**POLÍTICA DE ADMINISTRACIÓN DE ACTIVOS DE INFORMACIÓN, EQUIPAMIENTO Y PLATAFORMA DE SERVICIOS INFORMÁTICOS PARA USUARIOS**

**I.- DEFINICIONES ESTRATÉGICAS**

**a.- Objetivo general**

La [Empresa XXX], a través de su Comité de Riesgos y Seguridad de la Información, presenta en este documento la Política para la administración de los activos de Información, uso del equipamiento institucional y servicios computacionales provistos a través de la plataforma tecnológica de apoyo al cumplimiento de la gestión, en consistencia con los principios rectores de la política general de seguridad de la información.

**b.- Definición de los Activos**

Debe entenderse que los Activos de información, son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Empresa, cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten, tales como: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional, entre otros.

**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.- RESPONSABILIDAD SOBRE LOS ACTIVOS**

La información que se produce, procesa, transmite, almacena y los medios físicos utilizados la Empresa y sus empleados según lo especificado en el alcance del presente documento, es de propiedad de la empresa y su custodia y protección será de responsabilidad del dueño del proceso que se vincule con dicha información. Con relación a los datos contenidos en medios administrados por la **[unidad TIC o equivalente]**, esta unidad estará a su cargo y resguardo. Sin embargo, los accesos y usabilidad de la información, en las Unidades usuarias, son de responsabilidad de los dueños de los procesos y trabajadores que la acceden, los que deberán quedar formalmente establecidos en documentos de control de proyectos.

**a.- Inventario de activos**

Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados por cada Unidad a cargo y se debe mantener un inventario de dichos activos.

La información y campos que debe contener este inventario son:

* Código (Id) del activo: en el caso de ser un activo inventariable, identificar el código asignado por el departamento de Administración.
* Nombre del activo: Nombre operativo o comercial del activo.
* Tipo de activo: clasificación del activo, los utilizados son: software, sistema, equipos, documento, infraestructura, formulario, base de datos, y otros.
* Ubicación: identificación del lugar físico que aloja al activo o lógico, en caso de ser un software, sistema y/o base de datos.
* Fecha de creación: Fecha con el cual el activo fue creado o recibido.
* Definición de propietario.

El inventario debe estar automatizado y disponible en tiempo real para ser auditado por terceras partes interna o externas debidamente autorizadas.

Deberán emitirse informes mensuales que den cuenta del estado de los inventarios de los activos tecnológicos, que den cuenta de las existencias, corroborar sus parámetros certificando su asignación y su efectiva existencia en bodega.

**c.- Procesos sobre los activos de información**

Como parte del registro de los activos, deberán realizarse las siguientes actividades:

* Mantener un inventario de activos de la información, a cargo de cada Unidad responsable.
* Realizar un análisis de riesgos de los activos de información como mínimo una vez al año.
* Clasificar los activos de información en función de su importancia.
* Tomar decisiones y acciones para mitigar, transferir o aceptar los riesgos.
* Verificar anualmente o cada vez que lo amerite, el inventario de los activos de información bajo su responsabilidad, con el fin de mantener actualizados los registros.
* Revisar anualmente la clasificación de sus activos y reclasificarlos de ser necesario.
* Almacenar, manejar y custodiar los activos de información de acuerdo con su nivel de clasificación.
* Definir los criterios de eliminación de activos de información que se constituyan como obsoletos o sean respaldos sin utilidad.

Para el caso de los documentos electrónicos se deberá tener en consideración las siguientes fases:

* Fase Activa, que se refiere a la producción y gestión del documento electrónico en cada empresa pública, así como su utilización para los fines pertinentes
* Fase Semiactiva, que corresponde a la conservación temporal del documento al interior de cada empresa pública dependiendo del período de vigencia de cada expediente o documento
* Fase Histórica, que aplica a aquellos documentos que, de acuerdo con la normativa vigente y a su proceso de valoración, deben ser transferidos al Archivo correspondiente, para su preservación y disponibilización.

**d.- Uso aceptable de los activos de información**

Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información. En particular:

* Definir los sistemas que usarán la información.
* Indicar donde se encuentra almacenada la información institucional.
* Definir la información que tendrá carácter de intercambiable e interoperables con otras empresas u organismos.
* Adscribir las normas sobre datos personales y privacidad que la legislación vigente disponga.

**e.- Devolución de activos**

Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo. Lo que deberá estar registrado en Acta de Entrega/Devolución.

