**POLÍTICA DE TRABAJO A DISTANCIA Y TELETRABAJO**

**I.- DEFINICIONES ESTRATÉGICAS**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento las características mínimas obligatorias de seguridad de la información, confidencialidad, integridad y disponibilidad, para abordar el trabajo a distancia y teletrabajo.

Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Se denomina teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante esos medios.

En este contexto la empresa incorpora esta modalidad de trabajo bajo la ley vigente[[1]](#footnote-1) e introduce consideraciones de ciberseguridad para que estas labores se desempeñen sin poner en riesgo la información de la empresa ni los activos de información en general.

**a.- Objetivos**

Los objetivos que busca esta política son los siguientes:

* Definir las condiciones y las restricciones del uso del trabajo a distancia y del teletrabajo.
* Establecer medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo.

**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 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.- TRABAJO A DISTANCIA Y TELETRABAJO**

Por la complejidad y transversalidad del concepto se implementa una política específica y las medidas que apoyan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia y de teletrabajo.

**a.- Definiciones estructurales:**

Las definiciones fundamentales que se tendrán en consideración en todas las políticas en las que se integre el concepto de “trabajo a distancia” o “teletrabajo” serán las establecidas en la Ley N°21.220:

Trabajo a distancia:

Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Teletrabajo:

Se denominará teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios.

**b.- condiciones del uso del trabajo a distancia y del teletrabajo**

Cada unidad organizacional establecerá:

* que funcionarios están en condiciones de realizar trabajo a distancia o teletrabajo.
* que roles son los que se considerarán dentro de los posibles de incorporar.
* Que información o sistemas son lo que necesitan (previa validación con la [Unidad TIC])

La [Unidad TIC] establecerá:

* que servicios estarán disponibles para teletrabajadores
* los tipos de servicios de red y aplicaciones
* los esquemas de identificación, autenticación y autorización, es decir, cómo deben identificarse los teletrabajadores, autenticarse y recibir la autorización antes de acceder a los recursos de la empresa.
* Especificaciones de equipos y software: ¿hay algún dispositivo específico o producto de software que deba implementarse en el equipo del teletrabajador? (por ejemplo, firewall, pendrive encriptado o software de encriptación).
* Integridad y confidencialidad: cómo debe protegerse la conexión desde el equipo remoto (es decir, VPN) y cómo deben protegerse los datos en dicho equipo.
* Pautas de mantenimiento: ¿cómo debe ser la configuración equipo del teletrabajador?.
* Directrices del usuario: que aclaren el papel del usuario en la protección de los recursos de la empresa, por ejemplo, uso apropiado de los recursos; el usuario no debe modificar las configuraciones de seguridad; utilizar de software antivirus; almacenamiento de datos corporativos en unidades locales; uso de encriptación herramientas.

El [comité de Riesgos y Seguridad de la Información] deberá velar por que se cumplan las siguientes exigencias normativas:

* la seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;
* el entorno de teletrabajo físico propuesto;
* los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que se traspasará por el enlace de comunicaciones y la sensibilidad del sistema interno;
* la provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;
* la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;
* el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;
* las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;
* acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;
* acuerdos de licenciamiento de software que pueden hacer que las organizaciones se hagan responsables del software de cliente en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;
* requisitos de protección de malware firewall (cortafuegos).

Las pautas y disposiciones que se deberán incluir son:

* la provisión de equipos idóneos y muebles de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;
* una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;
* la provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;
* seguridad física;
* normas y orientación sobre el acceso a familiares y visitas a los equipos y a la información;
* la provisión de soporte y mantenimiento de hardware y software;
* la provisión de seguros;
* los procedimientos para el respaldo y la continuidad en el negocio;
* auditoría y monitoreo de seguridad;
* revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.

Siempre se deberá evaluar incorporar las recomendaciones y buenas prácticas sugeridas por el CSIRT de Gobierno.

**c.- consideraciones del uso del trabajo a distancia y del teletrabajo**

Las principales consideraciones que deberán contemplar los jefes de cada una de las unidades organizacionales son:

* Restricciones de información - ¿hay tipos de información confidencial/interna/sensible que no deberían estar a disposición de los teletrabajadores?
* Analizar los privilegios que necesitará el teletrabajador para aplicarlos bajo el principio de los mínimos privilegios (en cuando acceso a la plataforma de sistemas de la empresa) para funcionar.
* El equipo del teletrabajador debe estar protegido, actualizado y monitoreado.
* Educación del usuario: los usuarios deben conocer y entender los posibles riesgos de la información asociados con el teletrabajo, cómo se abordan esos riesgos y el papel del usuario en minimizando los riesgos.
* La seguridad en modalidad de trabajo a distancia o teletrabajo no debe ser inferior a la seguridad mínima exigida en modo presencial.

