GOBIERNO DE CHILE
JUNTA NACIONAL DE AUXILIO
ESCOLAR Y BECAS

APRUEBESE LA POLÍTICA A.06.02.02 QUE APOYA A LA SEGURIDAD DE LA INFORMACION A LA QUE SE ACCEDE, PROCESA O ALMACENA EN SITIOS REMOTOS DE LA JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

RESOLUCIÓN EXENTA Nº 2457

SANTIAGO, 27 de noviembre 2018

VISTO: Lo dispuesto en la ley N° 15.720 que crea la Junta Nacional de Auxilio Escolar y Becas; el decreto supremo. N° 5.311, de 1968, del Ministerio Educación reglamento general de JUNAEB, el decreto ley N° 180, de 1973, que reorganiza a JUNAEB, el D.F.L. N° 29, del Ministerio de Hacienda, del 2004, que fija el texto refundido, coordinado y sistematizado de la ley N° 19.834 sobre Estatuto Administrativo, en la ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; en la ley N°19.880 que establece Bases de los Procedimientos Administrativos, en la ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica, y Servicios de Certificación de dicha Firma, en el decreto N° 181, de 2012, que aprueba el reglamento de la ley N° 19.799; en la ley N° 19.233 sobre Delitos Informáticos, en la ley N° 20.285 que regula el principio de Transparencia de la Función Pública y el derecho de Acceso a la Información; en el decreto supremo N° 83, 2004, del Ministerio Secretaría General de la Presidencia que aprueba Norma Técnica para Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, en la Norma Chilena NCh-ISO 27001.Of2013 Tecnologías de la Información – Técnicas de Seguridad – Sistemas de Gestión de la Seguridad de la Información – Requisitos; en el Decreto Supremo N° 5, de 2018, del Ministerio de Educación que designa a don Jaime Tohá Lavanderos en el cargo de Secretario General de JUNAEB y en la Resolución N° 1.600, de 2008, de la Contraloría General de la República que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1.- Que, de conformidad al artículo 5 del D.F.L. N° 1-19.653, de 2001, del Ministerio Secretaria General de la Presidencia que aprueba el texto refundido, coordinado y sistematizado de la ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado, "las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública".

2.- Que, dada las características de la información que maneja este servicio respecto de personas naturales y jurídicas, en razón a la función pública que ejerce. La cual se encuentra en diversos formatos, pero en especial, en papel y que busca ser almacenada en depósitos que velaran por su confidencialidad, integridad y disponibilidad, resulta imperioso contar con una política de trabajo para dar fiel cumplimiento a la legislación vigente referente a la seguridad de la información.

3.- Que, en mérito de lo señalado precedentemente se ha elaborado una Política "**A.06.02.02 QUE APOYA A LA SEGURIDAD DE LA INFORMACION A LA QUE SE ACCEDE, PROCESA O ALMACENA EN SITIOS REMOTOS**" del Sistema de Gestión de la Seguridad de la Información, que tienen por objeto Proporcionar lineamientos sobre la seguridad de la información a la que se tienen acceso, cuando se realicen accesos remotos virtuales, ya sea por funcionarios de Junaeb o proveedores de servicio externo, que por razones de negocio se encuentren imposibilitados de acceder a las instalaciones físicas de JUNAEB

RESUELVO:

ARTÍCULO PRIMERO: APRUÉBESE la Política **A.06.02.02 QUE APOYA A LA SEGURIDAD DE LA INFORMACION A LA QUE SE ACCEDE, PROCESA O ALMACENA EN SITIOS REMOTOS** del Sistema de Seguridad de la Información de la **JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS**, cuyo texto se inserta a continuación:

DIRECCIÓN

POLITICA A.06.02.02 QUE APOYA A LA SEGURIDAD DE LA INFORMACION A LA QUE SE ACCEDE, PROCESA O ALMACENA EN SITIOS REMOTOS

JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS
JEFE
DEPTO. DE PLANIFICACIÓN Y CONTROL DE GESTIÓN Y ESTUDIOS
CHILE

Autorizado Firma Jefe del Informática	Autorizado Encargado de Seguridad de la Información
Elaborado por: Departamento de informática	**Revisado por:** Departamento de Planificación

INDICE

1. OBJETIVO

Proporcionar lineamientos sobre la seguridad de la información a la que se tienen acceso, cuando se realicen trabajos de accesos remotos virtuales, ya sea por funcionarios de Junaeb o proveedores de servicio externo, que por razones de negocio se encuentren imposibilitados de acceder a las instalaciones físicas de JUNAEB.