La responsabilidad de supervisión del debido cumplimiento de esta actividad recae en la respectiva Jefatura del usuario o de la División, Departamento, Sección o Unidad respecto de terceras partes cuya relación laboral ha finalizado.

**f.- Clasificación de los Activos de información**

La **información** es uno de los activos principales de cualquier empresa y como tal tenemos que protegerla adecuadamente.

Los activos de información pueden estar en formato digital o en otros soportes (papel, película fotográfica, etc.). En formato digital podrán ser desde documentos de todo tipo (texto, imagen, multimedia, bases de datos, entre otros), pasando por los programas y aplicativos que los utilizan y gestionan, hasta los equipos y sistemas que soportan estos servicios.

Para aplicar las medidas de seguridad ajustadas a cada activo de información se debe realizar un inventario y clasificarlos, de acuerdo con el impacto que ocasionaría su pérdida, difusión, acceso no autorizado, destrucción o alteración, aplicando para ello criterios de confidencialidad, integridad y disponibilidad. Así sabremos qué información debemos cifrar, quién puede utilizarla, quién es responsable de su seguridad, cada cuanto hacer *backup*, etc.

Estos son algunos ejemplos:

* el aplicativo de nóminas es confidencial y sólo tendrán acceso a él ciertos empleados del departamento de personal para los cuales habilitaremos permisos;
* el acceso al gestor de la página web está restringido al personal de marketing;
* se han de cifrar los documentos que se envíen a la gestoría por correo electrónico;
* los servicios que traten datos personales tendrán que cumplir la ley de datos personales y relacionadas;
* el ERP es crítico para la empresa y se debe hacer *backup* semanalmente.

Además, al clasificar los activos de información debemos establecer su **ciclo de vida**, que dependerá no sólo de la vida útil del soporte sino también de la vigencia de su contenido. Si el soporte actual caduca antes que el contenido tendremos que regenerarlo en otro soporte. El ciclo de vida de la información determinará el momento en el cual dejará de ser útil, y por tanto cuándo tenemos que eliminarla convenientemente.

**Confidencialidad:**

La información, independientemente de si su soporte es físico o lógico, debe ser protegida de la divulgación no y clasificada en 3 categorías al menos:

* Público
* Reservado
* Confidencial

Asimismo, se realizará una ponderación en el inventario de activos, con el objetivo de priorizar el tipo de acceso a la información, criticidad y protección.

Niveles de confidencialidad:

Valor: 1.

* Clasificación: Pública.
* Criterio: Información que puede ser conocida y utilizada por cualquier trabajador/a de la empresa, usuario/a, beneficiario/a y otros organismos. Si bien se considera información pública, el acceso a ésta nunca puede ser por medio de la vulneración de sitios o sistemas web o de plataformas tecnológicas institucionales internas o de bases de datos, considerándose esta acción un delito. Para esta última instancia se aplicarán las notificaciones pertinentes como una infracción a las políticas de seguridad de la información, del estatuto administrativo y se podrán ejercer las sanciones que estos cuerpos normativos dispongan sin perjuicio de seguir las acciones penales pertinentes.

Valor: 2.

* Clasificación: Interna.
* Criterio: Información que sólo puede ser conocida y utilizada por un grupo reducido de trabajador/as y cuya divulgación o uso no autorizado contraviene la legislación vigente. El acceso a ésta en ningún caso puede ser por medio de la vulneración de sitios o sistemas web o de plataformas tecnológicas institucionales internas o de bases de datos, considerándose esta acción un delito. Para esta última instancia se aplicarán las notificaciones pertinentes como una infracción a las políticas de seguridad de la información, del estatuto administrativo y se podrán ejercer las sanciones que estos cuerpos normativos dispongan sin perjuicio de seguir las acciones penales pertinentes.

Valor: 3.

* Clasificación: Confidencial.
* Criterio: Información que será conocida sólo por las autoridades o personas a las cuales vayan dirigidos y por quienes deban intervenir en su estudio o resolución. El acceso a ésta en ningún caso puede ser por medio de la vulneración de sitios o sistemas web o de plataformas tecnológicas institucionales internas o de bases de datos, considerándose esta acción un delito. Para esta última instancia se aplicarán las notificaciones pertinentes como una infracción grave de las políticas de seguridad de la información, del estatuto administrativo y se podrán ejercer las sanciones que estos cuerpos normativos dispongan sin perjuicio de seguir las acciones penales pertinentes, pudiendo invocarse agravantes que involucran a la Seguridad Nacional.

