**POLITICA DE SEGURIDAD FISICA Y DEL AMBIENTE**

**I.- DEFINICIONES ESTRATÉGICAS**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento la Política de Seguridad Física y del Ambiente, en consistencia con los principios rectores de la Política General de Seguridad de la Información.

**a.- Objetivos**

Esta Política se orienta a definir medidas de protección para toda la infraestructura de la empresa ya sea tecnológica o no. Se tienen en consideración aquellas amenazas físicas y del ambiente que pueden afectar a las plataformas tecnológicas y las instalaciones en general, pero con foco en la seguridad de las personas y las instalaciones de procesamiento de la información, ya sea en los centros de procesamientos de datos (CPD) o en los equipos bajo la cobertura de los usuarios. Se mencionan como principales amenazas objetivo, sin que sea una lista exhaustiva, pero que ilustra el amplio espectro de situaciones a tener en consideración, a la siguiente: daño físico por acción del fuego, daño físico por acción del agua, daño físico por acción de la contaminación, daño físico por acción de incidente tangible importante, destrucción de equipamiento o medios, daño físico por acción del polvo, la corrosión o el congelamiento, daños por acciones terroristas o vandálicas, daños por acción de eventos naturales tales como: fenómenos climáticos, fenómenos sísmicos, fenómenos volcánicos, fenómenos meteorológicos, inundaciones. Para esto se aplica una estrategia de seguridad basada en las mejores prácticas y controles sobre estos recursos con el fin de protegerlos de accesos no autorizados, de daños a la integridad, de impactos relevantes en su disponibilidad, y finalmente garantizar su operación y seguridad. En específico, se busca:

* Velar por la protección de la Infraestructura tecnológica de almacenamiento de información y de provisión de servicios tecnológicos de apoyo a la gestión institucional.
* Protección de los espacios Físicos.
* Dar condiciones de continuidad operacional a la gestión institucional en el contexto del cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que están orientados hacia la seguridad de la información.

**b.- 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).

**c.- Roles y Responsabilidades**

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

**d.- 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.

**e.- 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.

**f.- 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.

**g.- 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.- SEGURIDAD FÍSICA Y DEL AMBIENTE**

La [Unidad TIC] realizará el mayor esfuerzo en implementar y garantizar la efectividad de los mecanismos de seguridad física y control de acceso para proteger de las amenazas prioritarias y más probables, en base a una evaluación y priorización de riesgos, el perímetro de seguridad de los centros de procesamiento de datos (Salas Técnicas y CPD/Datacenter).

La [Unidad de Administración y Finanzas o unidad responsable por las instalaciones físicas] velará por la seguridad física de las áreas restringidas, áreas de funcionamiento del personal, áreas de carga y descarga, y en general de las instalaciones (*facilities*) así como entornos abiertos. Del mismo modo, establecerá controles contra potenciales amenazas físicas externas e internas y las condiciones medioambientales de las instalaciones de la empresa.

Para estas laboras, en cuanto a tecnología y respaldo técnico, deberá recurrir en primera instancia a la asesoría de la [Unidad TIC], pudiendo recurrir a la asesoría externa solo si no están disponibles los recursos de apoyo internos.

La seguridad de instalaciones tendrá en cuenta los siguientes aspectos:

* Vías de acceso.
* Unidades de apoyo.
* Distribución interna.
* Sistema de prevención y extinción de incendios.
* Sistemas de vigilancia y control.
* Controles de acceso y perimetrales.
* Plan de emergencia.
* Seguridad externa/interna a las áreas de procesamiento y/o almacenamiento de información sensible, siempre que no se encuentre bajo la cobertura de la [Unidad TIC].
* Sistema abastecimiento continuo 7x24 de energía y combustibles.
* Continuidad operacional de los sistemas de climatización
* Sistema de estacionamientos y su monitoreo.
* Instalaciones en general (faclilities).
* Sistema de carga y descarga de productos.

Y los demás aspectos necesarios que garanticen el fortalecimiento de la seguridad física de las instalaciones.

**a.- Áreas Seguras**

La empresa, deberá asegurar que el personal interno/externo o contratado en modalidad de servicio u outsourcing y proveedores que tengan acceso a las instalaciones institucionales, entiendan sus responsabilidades, y que este personal se encuentre capacitado para desempeñar los roles y tareas para los cuales están siendo considerados; esperando con ello, reducir el riesgo de daño, hurto, fraude o mal uso de las instalaciones, equipamiento e información propiamente tales.

**b.- Seguridad de los equipos**

Los equipos computacionales y de redes, y sus respectivos cableados de interconexión y alimentación de energía, serán ubicados y protegidos para reducir la exposición a riesgos ocasionados por amenazas ambientales y oportunidades de acceso no autorizado.

