**POLÍTICA DE PLANIFICACIÓN DE LA COTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**

**I.- DEFINICIONES ESTRATÉGICAS**

El presente documento contiene la definición respecto de la planificación de la continuidad de la seguridad de la información que deberá ser utilizada como mecanismo para continuar proporcionando el servicio afectado en caso de la ocurrencia de una contingencia que afecte el normal funcionamiento de la infraestructura tecnológica, de las comunicaciones y de los sistemas tecnológicos proporcionados por la empresa.

**a.- Objetivo general**

El objetivo de este documento es brindar una guía que permita, al personal designado por la [Unidad TIC] y en coordinación con las directrices del [Directorio o Gerencia], gestionar de mejor forma el desempeño diario de las tareas que involucran los activos de información de acuerdo con la normativa vigente, respecto de contingencias catastróficas o emergencias que impidan la operación normal de las plataformas tecnológicas que soportan los servicios y productos de la empresa.

El foco estará centrado en aquellas actividades críticas para el negocio según definición expresa del [Directorio o Gerencia General].

**b.- Objetivos específicos**

Establecer las acciones que la organización debe seguir, ante un incidente catastrófico, para recuperar y restaurar las actividades críticas del negocio en un tiempo prudencial y de manera progresiva regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información.

Establecer acciones concretas de prueba de los planes de continuidad. Uno de los aspectos más importante dentro de la gestión de la continuidad del negocio es que los planes de continuidad sean probados. De nada sirve tener todo documentado, definidos los responsables, contar con la tecnología de respaldo si no se hacen pruebas para determinar que las actividades definidas para responder ante una contingencia catastrófica o emergencia son las adecuadas para la organización. Si bien el estándar es único, la forma en que se desarrolla y se aplica es específico para cada institución y debe estar en concordancia con los procesos más críticos del negocio.

Determinar los requisitos para la seguridad de la información y la continuidad de la administración de la seguridad de la información ante situaciones adversas, es decir, durante una crisis o desastre.

Determinar si la continuidad de la seguridad de la información se incluye dentro del

proceso de administración de continuidad del negocio o dentro del proceso de administración de recuperación ante desastres. Se deberán determinar los requisitos de seguridad de la información al planificar la continuidad comercial y la recuperación ante desastres. En la ausencia de una continuidad comercial formal y una planificación de recuperación ante desastres, la administración de seguridad de la información debería suponer que los requisitos de seguridad de la información siguen siendo los mismos ante situaciones adversas, en comparación con las condiciones operacionales normales. De manera alternativa, la institución puede desarrollar un análisis de impacto comercial para los aspectos de seguridad de la información y determinar los requisitos de seguridad de la información que se aplican a situaciones adversas.

La empresan deberá satisfacer los siguientes objetivos operativos:

* exista una estructura de administración adecuada para prepararse para, mitigar y responder ante un evento disruptivo que utiliza personal con la autoridad, la experiencia y la competencia necesaria;
* se nomine al personal de respuesta ante incidentes con la responsabilidad, la autoridad y la competencia necesaria para administrar un incidente y mantener la seguridad de la información;
* que se desarrollen y aprueben planes documentados, los procedimientos de respuesta y recuperación detallando cómo la organización administrará un evento disruptivo y mantendrá la seguridad de su información a un nivel predeterminado, en base a los objetivos de continuidad de la seguridad de la información aprobada por el [Comité de Riesgos y Seguridad de la Información] y el [Directorio o Gerencia General].

De acuerdo con los requisitos de continuidad de la seguridad de la información, la organización deberá establecer, documentar, implementar y mantener:

* controles de seguridad de la información dentro de la continuidad comercial o los procesos, procedimientos y sistemas y herramientas de apoyo;
* procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa incluyendo los controles de compensación necesarios para minimizar el riesgo;

**c.- Alcance**

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la [Empresa XXX]. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la [Empresa XXX], establecidos en el documento institucional denominado Definiciones Estratégicas o equivalente, cubriendo a toda la organización independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

**d.- Roles y Responsabilidades**

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

**e.- Vigencia y Actualización**

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Riesgos y Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la [Empresa XXX].