**Integridad:**

La información debe ser protegida de cambios o destrucción no autorizados. Cualquier acción interna o externa ya sea tentativa o que efectivamente logre afectar la integridad de la información institucional, será considerada un delito. Para esta última instancia se aplicarán las notificaciones pertinentes como una infracción grave de las políticas de seguridad de la información, del estatuto administrativo y se podrán ejercer las sanciones que estos cuerpos normativos dispongan sin perjuicio de seguir las acciones penales pertinentes, pudiendo invocarse agravantes que involucran a la Seguridad Nacional según la información que haya sido afectada.

Valor: 1.

* Criticidad: Baja.
* Criterio: Información cuya modificación no autorizada puede corregirse, aunque podría ocasionar riesgos leves para la empresa o terceros.

Valor: 2.

* Criticidad: Media.
* Criterio: Información cuya modificación no autorizada es de difícil corrección y podría ocasionar riesgos significativos para la empresa o terceros.

Valor: 3.

* Criticidad: Alta.
* Criterio: Información cuya modificación no autorizada no podría corregirse, ocasionando graves consecuencias a la empresa o terceros.

**Disponibilidad**

La información debe estar disponible para los usuarios autorizados. Cualquier acción interna o externa ya sea tentativa o que efectivamente logre afectar la disponibilidad de la información institucional, será considerada un delito. Para esta última instancia se aplicarán las notificaciones pertinentes como una infracción grave de las políticas de seguridad de la información, del estatuto administrativo y se podrán ejercer las sanciones que estos cuerpos normativos dispongan sin perjuicio de seguir las acciones penales pertinentes, pudiendo invocarse agravantes que involucran a la Seguridad Nacional según la información que haya sido afectada.

Valor: 1.

* Criticidad: Baja.
* Criterio: Información cuya inaccesibilidad permanente, durante una semana, podría ocasionar consecuencias significativas para la empresa o terceros.

Valor: 2.

* Criticidad: Media.
* Criterio: Información cuya inaccesibilidad permanente, durante un día, podría ocasionar consecuencias significativas al organismo, al sector público nacional o terceros

Valor: 3.

* Criticidad: Alta.
* Criterio: Información cuya inaccesibilidad permanente, durante una hora, podría ocasionar consecuencias significativas para la empresa o terceros.

Todos los documentos físicos o digitales expedidos por la empresa, deberán estar etiquetados o rotulados, según el levantamiento del inventario de los activos de la información y de acuerdo con el esquema de clasificación definido en el punto Clasificación de la información, según su confidencialidad: público, reservado o Confidencial.

En el caso de los documentos electrónicos, deberán tener una etiqueta con la leyenda según su clasificación.

**g.- Actualización del Inventario de los activos de la información**

Se debe mantener actualizado el inventario de los activos de información, lo cual implica desarrollar o implementar los procedimientos para el manejo de activos. Este inventario indicará quién es el responsable administrativo del activo, el cual deberá velar por su seguridad; y deberá mantener o implementar las medidas de seguridad.

Se deberá registrar quienes tienen acceso a este activo, los niveles de privilegios asignados, su ubicación física o lógica y qué niveles de respaldo y duplicidad existen en caso de daño o pérdida asociado a planes de contingencia, en caso de ser necesaria la continuidad del negocio.

h.- Lista de verificación:

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

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 | **Inventario de la información**Elaborar un inventario detallado de los activos de información de su empresa. |
| PRO | **Criterios de clasificación de la información**Determinar claramente los criterios de seguridad con los que clasificará los activos de información de su empresa. |
| PRO  | **Clasificación de la información**Etiquetar los activos de información según los criterios de seguridad establecidos. |
| PRO | **Tratamientos de seguridad disponibles**Establecer una lista con todos los tratamientos de seguridad de la información disponibles en su empresa. |
| TEC | **Establecer y aplicar los tratamientos que corresponden a cada tipo de información** Aplicar correctamente los tratamientos de seguridad que corresponden a cada activo información. |
| TEC | **Auditorías**Realizar auditorías de comprobación cada ­­\_\_\_\_[frecuencia]\_\_\_\_\_\_.  |

i.- puntos relevantes en el despliegue de los aspectos de clasificación de activos de información que no pueden obviarse:

Los puntos clave son:

* **Inventario de la información.** Es necesario establecer un inventario de los activos de información disponible en la empresa, considerando registrar aspectos tales como su tamaño, ubicación, servicios o departamentos a los que pertenecen, quienes son sus responsables, etc.
* **Criterios de clasificación de la información.** Se Deben establecer claramente los criterios de clasificación que se van a aplicar a los activos de información. Estos deberán estar relacionados con las medidas de seguridad que plantea aplicar a su información. Algunos de estos criterios podrían ser:
	+ por el nivel de accesibilidad o confidencialidad:
		- Confidencial. Accesible solo por la dirección o personal concreto.
		- Interna. Accesible solo al personal de la empresa.
		- Pública. Accesible públicamente.
	+ por su utilidad o funcionalidad:
		- información de clientes y proveedores.
		- información de compras y ventas.
		- información de personal y gestión interna.
		- información sobre pedidos y procesos de almacén.
	+ por el impacto por robo, borrado o pérdida:
		- daño de imagen.
		- consecuencias legales.
		- consecuencias económicas.
		- paralización de la actividad.
* **Clasificación de la información.** Asignar a cada tipo de información una etiqueta según los criterios de clasificación establecidos.
* **Tratamientos de seguridad disponibles.** Elaborar un listado con todos los tratamientos de seguridad de los que dispone la empresa, tales como herramientas de cifrado, sistemas de copias de seguridad, sistemas de control de accesos, etc.
* **Establecer y aplicar los tratamientos que corresponden a cada tipo de información.** Una vez clasificada la información, se debe asignar y aplicar los tratamientos de seguridad oportunos para cada tipo de información. Entre estos tratamientos, podríamos contemplar los siguientes:
	+ limitar el acceso a las personas o grupos correspondientes
	+ cifrar la información.
	+ realizar copias de seguridad.
	+ medidas específicas como las exigidas por la ley de datos personales.
	+ información sujeta a acuerdos de confidencialidad concretos.
	+ control del acceso y/o modificación de la información.
* **Auditorías**. Realizar periódicamente auditorías de seguridad que certifiquen que se están aplicando los tratamientos estipulados para proteger su información.

**III.- USO DEL EQUIPAMIENTO INSTITUCIONAL Y SERVICIOS**

A continuación, se presentan el uso y cuidado del equipamiento computacional de la empresa, los cuales son asignados a cada uno de los trabajadores para cumplimiento de sus funciones.

**a.- Condiciones Ambientales**

Se deberá resguardar todo equipamiento para evitar daños producidos por disturbios, descuidos u otros daños causados por trabajadores, terceras partes, terrorismo, explosiones, actos maliciosos, sismo, y otros riesgos de la naturaleza o bien accesos a éstos por parte de otras personas no autorizadas, lo que será de responsabilidad del trabajador al que le son asignados. La empresa es responsable de proveer a sus trabajadores todos los medios necesarios para el debido resguardo de todo el equipamiento.

En caso de daños, robos o accesos no autorizados, el trabajador a cargo de éstos deberá dar aviso oportuno al Departamento de Soporte de Informático, a la instancia Jurídica que le corresponda y la Jefatura respectiva. En particular, el Departamento de Soporte Informático aplicará las medidas de resguardo de la plataforma y datos según sea el nivel de riesgo involucrado, el que depende del perfil del trabajador, de sus accesos a los sistemas y las bases de datos institucionales.

**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 asignación deberá estar registrada en Acta de Asignación. La seguridad para estos equipos será equivalente a la suministrada dentro de las instalaciones con controles adicionales, para mitigar los riesgos que por sí mismo conlleva el uso de éstos bajo ambientes no controlados, 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 el Departamento de Informática.
* El acceso a los equipos móviles deberá realizarse mediante el uso de usuario y contraseña.
* Periódicamente deberá conectarse a la red institucional para actualización de seguridad.
* Los equipos portátiles deberán contar con tecnología que permita encontrar los equipos en caso de robo o pérdida.
* Los equipos portátiles deberán contar con tecnología de encriptación de la información sensible, según el perfil del usuario y el nivel de confidencialidad de la información que almacena, que impida el acceso no autorizado interno o de terceras partes ante pérdida o robo. En primera instancia de no mediar algún estándar que reglamente este punto se utilizará como criterio general, que usarán la tecnología de protección de alto nivel (encriptado) aquellos equipos que alberguen, ya sea temporal o permanentemente, información con nivel de confidencialidad “Confidencial”, o bien guarde relación con la infraestructura crítica institucional o de cualquier otra organización que por la naturaleza de las funciones fuere necesario tomar conocimiento.