2. ALCANCE

La presente política aplica a todo funcionario JUNAEB (planta, contrata, agentes públicos, honorarios, practicantes u otra persona natural o jurídica que tenga que tenga relación contractual con JUNAEB), así como proveedores que presten servicio fuera de las dependencias de Junaeb, (desde ahora trabajador), a través del único medio valido para para tal efecto que es la conexión por túnel VPN.

3. ROLES Y RESPONSABLES

ROL	Responsabilidad
JEFE DE DEPARTAMENTO DE INFORMÁTICA	Velar por el cumplimiento de las directrices impartidas.
ENCARGADA SEGURIDAD DE LA INFORMACIÓN	Verificar la aplicación de la política, validando el ejercicio y conocimiento de la norma por los funcionarios y sus jefaturas. Coordinar las acciones del Comité de Seguridad de la Información.
JEFATURAS DE DIVISIONES Y DIRECTOR REGIONAL	Autorizar el uso de acceso remoto VPN para funcionarios de su dependencia.
FUNCIONARIOS	Cumplir con lo formalizado en este documento y así garantizar los activos que se encuentra a su cargo.
PROVEEDORES	Cumplir con lo formalizado en este documento y así garantizar los activos que se encuentra a su cargo
ENCARGADO DE UNIDAD DE INGENIERIA DE SISTEMAS E INFRAESTRUCTURA	Gestionar el acceso VPN a usuarios autorizados.
INGENIERO DE SISTEMAS	Ejecutar tareas de acceso y denegación de acceso a VPN.

4. REFERENCIAS NORMATIVAS

- Ley Nº 9.223, que tipifica figuras penales relativas a la informática.
- Ley Nº19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley Nº19.880, que establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
- Ley Nº20.521, que modifica la Ley Nº19.628, sobre protección de datos de carácter personal para garantizar que la información entregada, a través de predictores de riesgo, sea exacta, actualizada y veraz.
- Decreto Supremo Nº83/ 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los Órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.
- NCh-ISO 27001, sobre Sistemas de Gestión de la Seguridad de la Información.

POLITICAS Y PROCEDIMIENTOS ASOCIADO A ESTA POLITICA

- Acceso para Conexiones Externas.[1]
- Política de Control de Acceso.
- Procedimiento de Control de Acceso.
- Política de Escritorio y Pantalla Limpios.
- Ubicación y protección del equipamiento.

[1] Instructivo de trabajo VPN-SSL-Junaeb

5. DEFINICIONES

5.1 TRABAJO REMOTO

Sólo podrán realizar trabajo con acceso remoto en los sistemas de la institución, aquellas personas con vínculo de cualquier naturaleza con la Institución, previamente autorizadas, de acuerdo a la Política y Procedimiento de Control de Acceso, las conexiones de trabajo con acceso remoto realizadas por usuarios autorizados desde cualquier otro lugar situado fuera de las instalaciones físicas de la Institución, deben estar controladas de modo que se asegure la autenticación de los usuarios que acceden, la confidencialidad de la información transmitida, la limitación de los recursos accedidos por el funcionario y la supervisión de las mismas.

JUNAEB, autoriza la utilización de equipos institucionales y/o personales a los trabajadores para la ejecución de sus obligaciones y/o funciones, fuera de las instalaciones físicas de la Institución, donde debe implementar todas las medidas de seguridad definidas por organización.

El trabajador o cualquiera que tenga accesos remotos virtuales debe dar fiel cumplimiento a los contratos contractuales con sus cláusulas de confidencialidad, y lineamientos de las políticas y procedimientos de Seguridad de la Información, así como lo relacionado al uso exclusivo del equipo que se destine para la ejecución de sus obligaciones y/o funciones (según corresponda a la calidad jurídica).

Se debe dar un seguimiento de las conexiones remotas

Los trabajadores no deben almacenar en los equipos asignados o personales información sensible o reservada. En lo que respecta a la información que se encuentre contenida en medios digitales, los trabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de seguridad de la información establecidos por JUNAEB y que a continuación se relacionan:

- Si los equipos son personales, el trabajador debe instalar el sistema operativo desde una fuente fiable.

- Debe mantener el sistema operativo y las aplicaciones actualizadas manteniéndolo libre de amenazas tanto físicas[2] como lógicas software.

[2] Ubicación y protección del equipamiento

- Debe manejar cuentas de usuario independientes o incluso el uso de sistemas operativos o máquinas virtuales separadas al uso personal.

