POLÍTICA DE SEGURIDAD DE CONTINUIDAD DE NEGOCIOS

CODIGO: GA010035

RUTA DE VALIDACIÓN		
FUNCIÓN	CARGO	UNIDAD ORGANIZATIVA
ELABORADO POR:	Jefe de riesgo Tecnológico	Riesgo Tecnológico
REVISADO POR:	Miembros del Comité de Seguridad	Comité de Seguridad
APROBADO POR:	Miembros del Comité de Seguridad	Comité de Seguridad

Contenido

1 Control de Versiones

Versión vigente

Versión	Realizado por	Fecha	Revisado por	Fecha	Aprobado por	Fecha
00	Jefe de riesgo Tecnológico	2021	Miembros del Comité de Seguridad	2021	Miembros del Comité de Seguridad	2021

Historial de versiones

Versión	Vigente a partir de	Detalle de los cambios

2 Objetivo

La protección de la información y de los activos destinados a su tratamiento incluye medidas de diversas índoles. Se requieren tanto medidas tecnológicas como acciones que exigen la participación y compromiso de los usuarios.

Entre las medidas destinadas a la protección de la información, que presentan aspectos tanto tecnológicos como organizacionales, se encuentran las destinadas a procurar la continuidad de las operaciones de la organización.

Esta política define las reglas y criterios de seguridad que rigen la confección y mantenimiento del Plan de Continuidad del Negocio. Este plan debe permitir la más pronta recuperación de los servicios críticos frente a desastres, en los que todas o una parte de sus operaciones, servicios computacionales y/o servicios de comunicaciones se interrumpen o disminuyen significativamente.

Entre los procesos que deben ser considerados como objetivos de continuidad se debe incluir el proceso de Seguridad de la Información, de esta forma, se debe velar por la continuidad de la protección de los activos y por la continuidad de los procesos de gestión de seguridad aun frente a desastres.

3 Alcance

Esta Política aplica para todas las sociedades que integran el Grupo Andinas (Aguas Andinas S.A., Aguas Cordillera S.A., Aguas Manquehue S.A., Gestión y Servicios S.A., Análisis Ambientales S.A., Ecoriles S.A. y Aguas del Maipo S.A.), y deberá observarse por todas las personas que forman parte de dichas sociedades en todos sus niveles (directores, trabajadores y trabajadoras), que actúen en Chile o el extranjero. También otros terceros que actúan en nombre de la empresa.

Adicionalmente, aplica a todas las empresas, filiales y asociaciones en las que alguna sociedad del Grupo Andinas tenga el control. En aquellos casos en que la empresa

carezca de dicho control o tenga igualdad de participación con otros asociados, se deberá instar a que se adopten e implementen políticas y medidas que contribuyan a proteger la información de la Empresa.

Esta política considera la protección de la información en caso de situaciones de contingencia o desastre.

Se incluyen las situaciones de Interrupción por daños en la infraestructura, servicios e instalaciones.

Se incluyen las situaciones de Interrupción del funcionamiento de los sistemas computacionales por fallas de hardware, software o comunicaciones.

Interrupción de los procesos críticos de negocio por ausencia de personal interno o externo.

Este documento complementa (y no reemplaza o modifica) las definiciones respecto a continuidad de negocios que se establecen como parte del Sistema de Gestión de Continuidad de Negocios y aún cuando trata aspectos relativos a planes de continuidad, lo hace considerando la protección de la información, en situaciones de desastre.

4 Definiciones

Plan de Continuidad de Negocio : Plan utilizado por una organización para responder ante la interrupción de los procesos críticos de negocio.

Análisis de Impacto en el Negocio (BIA, por Bussiness Impact Analysis). : Corresponde al estudio que se realiza a los procesos de negocio de la organización para determinar el nivel de dependencia que existe de esos procesos y definir la necesidad y prioridad de recuperación.

Tiempo Objetivo de Recuperación (RTO, por Recovery Time Objetive). : Se trata del tiempo que la organización está dispuesta a asumir entre el momento de la interrupción de un proceso y el momento en que el proceso se restablece y se recuperan los datos eliminados.

Punto objetivo de Recuperación (RPO, por Recovery Point Objetive). : Corresponde a la máxima pérdida de datos aceptable, para un proceso de negocios.

5 Roles y Responsabilidades

Gerente General

- Velar por la existencia de un Plan de Continuidad de Negocios vigente.
- Velar por la inclusión del proceso de Seguridad de la Información, en los planes de continuidad de negocios.
- Aprobar los planes desarrollados, junto con verificar el éxito de las pruebas a las que periódicamente se les somete.