**Reutilización segura de equipos**

Antes de la reutilización o devolución de cualquier equipo de computación, se deberá realizar borrado seguro de la información o destrucción física del dispositivo de almacenamiento, especialmente en el caso de almacenamiento de información Interna o Confidencial.

**Deberes 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 institucional que se accede por medios tecnológicos institucionales:

* Almacenar bajo llave, los documentos en papel y los dispositivos de almacenamiento removibles, en cajones u otro tipo de archivo seguro cuando no están siendo utilizados, especialmente fuera del horario laboral.
* Guardar bajo llave la información Interna o Confidencial (preferiblemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso. Cuando la información de clasifique como Interna, Confidencial o relacionada con la infraestructura crítica, ya sea institucional o de terceras partes, y se encuentre en formato digital se debe solicitar a la [unidad TIC o equivalente] la disponibilización de software de alto nivel que resguarde efectivamente la confidencialidad, integridad y disponibilidad de dicha información.
* 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 sensible, una vez impresa.
* Accesos remotos a estaciones de trabajo vía VPN (virtual Private Network) que se solicitan y justifican a través de la [unidad TIC o equivalente].
* En ningún caso compartir clave, será considerado una infracción a las políticas de seguridad de la información, y que esta sea compleja para evitar usurpación de identidad y conexiones no autorizadas a los sistemas institucionales.
* No conectar dispositivos de memoria externos a los equipos, si no han sido autorizados por la [unidad TIC o equivalente].
* No conectarse a correo distinto al institucional. En caso de ser necesario y autorizado, evitar bajar archivos al equipo procedentes de correo no institucional ya que no pueden ser chequeados por las herramientas de seguridad que filtran código malicioso conocido que se encuentre inserto en ellos. Al respecto, en caso de necesitar bajar archivos en cuenta de correo no institucional, se recomienda reenviar al correo institucional para que se realice chequeo de seguridad automático.

**b.- Instalación y utilización de software**

Queda prohibido realizar descargas, distribución y ejecución de aplicaciones, documentos, películas u otros contenidos que vulneren los derechos de autor (copyright) o propiedad intelectual de personas o compañías.

Los trabajadores no deben instalar software en el equipamiento asignado (notebook, computador de escritorio, teléfono móvil, tablet u otros), sin la previa autorización de la jefatura correspondiente y con la evaluación de la [unidad TIC o equivalente].

**c.- Prohibiciones en uso de la red**

* El intercambio de archivos a través de programas no permitidos en la infraestructura de la empresa, del tipo P2P, TOR o equivalentes para acceder a la DeepWeb y la DarkWeb, y almacenamientos públicos en la nube, salvo que sea un servicio formalmente ofrecido, controlado y mantenido por la [unidad TIC o equivalente].
* Entregar o facilitar la contraseña institucional a otras personas ajenas a las funciones del trabajo.
* Uso de sitios de radios en línea y televisión en línea, salvo expresa justificación de la jefatura.
* Uso de sitios de chat online y aplicaciones (Messenger, Skype, entre otros).
* Uso de juegos online.
* Uso de internet para actividades ilícitas y realizar ofertas fraudulentas de productos o servicios.
* La descarga que no cumpla con la normativa vigente de copyright, transmitir o distribuir material que viole los derechos de autor regulado según la legislación chilena.
* Introducir programas maliciosos a la red (ej. Troyanos, virus, malware, otros).
* El acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro contenido inapropiado, salvo aquellos requeridos por la naturaleza de las funciones institucionales del usuario.
* No se debe compartir la conexión red inalámbrica.
* El uso de redes sociales para temas no relacionados con su función en la empresa.

**d.- Uso de la Red WIFI**

La información intercambiada por este medio deberá restringirse sólo a propósitos institucionales. La [unidad TIC o equivalente] estará facultada para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su correcto funcionamiento.

La Red WiFi deberá con métodos de autentificación para ingresar a la red inalámbrica basada en RADIUS, Active Directory, WPA2/3, o los estándares de autenticación robusta que los reemplacen. Se deberá incorporar un segundo factor de autenticación (2FA) si el acceso WiFi permite ingresar a la red interna.

Los trabajadores son los responsables de aplicar un buen juicio para el uso razonable de los recursos.

