de Seguridad de la Información y el Visto Bueno de la Gerencia de Tecnología de la Información, adicionalmente, se debe realizar un análisis de Riesgos del impacto que podría ocasionar esta interconexión en la Infraestructura de la Entidad.

6.5. MEDIOS TECNOLÓGICOS DE TELETRABAJO

Todo medio tecnológico e informático asignado para su uso en el teletrabajo debe contar con la aprobación del Supervisor de Seguridad de la Información y el Visto Bueno de la Gerencia de Tecnología de la Información, y adicionalmente debe realizarse el análisis de cumplimiento de la *Política de Teletrabajo (ADM02.AF.PO02)*.

6.6. SANCIONES POR INCUMPLIMIENTO

Todo incumplimiento de lo establecido en la presente Política de Seguridad de la Información será considerado falta y será sancionado según la gravedad de ésta, previa evaluación de la intencionalidad, impacto y daño que cause a la EDV, de acuerdo a las disposiciones legales vigentes, conforme al *Procedimiento Disciplinario y de Sanciones (ADM02.AF.FP05).*

7. DISPOSICIÓN FINAL

A partir de la presente política se desprende un conjunto de políticas específicas, junto con sus respectivos procedimientos, planes y otras herramientas de implementación.

8. CONTROL DE CAMBIOS

Razón del cambio	Descripción del cambio
Revisión anual a solicitud de la Gerencia de Gestión Integral de Riesgos de acuerdo con la normativa vigente	• En el numeral 3. Marco Normativo, se agregó como referencia las siguientes normas: - Recopilación de Normas para el Mercado de Valores, Libro 6, Título I, Capitulo III Actividades y Funcionamiento de la Entidad de Deposito de Valores, Sección 1, Artículo 5° Seguridad. - Norma ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad – Sistemas de Gestión de la Seguridad de la Información – Requisitos. • En el numeral 4. Definiciones, se agregó la definición del término Internet de las cosas (IoT). • En el numeral 6.1 (antes 6) Lineamientos Aplicables a la Seguridad de la Información, se añadió el inciso *c. El acceso a los datos deberá ser otorgado de acuerdo con la segregación de funciones, definiendo los privilegios para crear, leer, actualizar, ejecutar y borrar los mismos.* • En el numeral 6.6 (antes 11) Sanciones por incumplimiento, se referenció al Procedimiento Disciplinario y de Sanciones (ADM02.AF.FP05) el cual detalla las acciones para la aplicación de las sanciones. • Se realizaron modificaciones menores de forma y redacción.