La Política deberá ser revisada por el Comité de Seguridad de la Información. No obstante, aquello, la [Unidad responsable de Ciberseguridad] promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSI.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

* Cambios en las leyes o reglamentos que afecten a la [Empresa XXX].
* Incorporación o modificaciones relevantes de procesos críticos de la [Empresa XXX].
* Cambios significativos al soporte tecnológico.
* Modificaciones en la estructura de la organización.
* Cambios significativos en los niveles de riesgo a que se expone la información.
* Cambios relevantes en las Definiciones Estratégicas.
* Ajustes necesarios producto de Estados de Excepción Constitucional.
* Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

**f.- Revisión del cumplimiento**

El Comité de Riesgos y Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

**g.- Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información (SGSI) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

* Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
* Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Riesgos y Seguridad, incorporando Tabla en Capitulo final en cada documento.
* Se deberá controlar el uso no intencionado de documentos obsoletos.
* En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

**h.- Difusión**

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el [Comité de Riesgos y Seguridad de la Información] estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

**II.- PLAN DE CONTINUIDAD OPERACIONAL**

Para guiar el plan en lo relativo a su diseño, construcción e implementación, mientras no exista normativa o ley vigente que regule la materia y sus parámetros, se utilizarán como guía de buenas prácticas para la implementación de un sistema de gestión de la continuidad del negocio, los estándares internacionales ISO 22.301, ISO 27.002 e ISO 27.031.

**a.- Establecer el alcance inicial para el sistema de gestión de la continuidad del negocio**

La selección de los procesos a incluir en el alcance del sistema debe estar basada en la definición del apetito al riesgo, el cual debe ser preparado por el [Comité de Riesgos y Seguridad de la Información] y aprobado por el [Directorio o la Gerencia General], para garantizar que esté conforme con la definición estratégica de la empresa.

Se analiza el universo de procesos y unidades organizacionales a incorporar de acuerdo con lo establecido en la presente política, incorporando el máximo de criterios relevantes:

Como primera etapa se propone implementar un plan de continuidad operacional enfocado a riesgos tecnológicos generales o riesgos base, que permitan mitigar eficientemente un amplio rango amenazas que potencialmente pueden afectar a procesos críticos asociados a las plataformas de servicio.

* + Pérdida de suministro de energía eléctrica
  + Corte en los enlaces de comunicaciones
  + Falla en los equipos de comunicaciones
  + Ataque de virus informático
  + Falla operacional en el sitio principal (centro de procesamiento de datos)
  + Operación bajo situación de Fuerza Mayor u otras contingencias locales.

Como segunda etapa se propone un plan de continuidad operacional enfocado en los siguientes aspectos:

* Análisis de relevancia respecto de sus definiciones estratégicas de negocio.
* Análisis de relevancia respecto del impacto ante la disrupción de sus servicios hacia los clientes.
* Análisis técnico, económico y jurídico en recursos que podría implicar sumarlo al Plan de Continuidad.
* Análisis técnico, económico y jurídico en recursos humanos que podría implicar sumarlo al Plan de Continuidad. En particular las consideraciones relevante del teletrabajo o trabajo a distancia como un factor importante para la continuidad operacional ante fallas en las instalaciones principales o dificultades importantes para acceder físicamente a ellas.
* Análisis en recursos económicos que podría implicar sumarlo al Plan de Continuidad.

**b.- Realizar perfilamiento de nuevos riesgos adicionales a los riesgos base**

Se levanta el apetito de riesgo institucional y el perfil de riesgos mediante un proceso de evaluación de riesgos, criticidad de los activos de información.

Dentro de esta fase se establecen los escenarios de amenazas más probables bajo las cuales actuará el plan de continuidad operacional institucional.