**Disponibilidad**

La red Wifi o red inalámbrica estará disponible mientras esté dentro del rango de cobertura de los puntos de acceso de la red. La velocidad de accesos a los recursos y calidad de la conexión podrían variar por la distancia a que se encuentren las estaciones de trabajo con los puntos de acceso y la arquitectura de las instalaciones institucionales. Podrían existir interferencias provocadas por otros dispositivos inalámbricos. Por esta razón se sugiere no establecer aplicaciones de misión crítica sobre este tipo de redes, y realizar pruebas previas ante una nueva aplicación que quiera ponerse en producción.

**Privilegios**

La red inalámbrica presenta restricciones en la navegación por internet, las que se manifiestan como control de acceso a sitios que se identifiquen como contaminados o repositorios de código malicioso que puede poner en riesgo la seguridad informática de las redes institucionales al contaminar la estación de trabajo (virus, malware, troyano, etc.), sitios que degradan los servicios de red o sitios que no se ajustan a las normas de uso de la empresa.

**Solicitudes de acceso**

La dependencia que requiera red inalámbrica debe solicitarlo formalmente a la Jefatura de la [unidad TIC o equivalente], indicando las causas por la que requiere el servicio, donde se evaluará la factibilidad técnica y logística para su instalación, siendo esta Unidad el único autorizado para instalar, configurar y dar mantenimiento a la infraestructura de red inalámbrica.

 Cualquier equipo personal, que por necesidades institucionales deba conectarse a la red, debe ser autorizado por la jefatura correspondiente. El equipo personal será revisado por personal de la [unidad TIC o equivalente], minimizando las brechas de seguridad que podrían existir en estos (actualizaciones, aplicaciones ilegales, antivirus etc.)

**Seguridad**

La [unidad TIC o equivalente] al igual que la Unidad de Auditoría Interna, tienen la facultad de auditar el tráfico de la red para poder analizar el comportamiento, detectar infracciones a las políticas de seguridad de la información y prevenir tráfico indeseable que puede ser causa de virus, instalaciones defectuosas no autorizadas u otras causales, que puedan perjudicar la infraestructura tecnológica institucional.

**f.- Uso de contenidos multimedia en las estaciones de trabajo**

Cada usuario debe mantener el buen uso de las estaciones de trabajo o dispositivos, asegurando que no exista software no licenciado, archivos de música o audios en general (mp3 u otro formato), imágenes, libros electrónicos, archivos de películas o cualquier aplicación que requiera licenciamiento para su utilización que no se justifique en relación con las funciones laborales.

Adicionalmente la Ley 17.336 sobre Propiedad Intelectual en su Artículo 3°, ejemplifica algunos tipos de obras que quedan protegidos por esta ley. En este sentido todo documento electrónico (música, software, juegos, películas independientes del formato electrónico y/o repositorio) que viole los derechos de autor respecto del marco legal enunciado, puede ser considerado una violación del principio de probidad, y será considerado una infracción a las políticas de seguridad de la información. Lo anterior, sin perjuicio de la responsabilidad civil o penal que corresponda.

La [unidad TIC o equivalente] tiene la facultad de monitorear el mal uso de las estaciones, pero no será responsable por el mal uso de ellas. El mal uso recae sobre el usuario que ejecuta el mal uso, asumiendo también la responsabilidad la Jefatura directa del mismo.

**g.- Uso de Impresoras.**

Con relación al uso de las impresoras, se deben tener presente las siguientes consideraciones:

* Las impresoras, sólo podrán ser utilizadas para imprimir documentos requeridos por la empresa.
* El material impreso que contenga información Interna o Confidencial debe ser retirado de la impresora sin demora y no dejarlo descuidado en áreas abiertas sin protección. Se considera una falta grave exponer esta información a personas que no tengan el perfil necesario para tomar conocimiento de dicha información.
* Las impresiones de cheques, certificados, u otros documentos de similar naturaleza, deben ser almacenadas en forma segura y estar disponibles sólo al personal autorizado.
* Cada dependencia será responsable de mantener los suministros correspondientes para su funcionamiento.
* En caso del mal funcionamiento o uso deberá informar a la [unidad TIC o equivalente], según corresponda.

