**POLÍTICA DE SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**

**I.- DEFINICIONES ESTRATÉGICAS**

Es frecuente escuchar que «el eslabón más importante de la seguridad es el empleado», ya que evitar el error humano es clave para proteger los sistemas y la información de la empresa. Por ello es importante, además de realizar la oportuna concienciación y formación para fortalecer este eslabón, tomar medidas de seguridad en la gestión de los llamados «recursos humanos».

Una buena manera de garantizar que se va a contar con un equipo de trabajadores responsables en materia de ciberseguridad es establecer los oportunos filtros, pruebas y controles en la relación con los colaboradores y empleados, especialmente en las fases de firma y finalización del contrato. En ambas fases se tendrán en cuenta aspectos tales como:

* qué requisitos y acuerdos relativos a la seguridad deben conocer, aceptar y cumplir;
* qué políticas internas deben aplicar: uso del correo corporativo, clasificación de la información, aplicaciones permitidas, uso del puesto de trabajo, etc.;
* qué formación se les va a proporcionar;
* cuáles son los procesos para darles de alta/baja en los sistemas empresariales, etc

**a.- Objetivos**

* Asegurar que todo el personal tiene conocimiento sobre los derechos, deberes y responsabilidades en relación a la seguridad de la información, haciendo hincapié en las posibles sanciones ante un acto negligente que ponga en riesgo los activos de información de la organización.
* Administrar la Política de seguridad de la información dentro de la empresa, y establecer un marco general para iniciar y controlar su adecuada implementación, así como la determinación y asignación de funciones y responsabilidades.
* Asegurar el cumplimiento de los requisitos normativos, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en la empresa.
* Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.
* Implementar una metodología enfocada en la gestión del riesgo.
* Apoyar al modelo de continuidad de negocio.

**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.- CIBERSEGURIDAD EN LA GESTIÓN DEL PERSONAL**

Comprende todas las medidas adoptadas por la empresa para asegurar el cumplimiento de las leyes, reglamentos y políticas que regulan el acceso a la información aplicable en situaciones de contratación, desvinculación o cambio de la relación laboral por parte de 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

**a.- Previo al a la Contratación**

La empresa deberá asegurar que los trabajadores y personal en modalidad de servicio u outsourcing, 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 mal uso de la infraestructura tecnológica y de la información.

**Roles y Responsabilidades del Personal**

Los roles y responsabilidades del personal, respecto de la seguridad de la información, deberá formalizarse clara y específicamente en los respectivos contratos de trabajo y/o prestación de servicios.

**Selección del Personal**

El [Departamento de Desarrollo y Gestión de Personas], en su proceso de reclutamiento y selección, deberá efectuar las verificaciones necesarias para confirmar la veracidad de la información suministrada por las personas que se postulan como candidatos a ingresar a la empresa, en proporción a los requisitos del cargo, la clasificación de la información a ser accedida y a los riesgos percibidos.

**Términos y Condiciones Laborales**

El [Departamento de Desarrollo y Gestión de Personas], se encargará que todo el personal vinculado con la Institución, firme un acta de aceptación de las Políticas de Seguridad de la Información en la empresa; documento que será un anexo del contrato y formará parte de su hoja de vida. El personal externo firmará los acuerdos de confidencialidad para terceros y los documentos de cumplimiento de las Políticas de Seguridad de la Información, siendo esto parte integral del contrato o acuerdo de cooperación.

**b.- En el ejercicio del Cargo o Función**

El [Comité de Riesgos y Seguridad de la Información], por medio del [Departamento de Desarrollo y Gestión de Personas] y con el apoyo técnico de la [Unidad TIC] deberá capacitar, difundir, promover, concientizar al personal interno, contratistas y usuarios externos sobre las amenazas y las preocupaciones de la seguridad de la información, de sus responsabilidades y obligaciones, y asegurar su preparación para apoyar la Política de Seguridad en la Institución a través de concientización, educación y formación en Seguridad de la Información.

El [Comité de Riesgos y Seguridad de la Información], por medio del [Departamento de Desarrollo y Gestión de Personas] y con el apoyo técnico de la [Unidad TIC], en su interés por garantizar que el personal interno, cuente con el nivel deseado de los conocimientos de seguridad de la información y las buenas prácticas de uso y resguardo de los activos de información: diseñará un programa de capacitación y concientización en seguridad de la información para promover la protección, uso y procesamiento de la información.

Esta capacitación deberá ser implementada y coordinada por el [Departamento de Desarrollo y Gestión de Personas], con el apoyo técnico de la [Unidad TIC].

Será de obligación de todo el personal interno o externo de la empresa, que por sus funciones hagan uso de recursos tecnológicos, el participar de los entrenamientos y charlas que se programen en temas relacionados con la seguridad de la información y aplicar las recomendaciones allí impartidas en sus labores diarias.

El incumplimiento de las obligaciones contenidos en el presente documento acarreará las responsabilidades y sanciones propias de una infracción a las políticas de seguridad de la información, y en los casos más graves las que establezcan las leyes administrativas, civiles y penales, según el caso.

