**POLÍTICA CONTROL DE ACCESO**

**I.- DEFINICIONES ESTRATÉGICAS**

**a.- Objetivo general**

La empresa, a través de su [Comité de Riesgos y Seguridad de la Información], presenta en este documento la Política de Control de Acceso a las instalaciones físicas y tecnológicas institucionales.

Con esta Política, la empresa, se compromete, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo informático, asegurando el cumplimiento de los requisitos legales, junto a la racionalización del uso de los recursos.

La [Unidad TIC] establece como Política de Control a las medidas para controlar y limitar el acceso a la información, a sus instalaciones de procesamiento de datos e información (Datacenter) y a los procesos de empresariales implementados con plataforma tecnológica controlada por esta [Unidad TIC], los cuales deberán ser administrados sobre la base de los requisitos de eficiencia, eficacia, ciberseguridad y los que disponga la Ley vigente.

La [Unidad TIC] proveerá la plataforma tecnológica que permita a los diferentes actores en la materia, administrar el ciclo de vida de los usuarios, desde la creación de las cuentas, roles y permisos necesarios hasta su cierre por las causales que la empresa estimare necesarias.

**b.- Objetivos específicos**

* Identificar los requerimientos de seguridad de cada una de las aplicaciones.
* Identificar toda la información relacionada con las aplicaciones.
* Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
* Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
* Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en la empresa.
* Establecer los niveles de acceso apropiados a la información de la empresa, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

**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.- CONTROL DE ACCESOS**

**a.- Reglas para el control de acceso**

Las reglas para el control de acceso, estará documentado a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos.

**b.- Gestión de identidades**

La [Unidad TIC] implementa el control de acceso a la plataforma usuaria a partir de la identificación de funcionarios reportados por Departamento de Desarrollo y Gestión de Personas, en lo que se refiere a usuario de red, correo electrónico y telefonía IP. Para lo cual, se requiere conocer las altas y bajas del personal en forma oportuna.

El acceso de usuarios autorizados a los sistemas será determinado por el dueño de la información, para lo cual la [Unida TIC] habilita para cada sistema un Módulo de Administración de usuarios.

**Responsabilidad de los usuarios**

Todos el personal o terceros que dispongan de acceso a la plataforma tecnológica de la empresa son responsables del cuidado de su información de autenticación y de la información empresarial a la que acceda, cumpliendo con todas las normas de seguridad de la empresa.

**c.- Control de acceso a la red institucional**

La [Unidad TIC] controlará el acceso a los servicios de red tanto internos como externos con el propósito de garantizar la seguridad de los usuarios y mantener la estabilidad de los servicios, para lo cual se restringen los puertos de acceso por defecto, salvo casos particulares y debidamente justificados.

Las reglas de acceso a la red a través de los puertos[[1]](#footnote-1) estarán basadas en la premisa general de que “todo está restringido, salvo lo que esté expresamente permitido”.

**Procedimientos para la utilización de los servicios de red**

La [Unidad TIC] establecerá procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

* Control el acceso a los servicios de red tanto internos como externos.
* Control de acceso a los equipos de red en forma local y/o remota.
* Identificación de las redes y servicios de red a los cuales se permite el acceso.

**Autenticación de usuarios para conexiones externas**

La [Unidad TIC] proveerá servicios de conexión remota a la plataforma empresarial basados en la tecnología y plataforma de red privada virtual: servicio VPN (por sus siglas en inglés), con lo cual el tráfico de datos entre usuario remoto y red institucional se encontrará debidamente encriptada.

Dependiendo del perfil del usuario y de si la clasificación de la información a transferir a través de la VPN es confidencial o interna, relacionada con la infraestructura crítica o de terceras partes ya sean públicas o privas, o relativas a la seguridad nacional, la autenticación deberá contar, progresivamente, con el nivel más alto de robustez, incorporando múltiples factores: “algo que el usuario sabe”, “algo que el usuario tiene” y “algo que el usuario es”, es decir, utilizar un segundo o triple factor de autenticación:

* Algo que sabemos, por ejemplo, una contraseña o un código PIN.
* Algo que poseemos, por ejemplo, una tarjeta de coordenadas o un token RSA.
* Algo que somos (autenticación biométrica), como la forma de la mano o la huella dactilar.

**Identificación de equipos en la red**

La [Unidad TIC] controlará e identificará los equipos conectados a la red institucional, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.

**Seguridad y Protección de los equipos de comunicaciones**

El acceso a la administración directa de los equipos de comunicaciones debe ser debidamente protegida para lo cual se configura acceso lógico con sistema de autentificación y debe estar ubicado en lugar físico resguardado de accesos de personal no autorizado.