**h.- Computadores, equipos o dispositivos portátiles entregados por el Ministerio**

Para garantizar la seguridad y estabilidad de la red de la empresa, se deben considerar las siguientes condiciones para los computadores portátiles:

* Todo equipo o dispositivo portátil, institucional, que se conecta a la red empresarial debe ser incorporado al dominio empresarial. El uso debe estar relacionado con las actividades del área a la cual ha sido asignado.
* Los equipos o dispositivos portátiles, en general, deben permanecer en las instalaciones del trabajador asignado, durante los días y horarios hábiles de trabajo, salvo excepciones. Algunas excepciones son: asistencia en terreno, instancias de trabajo a distancia o teletrabajo, instrucciones especiales ante estados de excepción constitucional u otra situación de contingencia debidamente autorizada por la jefatura e informada a la [unidad TIC o equivalente].
* En caso de licencia o vacaciones del trabajador, el equipo portátil debe quedar a disposición del área. No obstante, si la jefatura inmediata lo autoriza, puede ser utilizado en periodos de licencia o vacaciones.
* La instalación, configuración, modificación o eliminación de software aplicativo sobre los equipos portátiles es responsabilidad exclusiva de la [unidad TIC o equivalente].
* La [unidad TIC o equivalente] tiene la potestad para remover, sin notificar al trabajador, cualquier software que no esté autorizado.

Para los equipos computadores, equipos o dispositivos portátiles no empresariales queda prohibida la conexión a la red interna, salvo que la [unidad TIC o equivalente] disponga de una red virtual de invitados o equivalente, separada lógicamente de la red interna, y en lo posible separada físicamente de la red interna. El acceso de equipos no empresariales en la red interna cualquiera sea su naturaleza deben ser tratados como un elemento externo y deben suscribirse los acuerdos de confidencialidad y tomar conocimiento de las políticas de seguridad de la información institucionales, emulando el acceso de un proveedor externo a datos y redes institucionales.

**i.- Servicio de telefonía IP**

La [unidad TIC o equivalente], es la encargada de suministrar el servicio de telefonía de voz sobre la red (VoIP) utilizando la red institucional. Dicho servicio es administrado mediante una plataforma centralizada, donde se encuentran configurados los parámetros específicos para la asignación de nuevos anexos, ejecución de las llamadas, brindando de esta manera un servicio centralizado, eficiente y expedito.

Toda llamada que se realice, entre anexos y/o hacia el exterior, se encuentra protegida a través de firewall, dispositivos que protegen de posibles ataques y/o intrusiones a la red, obteniendo con ello un nivel de protección acorde a lo implementado en los Data Center institucionales.

**j.- Servicio de Videoconferencia o teleconferencia institucional[[1]](#footnote-1)**

Se provee el servicio de videoconferencia a través de la Red empresarial para facilitar las comunicaciones entre la empresa y las Unidades relacionadas.

Las conexiones de videoconferencias que se establecen pueden ser monitoreadas por la [unidad TIC o equivalente], con el propósito de velar que se realicen de manera oportuna y eficiente.

Las conversaciones sostenidas dentro de las Videoconferencias o teleconferencias, así como material que sea compartido dentro de estas, no son registradas por la [unidad TIC o equivalente], en ningún medio de almacenamiento.

Se podrán establecer otras formas de teleconferencia según la tecnología y recursos disponibles, siempre que cumplan los requisitos mínimos establecidos por la [unidad TIC o equivalente]; en principio, se consideran los siguientes salvo que la [unidad TIC o equivalente] disponga algún ajuste al estándar de exigencias mínimo:

* Encriptado de extremo a extremo, utilizando algoritmos de cifrado robustos (verificando que no se incluyan aquellos que ya se han descartado por haberse quebrado su seguridad). Al menos considerar AES-256 para las conferencias normales y algoritmos de rango superior para conferencias de nivel seguridad nacional.
* Encriptado de las contraseñas.
* Autenticación de los participantes, en lo posible con segundo factor de autenticación.
* En lo posible con servidores centrales que estén bajo control institucional. Si la solución utilizada se encuentra en la nube se deben tomar los resguardos para que las comunicaciones, conversaciones y documentos que se intercambian queden, de ser requerido, almacenados de manera segura (encriptada).
* Soporte de cumplimiento e integración con otras soluciones de ciberseguridad como “Prevención de Robo de Datos” (DLP por sus siglas en inglés) por ejemplo, e integración con otras herramientas organizacionales que permitan interoperar las funciones y plataformas de productividad y de uso institucional.
* Opciones de seguridad para los administradores de la plataforma.
* Las comunicaciones en lo posible deben ofrecer trazabilidad para efectos de auditorías posteriores en cuanto a su utilización.
* Establecer las consideraciones requeridas para verificar que la información transmitida NO es almacenada por el proveedor, sin el consentimiento o gestión del administrador del servicio, y que no se tiene acceso por parte de este, a la información personal de los participantes.
* Los aplicativos deben en un entorno rico en dispositivos de múltiples sistemas operativos, ofrecer capacidad multiplataforma para maximizar la flexibilidad de uso.
* Todo aplicativo eventualmente puede tener vulnerabilidades, ya sea por su codificación propia como por la plataforma sobre la cual se instala. Por tanto, un factor relevante a considerar es el soporte profesional con el que cuenta y el respaldo de sus desarrolladores para garantizar estabilidad, continuidad y seguridad mientras duren los contratos o expectativas de utilización de la herramienta.
* Cada herramienta debe entonces ser evaluada también por sus vulnerabilidades que pueden finalmente afectar o comprometer la seguridad de la teleconferencia, de la información personal e institucional de los participantes, y los activos institucionales.
* Con estos criterios generales e debe realizar un proceso de verificación que permita seleccionar la herramienta óptima en funcionalidad y en seguridad para tomar las bondades del trabajo a distancia sin comprometer la seguridad de la información institucional.