* Los equipos de comunicaciones tales como: router, switch, servidor y otros, deberán estar agrupados en un solo lugar, denominados salas técnicas o Datacenter. Estos lugares deberán contar con controles de accesos físicos y ambientales, de modo que el acceso sea restringido.
* Los equipos computacionales se ubicarán de tal manera que se reduzca el riesgo de robos, daño físico y visualización de la información por personas no autorizadas, durante su uso.

**c.- Servicios de Suministro de Energía**

Los centros de procesamiento de datos y salas técnicas deben estar protegidos frente a posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía debe estar de acuerdo con las especificaciones del fabricante y norma técnica nacional respectiva.

Para asegurar la continuidad del suministro de energía en las condiciones requeridas para la protección del equipamiento, deberá disponerse de documento complementario “Requerimientos eléctricos para centro de procesamiento de datos y Salas Técnicas”, en el cual se entregarán las especificaciones técnicas vigentes y condiciones afectas a controles de cumplimiento de esta política y que se resumen a continuación.

* Documentar los sistemas eléctricos mediante planos que cumplan con las especificaciones de las normas que apliquen al respecto.
* Disponer de múltiples toma corrientes o líneas de suministro.
* Contar con un suministro redundante de energía ininterrumpida (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la institución. La determinación de dichas operaciones críticas será el resultado del análisis de riesgos realizado por la [Unidad TIC] en conjunto con los responsables de los procesos.
* Los planes de continuidad de negocio y recuperación de desastres contemplarán las acciones que han de emprenderse ante una falla de la UPS.
* Los equipos de UPS, dimensionados con la ayuda de la [Unidad TIC], serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida, de lo cual se dejará evidencia documental en el informe de mantención periódica. Asimismo, se verificará que los niveles de carga no superen los establecidos por las normas.
* La institución contará con grupos electrógenos, cuya potencia adecuada se determinará en conjunto con la [Unidad TIC], para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante una interrupción prolongada del procesamiento, con el objeto de definir qué componentes será necesario abastecer de energía alternativa. Dicho análisis será realizado por la [Unidad TIC] en conjunto con los responsables de los procesos.
* Se dispondrá de un adecuado suministro de combustible y mantenimiento para garantizar que el generador pueda funcionar por un período prolongado. Cuando el encendido de los generadores no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos. Los generadores serán inspeccionados y probados periódicamente para asegurar que funcionen según lo previsto, dejando la información documentada en el “Procedimiento de funcionamiento de grupo electrógeno”.
* Todas las instalaciones eléctricas estarán protegidas por sistemas de tierras de protección, que cumplan con los estándares vigentes para sistemas de comunicaciones.
* Todas las instalaciones eléctricas estarán protegidas contra fluctuaciones de voltaje por dispositivos adecuados.
* Las instalaciones eléctricas para los sistemas de comunicaciones deberán estar debidamente aisladas y protegidas contra eventos relacionados con humedad, filtraciones de agua y agentes químicos que lo puedan deteriorar o causar fallas.
* Se ubicarán los interruptores de emergencia cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.
* Se proveerá iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.
* Se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo con las normativas vigentes[[1]](#footnote-1).

**d.- Seguridad del Cableado**

Para el cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información para protegerlos contra intercepción o daño, se deberán cumplir las siguientes condiciones:

* Cumplir con los estándares ISO/IEC/11801, ANSI/EIA/TIA 568A o 568B o con la normativa vigente al respecto.
* Las instalaciones de cableado estructurado deberán protegerse contra la influencia o daño causado por agentes externos.
* Los elementos metálicos que forman parte de los cableados estructurados deberán conectarse al sistema de tierras del edificio.
* Los equipos deberán albergarse en sitios acondicionados a temperaturas entre 20 y 25 grados Celsius, según la norma TIA/EIA-942. Los objetivos primarios para tener en consideración al momento de establecer la temperatura de operación en los centros de procesamiento de datos son: Seguridad de las personas, seguridad de los equipos y minimización del uso de energía (costo).
* Los centros de cableado deberán contar con un Rack para alojar los equipos y terminaciones de los cableados, asegurados con chapas o cerraduras de seguridad, cumpliendo las normas técnicas y cuyas llaves serán administradas por personal de Operaciones de la [Unidad TIC].
* Las instalaciones deberán realizarse siguiendo la arquitectura de los edificios, debidamente protegidos con canaleta en caso de instalación interior, o con tubo galvanizado y/o metálico en caso de instalación a la intemperie.
* Toda instalación de dispositivos adicionales deberá ser visados por la [Unidad TIC] previamente.