**d.- medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo**

**Modo de operación**

La activación del trabajo remoto deberá estar previamente autorizada por el jefe de la unidad correspondiente y los usuarios definidos deberán tener sus anexos de contrato firmados y validados por sus jefaturas correspondientes y con su equipamiento de trabajo debidamente asignado.

**Consejos preventivos para teletrabajo**

* Habilitar una zona dentro de tu hogar con suficiente espacio para contener los equipos y materiales de trabajo.
* Aislar los ruidos externos y los propios de la casa
* Controlar la iluminación, temperatura y ventilación de lugar definido.
* Es conveniente disponer de luz natural, esta disminuye el riesgo de fatiga visual.
* Evite consumir alimentos y líquidos cerca del su equipo, podría dañarlo.
* Evite cableado eléctrico suelto, fíjelo cosa de evitar accidentes.
* Utilice pausas de trabajo para consumir alimentos.
* Si tiene cansancio o pérdida de concentración realice un descaso.

**Medidas de seguridad**

* A modo de “mejores prácticas” se deben promover e implementar las siguientes medidas de seguridad, asociadas al uso de computadores utilizados bajo modalidad de teletrabajo:
* Usar protector de pantalla con clave cuando el computador no esté en uso.
* No dejar Pendrive/Flash Drive olvidados en los computadores.
* Bloquear puertos USB del equipo para periféricos de almacenamiento externos. Es importante mencionar que en caso de excepciones previamente autorizadas podrán ser habilitados para tal efecto en forma temporal.
* Fomentar la costumbre de: “Darle a los bienes el mismo cuidado que le daría Ud. Como si fuera el propio”.
* El usuario debe asegurarse de que su equipo cuenta con el software antivirus, el cuál debe ser actualizado por lo menos una vez por semana.
* Queda estrictamente prohibido que el personal conecte a la red equipos o dispositivos que no sean de la empresa, salvo que algún apolítica específica lo autorice y regule, acogiendo conceptos como BYOD[[2]](#footnote-2).
* Quedará prohibido la conexión a redes que no sean de la empresa mientras se encuentre en dependencias de la ésta.
* Queda prohibido la descarga de aplicaciones o software no autorizado por parte de los usuarios en particular para aquellos definidos con acceso remoto.
* El usuario es responsable de copiar, en forma periódica, los archivos de trabajo que residan en su PC; para ello, deberá copiarlos en el servidor que estará disponible en la red para estos efectos. La [Unidad TIC] no considera dentro de sus procedimientos el respaldo de archivos de usuarios.

**Instalación de software base**

A todo equipo, antes de ser asignado para trabajo remoto, se le deberá instalar el siguiente software base:

* Sistema operativo cliente debidamente licenciado y aprobado por la entidad.
* Drivers internos y de periféricos utilizados en la organización.
* Actualizaciones, probadas en la organización.
* Software de ofimática debidamente licenciado.
* Antivirus corporativo.
* Cliente Firewall activo.
* Compresor de archivos utilizado por la organización.
* Aplicaciones requeridas y utilizadas por la organización.
* Visualizador de PDF de ser requerido.
* Java (JRE = Java Runtime Environment), de ser requerido.
* Browser actualizado, como navegador de Internet.
* Acceso VPN requerido.
* Software especializado para acceso remoto.
* Software especializado para realización de video conferencia o teleconferencias.
* Control de dirección “MAC” y dirección “IP”.

Una vez que el computador tenga todo el software base instalado, pasará a llamarse Dispositivo para trabajo remoto y podrá ser asignado a un usuario.

**Registro e inventario de equipos y software instalado**

La [Unidad TIC] es responsable de llevar un registro detallado de los recursos de hardware y software, instalados dentro y fuera de los centros de cómputo, y las descripciones de su localización. Para ello deberá existir un documento de Inventario del equipamiento, en el cual al menos deberá ser identificado:

* el modelo
* la serie del equipo
* su dueño
* el nivel de criticidad (alto, medio o bajo)
* el tipo de acceso que el usuario tendrá (local, remoto)
* N° de IP
* características del equipo (Ram, DD, CPU)
* otros antecedentes que sean importantes a considerar.