Por lo cual, al realizar algún soporte o mantenimiento a los equipos de red, sólo personal autorizado por la [Unidad TIC] puede acceder a estos equipos.

**Separación de redes**

Para la gestión de la red, se aplicará segmentación de redes apoyada con dispositivos de seguridad denominados Cortafuegos o “Firewalls”, para controlar el acceso entre los segmentos.

Los criterios para implementar son:

* Ubicación geográfica
* Funcionalidad
* Ubicación espacial
* Organizacional
* Tipos de conexión
* Otros.

**Control de conexión de las redes**

La [Unidad TIC] controlará y limitará el acceso de los equipos, para los siguientes servicios:

* Conexiones WiFi será WPA2/AES/CMMP o superior.
* Mensajería instantánea.
* Telefonía IP a través de internet.
* Videoconferencia o Teleconferencias través de la intranet institucional e internet.
* Correo electrónico comercial no autorizado que sea identificado como tal.
* Descarga de archivos de sitio peer to peer (P2P).
* Conexiones a sitios de streaming o multimedia no autorizado.
* Servicios de escritorio remoto a través de internet.
* Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de esta.
* El acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, xenofóbico, sexistas, negación, minimización grave, aprobación o justificación de genocidios o delitos contra la humanidad o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.

**Acceso a internet**

La [Unidad TIC] proveerá este servicio a través de sus ISPs (Proveedor de Servicio de Internet), el que será el único servicio de internet autorizado.

La instalación de cualquier dispositivo, no autorizado por la [Unidad TIC], que permita acceder a internet a un equipo de la empresa será considerado una infracción grave a la seguridad de la información.

**d.- Control de acceso al sistema operativo**

**Registro de inicio seguro**

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, permitiendo el acceso al usuario autorizado exclusivamente, contemplando las siguientes condiciones:

* No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
* No suministrar mensajes de ayuda, durante el proceso de autenticación.
* Validar los datos de acceso, una vez se han entregado todos los datos de entrada.
* Limitar el número de intentos fallidos de conexión, auditando los intentos no exitosos posteriormente.
* No mostrar las contraseñas digitadas.
* No transmitir la contraseña en texto claro, es decir se transmite siempre encriptada y verificando que los protocolos de encriptado estén vigentes y no declarados como obsoletos o débiles.
* Se protegen los registros de los accesos a las estaciones de trabajo, permitiéndose el acceso exclusivamente para casos de auditorías e investigaciones instruidas por el Jefe de Servicio.

**Gestión de contraseñas**

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo de la [Unidad TIC]. Las recomendaciones mínimas para proteger las contraseñas y evitar que sean conocidas por otros, de modo de minimizar los riesgos de accesos no autorizados son:

* No escribirlas en papeles de fácil acceso, agenda, ni en archivos sin cifrar.
* No habilitar la opción “recordar clave en este equipo”, que ofrecen los programas.
* No enviarla por correo electrónico.
* Mantener las contraseñas confidenciales en todo momento.
* No compartir las contraseñas con otros usuarios. Hay que recordar que las credenciales de usuario/contraseña pueden considerarse como una firma electrónica según la Ley N° 19.799[[2]](#footnote-2).
* Cambiar su contraseña si piensa que alguien más la conoce.
* Seleccionar contraseñas que no sean fáciles de adivinar.
* El sistema de validación para el ingreso a la red (controlador de dominio o sistema equivalente) solicitará cambiar sus contraseñas cada 90 días.
* No utilizar la opción de almacenar contraseñas en Internet.
* No utilizar contraseña con números telefónicos, nombre de familia etc.
* No utilizar contraseña con variables (Por ejemplo: soporte1, soporte2, soporte3).

**Uso de software del sistema**

Todo software que se utilice en la institución debe cumplir con los licenciamientos correspondientes del proveedor y contratos de mantención de al menos las actualizaciones de solución de problemas de seguridad. Los equipos computacionales contemplan una instalación de software estándar descrito en la normativa “Utilización de equipos personales” e “Instalación legal de software” publicadas en la [Intranet o sitio web interno de la empresa]. En estas, se establece una política a nivel de controlador de dominio o sistema equivalente para la gestión centralizada de autenticación e identidad, que no permite la instalación de software y cambios de configuración del sistema, salvo que se trate de personal autorizado de la [Unidad TIC].

Ningún usuario final, deberá tener privilegios de usuario administrador en ningún equipo o dispositivo.

**Tiempo de inactividad de la sesión**

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión automáticamente, sin cerrar las aplicaciones que se encuentren abiertas.