**c.- Identificar los activos estratégicos y actividades críticas vinculados a:**

* Procesos, activos e Información sensible.
* Procesos, activos e Información interna.
* Procesos, activos e Información confidencial.
* Procesos, activos e Información vinculada a la infraestructura crítica o de terceras partes ya sea pública o privada. Esta definición puede provenir desde directivas legales vigentes. Este aspecto se aplica también en la medida que la empresa se constituya como proveedora de servicios para un tercero que tenga catalogación de actividad crítica o estratégica para el país.
* Procesos, activos e información relacionada con materias de Seguridad Nacional. Este especto puede aplicar en caso de que la empresa se constituya en proveedor de instituciones que implementan la Seguridad Nacional.

**d.- Establecer parámetros estratégicos**

La normativa internacional establece diferentes parámetros y factores a considerar en el plan de continuidad operacional institucional. Estos parámetros definen las condiciones de borde, entre otros aspectos, para los cuales se gatilla la activación del Plan y sus diferentes criterios de diseño.

Se deben establecer los impactos en la institución (BIA Bussines Impact Analysis), tiempos de espera antes de guillar el plan, tiempos de puesta en marcha de la operación en contingencia, impacto en la calidad del servicio cuando se opera en contingencia, tiempos asociados para la restauración de las operaciones normales cuando la contingencia haya desaparecido, entre otros que son funcionales a la institución.

**e.- Diseñar la solución**

Se diseñarán las soluciones con o sin tecnología pertinentes a cada uno de los escenarios establecidos y para los procesos o actividades debidamente seleccionados para ser incluidos en la continuidad operacional del negocio (BCP).

Una vez implementados los planes de continuidad operacional para los riesgos establecidos, se iniciará el diseño de planes de recuperación ante desastres (DRP Disaster Recovery Plan) y las estrategias para su implementación.

**f.- Implementar las Soluciones**

Los planes de continuidad operacional para cada riesgo definido se implementarán precaviendo márgenes de holgura para imprevistos.

**h.- Sensibilizar y capacitar**

Es crucial que quienes vayan a ser parte de la operación del plan de continuidad operacional institucional estén perfectamente entrenados y capacitados para articularlo, coordinarlo y gestionarlo cuando las condiciones sean adversas y la contingencia está actuando.

Por otro lado, los usuarios deben estar conscientes de cómo se debe funcionar en la modalidad de contingencia, teniendo muy claro quienes tendrán servicios activos y quienes no.

**i.- Realizar pruebas**

Uno de los aspectos prioritarios para contar con un sistema de continuidad operacional del negocio exitoso es poder contar con un plan de pruebas de éste, garantizando a través de estas que es funcional y todos los actores conocen el protocolo de acción y respuesta.

La meta es lograr que los usuarios que participan del plan tanto sus operadores como los usuarios de los sistemas cubiertos tengan absoluta claridad del proceder.

En este contexto, y en tanto no exista una definición operativa que eleve la exigencia por normativa de la empresa o exigencia legal, los planes de continuidad se probarán al menos una vez al año, generándose informes y análisis del proceso de prueba.

**j.- Aplicar mejora continua**

Como producto de las pruebas y simulaciones de contingencias quedarán informes de análisis de estas. Estos informes deben contener análisis de la efectividad del plan, cumplimiento de los tiempos, nivel de involucramiento y conocimiento de los operadores y de los usuarios; detección de problemas en el plan, respecto de los operadores, de los usuarios, de las tecnologías y plataformas si fueren parte de este, de los proveedores de servicios atingentes al plan.

Con toda la información recopilada de las pruebas o ejecuciones reales del plan, el [Comité de Riesgos y Seguridad de la Información], debe identificar puntos de mejora del plan y establecer una estrategia para:

* Diseñar las correcciones pertinentes en el plan.
* Diseñar los ajustes tecnológicos y de plataforma que sean necesarios.
* Implementar un plan de sensibilización sobre los cambios y mejoras.
* Plan de implementación de las mejoras.
* Plan de pruebas acotado para corroborar la operatividad de las mejoras integradas al plan de continuidad operacional.