**e.- Mantenimiento de los Equipos**

Dado que contar con los adecuados servicios de mantenimiento a la plataforma tecnológica posibilita su disponibilidad e integridad, se deberán considerar las siguientes condiciones:

* Realización de mantenimiento preventivo a los equipos de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante.
* Llevar registro detallado de los mantenimientos contratados (preventivos y correctivos), condiciones y puntos de contacto; detalle de garantías; suministro de nuevos accesorios; custodia de partes y piezas en mantenimiento; fallas, movimientos, entre otros. Esta actividad es de cargo del responsable técnico que se designe para cada caso.
* Controlar acceso a los equipos, sólo al personal autorizado y debidamente identificado, para realizar tanto mantenimiento como reparaciones en los equipos.
* Eliminación de manera segura de la información de la empresa que contenga cualquier equipo que sea necesario retirar, realizándose previamente las respectivas copias de respaldo.
* En las especificaciones técnicas para los contratos de mantenimiento o garantía se contemplará el suministro de nuevos discos manteniendo la custodia del disco duro dañado.
* El responsable funcional del equipo acompañará el mantenimiento de los equipos que contengan información sensible.

**f.- Seguridad de los equipos fuera de las instalaciones**

El uso de equipos de computación, fuera de las instalaciones, estará restringido a equipos portátiles y móviles, y su uso estará regulado por el “Formulario de asignación de computador portátil”. Cualquier otro equipamiento no portátil que requiera estar fuera de las instalaciones, deberá contar con la autorización del jefe de la división dueña del proceso afectado y de la [Unidad TIC]. La seguridad para estos equipos será equivalente a la suministrada dentro de las instalaciones sumando controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso de éstos fuera de las instalaciones, por tanto:

* Los equipos móviles institucionales, no podrán conectarse a redes inalámbricas públicas o no conocidas.
* El software instalado en los dispositivos móviles deberá estar totalmente licenciado y avalado por la [Unidad TIC].
* El acceso a los equipos móviles deberá realizarse mediante el uso de usuario y contraseña.

**g.- Destrucción o reutilización segura de equipos**

El borrado seguro y destrucción de dispositivos de almacenamiento, estará regulado por el “Procedimiento de destrucción y reutilización segura de equipos” que define la [Unidad TIC]. Este procedimiento deberá garantizar la mayor dificultad técnica para la recuperación de la información por parte de terceras partes no autorizadas, proponiendo al menos dos niveles de borrado seguro: uno orientado a equipos con información pública o normal, denominado “borrado seguro normal” y uno denominado “borrado seguro crítico”, para equipamiento que albergue información Confidencial o Interna, siendo este último nivel el más alto en la escala, el cual podrá contemplar incluso la remoción y destrucción física del o los componentes que contienen la información.

Antes de la reutilización o devolución de cualquier equipo de computación, se deberá realizar borrado seguro de la información, nivel “borrado seguro normal”, o la remoción del o los componentes de almacenamiento, o la destrucción física del dispositivo del o los componentes de almacenamiento.

A todo equipamiento que vaya a ser reutilizado y que haya contenido información Confidencial o Interna se le deberá aplicar obligatoriamente el “Procedimiento de destrucción y reutilización segura de equipos” para el nivel “borrado seguro crítico”.

**h.- Recomendación de buenas prácticas para escritorio limpio y seguro**

A continuación, se establecen pautas de trabajo que corresponden a buenas prácticas para reducir los riesgos de acceso no autorizado, pérdida y daño de la información que se almacena y procesa en las estaciones de trabajo de la empresa (escritorio físico y equipos computacionales):

* Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones y/u otro tipo de archivo seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
* Guardar bajo llave la información reservada (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso.
* Bloquear la sesión de los computadores personales cuando no se está usando.
* Después de cinco (5) minutos de inactividad, el protector de pantalla se deberá activar en forma automática.
* Retirar inmediatamente de la gaveta de la fotocopiadora o impresora la información Confidencial o Interna, una vez fotocopiada, escaneada impresa.

**i.- Retiro de bienes de las instalaciones**

Todo retiro de los equipos de la empresa, software e información desde las instalaciones, deberá estar documentado a través de una “Orden de Salida y Autorización de retiro de Equipamiento” para tal fin, lo que será de responsabilidad del jefe responsable del Área y enviado a la [Unidad TIC], la que mantendrá la custodia de la documentación de control de las salidas de equipamiento que le son enviadas. Además, se deberá dar aviso de reingreso a las instalaciones.

En caso del retiro permanente de las instalaciones, se deberán dar los avisos correspondientes a los encargados del Inventario, [División de Administración y Finanzas u otra unidad responsable por los activos de la empresa] en caso de los bienes muebles, inmuebles, y fungibles de la empresa, y para el caso de bienes tecnológicos se deberá incluir en la notificación a la [Unidad TIC] o [Unidades de Administración y Finanzas]. Los responsables del Inventario deberán realizar verificaciones periódicas, para detectar el posible retiro no autorizado de activos.

1. https://www.sec.cl/ [↑](#footnote-ref-1)