Los usuarios deberán bloquear sus sesiones, cuando abandonen temporalmente su puesto de trabajo (Tecla Windows + L) y apagar los equipos al finalizar la jornada laboral o cuando se ausenten por más de dos (2) horas.

Téngase presente que si se están desarrollando trabajos remotos que requieran el acceso al equipo, éste podrá quedar encendido pero debidamente bloqueado su acceso.

**Control de acceso a la información**

El control de acceso a la información a través de una aplicación se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

Todo acceso a información confidencial debe estar registrado y auditado.

**Alistamiento de sistemas sensibles**

La [Unidad TIC] identificará según los niveles de clasificación de información, o por definición legal, o a requerimiento de otra unidad debidamente fundado, cuáles son los sistemas sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes, con requerimientos de seguridad de la información robustos y resilientes, propios del tratamiento de infraestructura crítica o equipamiento de misión crítica.

Al aislar estos sistemas, se preverá que el intercambio de la información con otras fuentes de datos sea seguro, ya que no se permitirá duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

**e.- Computación móvil y trabajo remoto**

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, como así mismo, el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional al utilizar estos medios, a continuación, se establecen directrices orientadas a regular el uso de la computación móvil y trabajo remoto y que son de responsabilidad de los funcionarios usuarios de la plataforma institucional.

**Computación y comunicaciones móviles**

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

* Uso de usuario y contraseña para acceso al mismo.
* Cifrado de la información.
* Uso de software antivirus provisto por la [Unidad TIC].
* Restricción de privilegios administrativos para los usuarios.
* Uso de software licenciado y provisto por la [Unidad TIC].
* Realización de copias de seguridad periódicas.
* Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
* Permanecer siempre cerca del dispositivo.
* No dejar desatendidos los equipos.
* No llamar la atención, acerca de portar equipos móviles.
* No identificar el dispositivo con distintivos de la [Unidad TIC] o de la empresa.
* No colocar datos de contacto técnico en el dispositivo.
* Mantener cifrada la información confidencial.
* No conectarse a redes WiFi-públicas.
* Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica equivalente, si es que no se está utilizando.
* Informar de inmediato a la [Unidad TIC] en caso de pérdida o hurto del dispositivo, quien procederá al bloqueo del usuario.

Para dispositivos de comunicación móvil (telefonía celular) y tablets de la empresa se deben aplicar y mantener las siguientes condiciones:

* Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.
* No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.
* Sólo a los dispositivos entregados por la institución se les realizaran las configuraciones de correo electrónico.
* En el dispositivo se deben instalar las “apps”[[3]](#footnote-3) mínimas para la función laboral y siempre revisando los permisos que se entregan sean los mínimos necesarios.

**Trabajo remoto**

El trabajo remoto sólo será autorizado por el responsable de la División o centro de responsabilidad de la cual dependa el personal que solicite el permiso. Dicha autorización sólo se otorgará para los servicios y sistemas en que se verifique se dan las condiciones de seguridad de las comunicaciones establecidas por las Políticas Institucionales en la materia, lo que será confirmado por la [Unidad TIC].

Lista de verificación final:

A modo de resumen se deberán verificar, al menos, los siguientes aspectos para confirmar operatividad de la política de control de acceso y sus respectivos procedimientos:

* Política de usuarios y grupos
	+ Definir los roles de usuarios y de grupos en función del tipo de información al que podrán acceder.
* Asignación de permisos
	+ Asignar los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones oportunas sobre la información a la que tienen acceso.
* Creación/modificación/borrado de cuentas de usuario con permisos
	+ Definir y aplicar un procedimiento para dar de alta/baja o modificar las cuentas de usuario.
* Cuentas de administración
	+ Gestionar las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad.
* Mecanismos de autenticación
	+ Determinar e implantar las técnicas de autenticación más apropiados para permitir el acceso a la información de la empresa.
* Registro de eventos
	+ Establecer los mecanismos necesarios para registrar todos los eventos relevantes en el manejo de la información de la empresa.
* Revisión de permisos
	+ Revisar cada cierto tiempo que los permisos concedidos a los usuarios son los adecuados.
* Revocación de permisos y eliminación de cuentas
	+ Desactivar los permisos de acceso y eliminar las cuentas de usuario una vez finalizada la relación contractual.
1. https://es.wikipedia.org/wiki/Puerto\_de\_red [↑](#footnote-ref-1)
2. https://www.bcn.cl/leychile/navegar?idNorma=196640 [↑](#footnote-ref-2)
3. https://es.wikipedia.org/wiki/Aplicaci%C3%B3n\_m%C3%B3vil [↑](#footnote-ref-3)