**II.- MODO DE OPERACIÓN DEL PLAN.**

La operación del plan deberá quedar establecida en un procedimiento de continuidad operacional para cada riesgo definido, con los detalles específicos de los procesos y actividades críticas involucrados, con la definición de roles y responsabilidades claramente definidas, los aspectos tecnológicos involucrados y un flujo detallado de la operación bajo contingencia de los riesgos señalados y los canales de comunicación definidos para el control del riesgo.

La activación del Plan de Contingencia que deberá ser dictaminada por el líder de la contingencia se deberá realizar mediante un comunicado masivo correo electrónico o por cualquier otro método disponible informado al equipo de contingencia, a los usuarios y clientes.

Debe considerarse que en caso de que las actividades y funciones de la empresa sean por si mismas o tengan relación cliente-proveedor con infraestructura crítica, deberán informar según la legislación vigente los incidentes y los protocolos de respuesta a ellos.

**III.- ESCENARIOS POSIBLE A CONSIDERAR EN LA DEFINICIÓN DE LOS RIESGOS.**

**a.- Escenarios**

El escenario considerado en esta política es la indisponibilidad de los sistemas que soportan los procesos críticos definidos en el alcance. Este escenario puede ser provocado por las siguientes causas, por acción deliberada (D), accidental (A) o ambiental (E), según la notación ISO 27.005, entre otras:

**Desastre por indisponibilidad de las instalaciones**

Corresponde a la pérdida de las instalaciones físicas o suministros básicos que soportan los sistemas de información, frente a la materialización de un desastre, o la imposibilidad de acceder a las instalaciones.

Estas amenazas pueden ser generadas por las siguientes causas:

* Fuego. [A,D,E]
* Agua. [A,D,E]
* Contaminación. [A,D,E]
* Incidente importante. [A,D,E]
* Destrucción de equipamiento o medios. [A,D,E]
* Polvo, corrosión o congelamiento. [A,D,E]
* Fenómeno climático. [E]
* Fenómeno sísmico. [E]
* Fenómeno volcánico. [E]
* Fenómeno meteorológico. [E]
* Inundación. [E]
* Falla de aire acondicionado o sistema de suministro de agua. [A,D]
* Pérdida de suministro de energía. [A,D,E]
* Falla de equipamiento de telecomunicaciones. [A,D]
* Ataques terroristas. [D]
* Interrupciones organizadas o deliberadas (Sabotaje). [D]
* Radiación electromagnética. [A,D,E]
* Radiación térmica. [A,D,E]
* Pulsos electromagnéticos. [A,D,E]

**Desastre por sabotaje de ciberseguridad**

De acuerdo con su efecto, los sabotajes de Ciberseguridad se pueden dividir en aquellos:

* Orientados a afectar programas (Software Básico, Aplicaciones o Datos).
* Destinados a afectar las capacidades de procesamiento.
* Con el objetivo de interrumpir las comunicaciones.

Algunas amenazas específicas que se pueden considerar:

* Señales de interferencia e interceptación que comprometen la información crítica. [D]
* Espionaje remoto. [D]
* Escucha secreta. [D]
* Robo de medios o documentos. [D]
* Robo de equipos. [D]
* Recuperación de medios reciclados o descartados. [D]
* Divulgación de información crítica. [A,D]
* Datos de fuentes poco fiables. [A,D]
* Manipulación con hardware. [D]
* Manipulación con software. [A,D]

**Desastres por falla técnica**

Pueden dañar seriamente la continuidad de las operaciones tecnológicas, pudiendo afectar a servidores, almacenamiento, las comunicaciones o suministro de energía.