**Cuidados especiales para trabajo remoto**

* Protector de pantalla con clave activado y con tiempo de activación inferior a 5 minutos.
* Evitar navegar por sitios desconocidos.
* No descargue música, videos, películas o programas desde Internet.
* No instale ninguna aplicación en los equipos móviles que no sea autorizada y supervisada por área de TI
* Evite ingresar a sitios desde publicidad en páginas web.
* Si el remitente de un mail no es seguro o es extraño, ¡Nunca abra los archivos adjuntos!
* Mantenga su antivirus actualizado.
* Revisiones periódicas (diarias) de su equipo para asegurar que esté actualizado (antivirus y sistema operativo).

**Consideraciones especiales en trabajo remoto:**

Contacte vía teléfono a la [Unidad TIC] cuando:

* su equipo no se pueda conectarse a internet.
* su equipo no se pueda conectarse a alguna aplicación.
* su equipo no se encienda.
* su conexión VPN no funcione.

**e.- Aspectos mínimos para verificar la operatividad de la política**

* Normativa de protección del puesto de trabajo remoto.
  + Informar al personal sobre la normativa de protección del puesto de trabajo fuera de la oficina llevando a cabo auditorías periódicas para asegurar su cumplimiento.
* Relación de usuarios que disponen de la opción de trabajar en remoto.
  + Llevar un control de las personas que, por su perfil dentro de la empresa o las características de su trabajo, tienen la opción de teletrabajar.
* Procedimientos para la solicitud y autorización del teletrabajo.
  + Redactar un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración del mismo, dispositivos facilitados, etc.), que será firmado por cada teletrabajador.
* Periodo de implantación y pruebas.
  + Valorar diferentes escenarios y configuraciones antes de habilitar el teletrabajo, contemplando todos los riesgos de seguridad.
* Realizar pruebas de carga en escenarios simulados.
  + Si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, valorar la carga que esto ocasiona en los sistemas internos de la empresa.
* Aplicaciones y recursos a los que tiene acceso cada usuario.
  + Dar acceso a cada empleado solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro de la organización. Detallar las aplicaciones permitidas así como sus condiciones de uso. Valorar la inclusión del nuevo software solicitado por los empleados.
* Acceso seguro.
  + Gestionar las credenciales de acceso de los empleados forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación siempre que sea posible.
* Configuración de los dispositivos de teletrabajo.
  + Configurar los dispositivos utilizados por el empleado para teletrabajar (sistema operativo, antivirus, control de actualizaciones, etc.), tanto si son corporativos como si son aportados por el trabajador (BYOD).
* Cifrado de los soportes de información.
  + Implantar tecnologías de cifrado que protegen la información de posibles accesos malintencionados.
* Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa.
  + Elaborar las políticas que detallan a los empleados dónde deben guardar la información con la que trabajan en remoto.
* Planificación de las copias de seguridad de todos los soportes.
  + Compruebar regularmente que se realizan periódicamente y que pueden restaurarse.
* Uso de conexiones seguras a través de una red privada virtual o VPN.
  + Implementar una red VPN extremo a extremo que permite que la información que se intercambia entre los equipos de la organización viaje cifrada a través de Internet.
* Aplicaciones de escritorio remoto siempre a través de una VPN.
  + Para ofrecer un extra de seguridad y privacidad a las comunicaciones, solo se permite el uso de las aplicaciones de escritorio remoto bajo una VPN.
* Virtualización de entornos de trabajo.
  + Valorar la implementación de la virtualización como método para proporcionar a cada empleado su propio espacio de trabajo, eliminando los riesgos asociados al uso de un dispositivo físico.
* Priorizar el uso de dispositivos corporativos.
  + Elegir los dispositivos corporativos para teletrabajar, ya que cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura.
* Conexión a Internet.
  + Cuando no es posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizar la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi públicas.
* Uso de dispositivos personales bajo una política BYOD.
  + Utilizar las configuraciones y conexiones permitidas y seguras al teletrabajar desde tus dispositivos personales.
* Concienciar a los empleados antes de empezar a teletrabajar.
  + Educar a los empleados en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas y las medidas que se llevaran a cabo en la empresa.
* Cumplimiento Ley de Datos Personales.
  + Educar a los empleados que manejan datos personales para la protección de los mismos durante el teletrabajo y realizar los cambios en los tratamientos para contemplar estas situaciones.
* Aplicaciones de teleconferencia y colaborativas.
  + Configurar estas aplicaciones para un uso seguro que permita que se respeten la privacidad y la propiedad intelectual de los participantes.

1. Ley N° 21.220 https://www.bcn.cl/leychile/navegar?idNorma=1143741 [↑](#footnote-ref-1)
2. https://es.wikipedia.org/wiki/Bring\_your\_own\_device [↑](#footnote-ref-2)