**k.- Servicio de Correo electrónico**

Por su naturaleza, complejidad técnica y jurídica, se desarrolla en una Política Específica independiente.

**IV.- SERVICIO SOPORTE INFORMÁTICO**

A continuación, se presentan las actividades de Soporte técnico que realiza la [unidad TIC o equivalente], en relación con el equipamiento y servicios computacionales que son entregados para el uso directo de los trabajadores.

**a.- Actividades y funciones**

* Mantener registro de los equipos que se conectan a la empresa, que han sido asignados a través de la [unidad TIC o equivalente] y teniendo presente que también hay otras Unidades que administran la asignación de recursos computacionales. En consecuencia, la [unidad TIC o equivalente] reportará a la Unidad responsable de Inventario los movimientos que se realicen para que mantengan actualizado Inventario institucional.
* Determinar la vida útil de los equipos informáticos e informar las renovaciones necesarias.
* Apoyo en las especificaciones técnicas requeridas para las solicitudes de contratación y compra de equipos personales institucionales.
* Realizar el mantenimiento lógico preventivo de todos los equipos informáticos de la empresa.
* Encargado de instalar, modificar, desinstalar aplicaciones.
* Encargado de instalar y configurar estaciones de trabajo habilitando los servicios computacionales que sean requeridos.
* Implementar procesos automáticos para actualización de software de productividad, antivirus y antispam.
* Verificar que los equipos se encuentren en condiciones de funcionamiento para su uso.
* Mantener registro de los programas computacionales que se encuentren instalados en los equipos, asegurando su correcta licencia y uso.
* Instruir al usuario de las políticas de seguridad, normativas, y procedimientos que se encuentran en la intranet, cuando sea necesario.
* Mantención de usuarios con sus privilegios correspondiente a su cargo, lo que se refiere a la creación, actualización y eliminación de usuarios de la red de acuerdo con lo informado por el Departamento Desarrollo y Gestión de Personas. La definición de perfiles se refiere a los permisos de navegación y atribuciones de acceso remoto para soporte técnico.
* Entregar soporte técnico en los sistemas desarrollados por la [unidad TIC o equivalente] y servicios computacionales institucionales.
* Se realizarán los respaldos de equipos computacionales que sean requeridos por la autoridad pertinente y vaciado a dispositivos externo y entregado al solicitante.

**b.- Asistencia a Usuario**

Las solicitudes de soporte técnico podrán ser solicitadas por las siguientes vías:

* Correo electrónico a soporte@miempresa.cl;
* Llamada telefónica dirigidas al +56 2 2345 6789;
* Documento formal dirigido a la jefatura de la [unidad TIC o equivalente];

Todas las solicitudes de Soporte ingresan al Sistema de Mesa de Ayuda cuya respuesta no podrá ser mayor a 24 horas laborales.

Para la resolución de problemas en las estaciones de trabajo, los técnicos podrán tomar control del equipo vía remota con previa autorización del trabajador. Lo que queda reflejado en Auditoria de las estaciones de trabajo, la cual podrá ser revisada ante requerimiento de la autoridad. Esta auditoría será mantenida a lo menos por un año y siempre y cuando los recursos disponibles lo permitan.

En caso de usuarios con perfil autoridad, no es posible acceder a los dispositivos por vía remota, por lo que soporte técnico deberá ser realizado presencialmente.

1. https://www.csirt.gob.cl/media/2020/04/Recomendaci%C3%B3n-Teleconferencia.pdf [↑](#footnote-ref-1)