Estas amenazas pueden ser generadas por las siguientes causas:

* Fallos de equipo. [A]
* Mal funcionamiento del equipo. [A]
* Saturación del sistema de información. [A,D]
* Mal funcionamiento del software. [A]
* Brecha de mantenimiento del sistema de información. [A,D]
* Fallos en el suministro eléctrico. [A,D,E]
* Virus, amenazas y ataques informáticos. [D]

**Desastre por acciones no autorizadas:**

Algunas amenazas específicas que se pueden considerar:

* Uso no autorizado del equipamiento, [D]
* Copia fraudulenta de software. [D]
* Uso de software falsificado o copiado. [A,D]
* Corrupción de datos. [D]
* Procesamiento ilegal de datos. [D]

**Desastre por efecto de compromiso de funciones:**

Algunas amenazas específicas que se pueden considerar:

* Error de uso. [A]
* Abuso de derechos. [A,D]
* Falsificación de derechos. [D]
* Brecha de disponibilidad de personal. [A,D,E]

**Desastre por acciones específicamente humanas:**

Algunas amenazas específicas que se pueden considerar:

* Acción de hackers/crakers. [A,D]
* Acción de delitos informáticos. [A,D]
* Acción terrorista. [D]
* Acción de espionaje industrial (inteligencia de compañías, gobiernos extranjeros). [D]
* Acciones internas (empleados pobremente entrenados, descontentos, maliciosos, negligentes, deshonestos o despedidos). [D]

Al momento de ocurrir una situación disruptiva que afecte el normal funcionamiento de los procesos de la Subsecretaría del Interior o el Servicio de Gobierno Interior, se deberá aplicar los planes definidos para mitigar el riesgo ocurrido. Es responsabilidad del Encargado de Ciberseguridad velar por mantener la seguridad de la información durante la administración de la situación.

**b.- Controles**

Se establecen como requisitos de seguridad, en los casos que sea posible y dependiendo de las circunstancias, los siguientes:

**Controles de seguridad física:**

* Cuidar y proteger áreas que contienen y/o procesan información.
* Proteger y mantener controles físicos de entrada a las áreas seguras.
* Restringir a lo estrictamente necesario el ingreso de proveedores, privilegiando a aquellos que sean indispensables para la ejecución de los planes.
* Monitorear y controlar el uso y acceso a las áreas de carga y descarga.
* Verificar las condiciones ambientales de manera de evitar que éstas puedan afectar adversamente a la operación de las instalaciones de procesamiento de información y en las áreas seguras.

**Controles de seguridad para sistemas y redes:**

* En el caso que la contingencia afecte a las redes, la seguridad de estas se deberá gestionar siguiendo lo indicado en las políticas y procedimientos respectivos.
* Se debe cautelar el uso seguro de los distintos perfiles de usuario, evitando que la contingencia afecte las reglas de acceso a los distintos sistemas de la Institución.

**c.- Lista de puntos clave a verificar como cumplimiento de la presente política**

* Determinar el alcance del plan
  + Analizar para que activos, procesos y actividades críticas se debe garantizar la continuidad.
* Concretar el flujo de responsabilidades
  + Determinar las responsabilidades de las personas que deben llevar a cabo el plan de continuidad en caso de aparición de desastres.
* Realización del BIA (Análisis del Impacto en el Negocio)
  + Elaborar detalladamente el BIA de la empresa.
* Definir la política de comunicación y aviso a entidades externas
  + Definir qué tipo de mensajes debe transmitir la empresa en caso de desastre.
* Caducidad del plan
  + Actualizar el plan de continuidad de negocio de la empresa cada año o una frecuencia distinta establecida por el [directorio o Gerencia General].
* Elegir la estrategia de continuidad
  + Elegir la estrategia de continuidad óptima para la empresa. Teniendo en cuenta si fuera preciso la implantación de un centro de respaldo.
* Detallar la respuesta a la contingencia
  + Detallar los procedimientos y controles específicos a ejecutar ante la aparición de un desastre.
* Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio
  + Probar y evaluar cada año o en un frecuencia distinta establecida por el [Directorio o Gerencia General] el plan de continuidad de negocio de la empresa.

**V.- GLOSARIO Y TÉRMINOS.**

Desastre: Evento catastrófico y repentino que anula la capacidad de la Subsecretaría del Interior o SGI para llevar a cabo sus procesos críticos. Un desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación o la incapacidad de los empleados para acceder a las instalaciones, generado por algún tipo de desastre natural, una contingencia sanitaria, una huelga, etc.