**Finalización o Cambio de la Relación Laboral o Empleo**

El [Departamento de Desarrollo y Gestión de Personas] deberá gestionar la desvinculación de funcionarios o personal interno o externo, debidamente coordinado con la [Unidad TIC], para efecto de asegurar la protección, reserva y/o entrega de los activos de información que hubiesen estado a su cargo. Se debe procurar que esta coordinación sea automatizada y en tiempo real.

**Responsabilidad en la desvinculación**

El [Departamento de Desarrollo y Gestión de Personas] deberá mantener el registro actualizado del estado laboral y permanencia de todo el personal interno y externo de la empresa, comunicando de forma inmediata a la [Unidad TIC] cuando el personal se encuentre temporal (por más de 30 días) o definitivamente fuera de sus labores. Se debe procurar que esta coordinación sea automatizada y en tiempo real.

El [departamento o unidad] que mantenga personal externo bajo su supervisión deberá informar de manera inmediata a la [Unidad TIC], el inicio de las labores que se han contratado y la terminación del contrato cuando corresponda, con el objetivo de conocer y autorizar el acceso y disponibilidad los recursos tecnológicos, así como, de la remoción de los permisos sobre los activos de información en general.

Al momento de la desvinculación del personal interno o externo, la jefatura directa deberá encargarse de que el puesto y los activos de información, sean íntegra y formalmente entregados por el personal desvinculado, solicitando la aprobación al [Departamento de Desarrollo y Gestión de Personas] y la [Unidad TIC].

**c.- Lista de puntos para verificar**

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a la **gestión de recursos humanos**.

Los controles podrán tener el siguiente **alcance**:

* Procesos (**PRO**): aplica a la dirección o al personal de gestión.
* Tecnología (**TEC**): aplica al personal técnico especializado.
* Personas (**PER**): aplica a todo el personal.

| **ALCANCE** | **CONTROL** |
| --- | --- |
| PRO | **Cláusulas contractuales**  Reflejar en los contratos laborales de sus empleados los aspectos más importantes en materia de ciberseguridad. |
| PRO | **Acuerdos de confidencialidad**  Concretar en acuerdos de confidencialidad la manera de gestionar el acceso a la información más sensible. |
| PRO | **Revisar las referencias de los candidatos**  Revisar las referencias de los candidatos antes de su contratación en aquellos puestos que requieren acceso a información muy confidencial. |
| PRO | **Plan de formación y concienciación en ciberseguridad**  Mantener concienciado y formado a todo el personal en aspectos relacionados con la ciberseguridad. |
| PRO | **Política de sanciones y expedientes**  Informar a su personal de las sanciones que conlleva el uso negligente de la información de la empresa. |
| PRO | **Finalización del contrato**  Comunicar al personal las obligaciones que deben cumplir con la información de la empresa al finalizar el contrato. |
| TEC | **Concesión autorizada de los permisos de acceso**  Conceder los permisos oportunos para garantizar que cada empleado solo accede a la información conveniente. |
| TEC | **Revocación de permisos de acceso**  Eliminar los permisos y cuentas de usuario del personal que finalizan su contrato. |
| PER | **Aceptación de las cláusulas y políticas de seguridad de la información**  Leer, entender y firmar los acuerdos, cláusulas y políticas relacionados con la seguridad de la información. |
| PER | **Aprovechamiento de las sesiones formativas y de concienciación**  Participar de manera activa en las sesiones formativas de la empresa en materia de ciberseguridad. |

**d.- Puntos clave**

Los puntos clave de esta política son:

* **Cláusulas contractuales.** El empresario, con el [Departamento de Desarrollo y Gestión de Personas], establecerán qué aspectos relevantes en relación con la seguridad de la información deben ser reflejados en el contrato de trabajo. Se considerarán todas las responsabilidades y derechos legales en lo relacionado con la propiedad intelectual o con datos de carácter personal (Ley N°19.628 o la que la reemplazare).
* **Acuerdos de confidencialidad.** Los empleados y colaboradores firmarán acuerdos relativos a la confidencialidad de la información de la empresa, que contendrán la siguiente información:
  + partes intervinientes;
  + qué información tendrá carácter confidencial;
  + compromisos por ambas partes;
  + posibles sanciones y legislación aplicable.
* **Revisar las referencias de los candidatos.** En ciertas ocasiones (sobre todo para puestos de especial criticidad o con acceso a información muy confidencial) se deberán detallar las comprobaciones a realizar antes de incorporar a algún candidato a la empresa. Será necesario determinar las referencias que han de ser revisadas y qué datos del currículum tienen que verificarse. Además, se indicarán qué puestos concretos necesitarán una acreditación especial de estar libre de antecedentes penales.
* **Plan de formación y concienciación en ciberseguridad.** Se establecerán las actividades oportunas para mantener al personal concienciado y formado en todo momento en aspectos relativos a la seguridad de la información.
* **Política de sanciones y expedientes.** Se deberá elaborar un procedimiento disciplinario formal que recoja las sanciones a aplicar en aquellos casos en los que se haya producido una negligencia en relación con la seguridad de la información (fuga o pérdida de datos confidenciales o sensibles, actuaciones intencionadas, ataques a la reputación en redes sociales, permitir ataques de terceros como infecciones por malware, etc.). Este procedimiento deberá ser notificado al personal y estar accesible en todo momento.
* **Finalización del contrato.** Para evitar fugas de información es importante comunicar al personal las responsabilidades y obligaciones de seguridad y confidencialidad que deberán cumplir una vez finalizada la relación contractual.
* **Concesión autorizada de los permisos de acceso.** Se deberá garantizar que cada empleado solo acceda a la información oportuna, para lo que se deberá darle de alta en los sistemas de acuerdo con las políticas de control de acceso (físico y lógico) correspondiente. En este punto, entre otras, se deberán realizar las siguientes acciones:
  + entregar las tarjetas de acceso físico;
  + asignar las cuentas de correo electrónico;
  + conceder los permisos de acceso a servicios, aplicativos y recursos compartidos;
  + asignar el puesto de trabajo, los dispositivos y equipos.
* **Revocación de permisos de acceso**. Del mismo modo que en su incorporación se dan los accesos y permisos oportunos a los nuevos empleados para que puedan realizar su trabajo, al finalizar la relación contractual se deberán revocar:
  + recogiendo las tarjetas de acceso y los dispositivos entregados;
  + eliminando sus cuentas de correo;
  + eliminando sus permisos de acceso a sistemas y aplicativos;
  + recuperando los activos asignados.
* **Aceptación de las cláusulas y políticas de seguridad de la información.** El personal de la empresa deberá asegurarse de leer, comprender y firmar cada uno de los acuerdos, contratos, cláusulas y documentos de políticas relacionados con la seguridad de la información.
* **Aprovechamiento de las sesiones formativas y de concienciación**. Se procurarán las facilidades para que el personal aproveche al máximo las sesiones formativas y de concienciación que la empresa ponga a disposición de ellos. De esta forma la empresa se asegura que el personal comprende los riesgos a los que se enfrenta la empresa en materia de ciberseguridad.

**III.- GLOSARIO DE TÉRMINOS**

**Definiciones.**

Para los propósitos de esta Política, se entenderá por:

Acceso a la información: Es el derecho que tiene toda persona de buscar, recibir y difundir información.

Activos de información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo, dispositivos móviles, tarjetas de accesos, software, equipamiento computacional.

Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado un sistema u organización. Ejemplos: terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.

Confidencialidad: La información debe estar protegida de accesos no autorizados, por lo tanto, se debe asegurar que la información es accedida únicamente por las personas autorizadas.

Derechos de accesos: Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recurso.

Disponibilidad: Es la certeza de que sólo los usuarios autorizados tienen acceso a la información y a los activos asociados cuando es requerido.

Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Documento público : Documentos que no son confidenciales y cuyo conocimiento no está circunscrito a un grupo acotado y definido de destinatarios.

Documento confidencial: Aquel documento cuyo conocimiento está circunscrito a un ámbito reducido y cuya divulgación o uso no autorizados contraviene la legislación vigente.

Estación de Trabajo : Equipo computacional conectado a una red de computadores que facilita a los usuarios el acceso a los servidores y periféricos de la red.

Evaluación del riesgo: Comparar los niveles de riesgo encontrados contra los criterios de riesgo prestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.

Gestión del riesgo: Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización. Es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.

Incidente de Seguridad: Se define incidente como cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y confidencialidad de la información, junto con la plataforma tecnológica, proceso y aplicativos que permitan acceder a ésta en forma oportuna. En general, es una violación de una política, estándar o procedimiento de seguridad, que no permite prestar un servicio computacional. Como ejemplos de incidentes de seguridad podemos enumerar: Acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio.

Integridad: La información debe estar completa, actualizada y ser veraz, sin modificaciones o alteraciones no autorizadas o corruptas.

Medios de procesamiento de información: Dispositivos internos y/o externos que tengan la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario. Como ejemplos de medios de procesamiento de información, podemos señalar a: servidores de aplicaciones, servidores de correo, de impresión, aplicaciones web, servidores de almacenamientos, computadores personales, discos duros externos, pendrives y teléfonos móviles.

Política de Seguridad: Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.

Programa malicioso : Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.

Restringir el acceso: Delimitar el acceso de los funcionarios, servidores públicos a honorarios y terceras partes a determinados recursos.

Riesgo: Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.

Sanción: Puede ser definida como consecuencia administrativa, civil, jurídica o penal por el incumplimiento del deber que produce en relación con el obligado.

Seguridad de la Información: Proceso encargado de asegurar y proteger los recursos de un sistema de información para que sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.

Sistema informático: Software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.

Terceras partes: Persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión. Para este procedimiento, se entenderá como terceras partes a: Proveedores de servicios y de red, proveedores de productos de software y servicios de información, outsourcing de instalaciones y operaciones, servicios de asesoría de seguridad y auditores externos.

Usuario: Persona que utiliza el sistema informático de la empresa, independientemente de la calidad contractual.