Equipo de Gestión de Crisis

- Coordinar y responder por la adecuada ejecución de las acciones definidas en el plan, para cada área o función.

Comité de Seguridad de la Información

- Verificar la inclusión del proceso de Seguridad de la Información en los planes de continuidad.
- Aprobar el resultado y conclusiones de la evaluación de riesgo y del Plan de Continuidad del Negocio.
- Velar por la vigencia de los planes de continuidad del negocio.

6 Directrices

6.1 Formalización del Plan de Continuidad de Negocio

- El Plan de Continuidad del Negocio (BCP por Business Continuity Plan) debe ser formalmente escrito, divulgado, probado y periódicamente revisado y actualizado.

6.2 Identificación de Procesos Críticos

- Se deben identificar los procesos de los que la empresa depende para la correcta y oportuna entrega de los servicios que ha comprometido con su entorno de negocios. Entre los procesos críticos para el funcionamiento de la organización, se debe considerar el proceso de Seguridad de la Información
- Al mismo tiempo que se identifican los procesos críticos, se debe determinar el tiempo que la empresa puede resistir la falta de disponibilidad del proceso (RTO) y la cantidad de datos que puede perder en un siniestro antes que se comprometa la operación de la organización (RPO).

- El análisis de impacto debe determinar cuáles son los procesos de negocio críticos y una ponderación de su criticidad, incluyendo el tiempo máximo de interrupción tolerable por cada uno de estos procesos.
- Para cada proceso crítico identificado, se debe definir, recopilar y conservar un conjunto de información vital, entre la que se cuenta:
    - Objetivo del proceso
    - Descripción general
    - Dependencia de otros procesos
    - Recursos materiales utilizados
    - Recursos humanos involucrados

6.3 Evaluación de Riesgo

- Una vez determinada la criticidad de los procesos, se deben identificar los escenarios de amenazas conocidas que puedan afectar la continuidad de las operaciones de Grupo Andinas, a fin de determinar los riesgos a los que esos procesos están expuestos y reconocer los controles y protecciones que se deben implantar para minimizar los riesgos de interrupciones.

6.4 Estrategia de Continuidad y Recuperación

- Se deben identificar, analizar y evaluar estrategias que satisfagan los requerimientos del negocio, seleccionando e implantando las más adecuadas, en función de su eficiencia y eficacia.
- Se deben definir los procedimientos específicos según cada escenario determinado, para mantener activos los servicios para los clientes, el proceso de Seguridad de la Información y minimizar los tiempos de interrupción, ante la ocurrencia de un evento disruptivo.

6.5 Organización, Documentación y Difusión de los Planes

- Se deben construir procedimientos específicos para la recuperación de los procesos en los escenarios de interrupciones reconocidos.
- Se debe velar por la coherencia de los contenidos e interdependencias de las acciones y procedimientos definidos para la continuidad del negocio de Grupo Andinas.
- Se debe velar por la adecuada difusión de los planes actualizados y los procedimientos asociados, a todos los involucrados, resguardando su disponibilidad frente a contingencias.
- Se debe proteger la información contenida en estos documentos, de acuerdo con la clasificación de la confidencialidad de sus elementos componentes.

6.6 Administración de Crisis

- Debe existir un Plan de Administración de Crisis, definido como el eje central común, que controle las acciones que se ejecutan ante cualquier escenario de contingencia definido.
- Este plan debe ser desarrollado con el objetivo de fijar los procedimientos de activación y notificación de la crisis, coordinación de la comunicación con los medios internos y externos, así como la coordinación de la restauración de las operaciones.

6.7 Capacitación y Sensibilización respecto del Plan

- Se debe establecer un programa formal de capacitación para todo el personal involucrado en los diferentes planes.

- De la misma forma, se debe capacitar respecto a las mejores prácticas de seguridad y continuidad y las acciones que se desprendan de estos planes.

6.8 Pruebas

- Se deben definir, programar, ejecutar y revisar los resultados de un conjunto de pruebas de los planes desarrollados. El principal objetivo de estas pruebas es verificar el funcionamiento de los planes y encontrar oportunidades de mejoras.
- Estas pruebas deben ser cuidadosamente programadas, para que el desarrollo de las actividades de las pruebas no cause daño a la operación normal de la empresa.

7 Flujograma

N/A

8 Anexos

N/A