- Los equipos no deben dejarse desatendidos, el trabajador debe evitar transportar el equipo si no es necesario.

- Debe borrar el histórico de navegación, las cookies y otros datos del navegador web que sean de acceso referentes a JUNAEB.

- No utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas) sin algún tipo de cifrado punto a punto como puede ser VPN o conexiones a sitios web protegidos con SSL (los que empiezan por HTTPS), siempre y cuando no sean provistas por JUNAEB.

- Utilizar contraseñas según política y procedimientos de gestión de contraseñas siguiendo de JUNAEB.

- Por políticas de seguridad de la Información, el trabajador, no debe usar el cuadro de dialogo en el que se sugiera recordar contraseña.

- Al finalizar el trabajo, cerrar todas las conexiones con servidores y páginas web utilizando cuando sea posible la opción "desconectar" o "cerrar sesión".

- Eliminar la información temporal alojada en carpeta de descargas, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del dispositivo.

En lo que respecta a la información que se encuentre contenida en medios físicos, los trabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de seguridad de la información establecidos por la entidad y que a continuación se relacionan:

Almacenar los documentos en un lugar seguro solo de acceso para el trabajador.[3]

En caso de se deban destruir documentos será necesario romperlo o triturarlo con el objeto de evitar que la pieza documental se arroje de manera completa al contenedor o papelera y

[3] Política de pantallas y escritorio limpios

sea reutilizada para labores domésticas que de alguna manera ponga en riesgo la información institucional.

No dejar las copias impresas desatendidas en la bandeja de la impresora.

No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de trabajo.

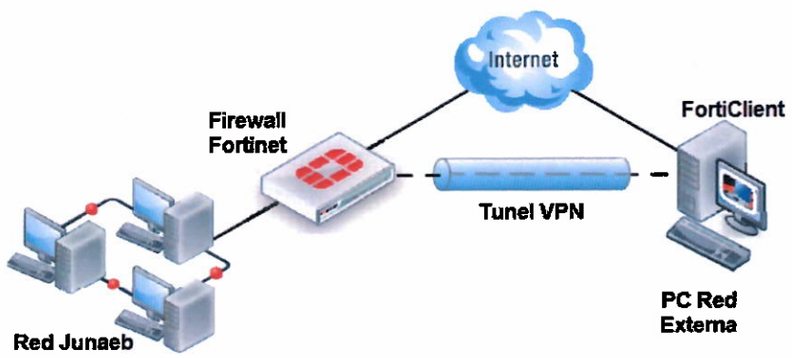
5.2 ACCESO REMOTO

Los servicios de acceso remoto permitidos son aquellos que respondan a necesidades de la Institución, tales como desarrollo, mantenimiento y soporte. En estos casos, existen mecanismos técnicos para manejar convenientemente la información transmitida, los sistemas y recursos accedidos, la identidad de los individuos que realizan dichos accesos y las posibles implicancias que el acceso conlleva.

Los servicios de acceso remoto deben ser asignados de manera exclusiva a través de lo descrito en el Procedimiento de Control de Acceso.

El acceso remoto asignado por el Departamento de Informática es generado a través de un protocolo de conexión específico para el establecimiento de una conexión VPN de manera directa entre el equipo que se conectará desde el exterior y el cortafuego (firewall) y los sistemas internos de la Institución que no estén publicados hacia el exterior, proporcionando acceso a los recursos de la red de datos institucional y generando tráfico de datos bajo un formato encriptado, de manera controlada y segura. Con ello, se evita el procesamiento y almacenamiento de información en equipos de propiedad privada, excepto a proveedores que presten servicios desde sus dependencias previa autorización de la jefatura de departamento demandante y jefatura del Departamento de Informática.

Topología VPN



Fuente propia Departamento de Informática

5.3 CONSIDERACIONES GENERALES

Para minimizar el riesgo de acceso no autorizado a las redes de JUNAEB, un usuario remoto nunca deberá almacenar sus contraseñas tal como lo indica la Política de Escritorio y Pantalla Limpios.

En caso de uso de equipamiento tecnológico con acceso remoto, bajo entornos de redes domésticas o públicas, el usuario se deberá asegurar que ésta siempre contenga mecanismos de seguridad. Esto será de exclusiva responsabilidad del usuario

En caso de pérdida, robo o hurto del equipamiento tecnológico, si fuese propiedad de JUNAEB, utilizado para trabajo con acceso remoto, debe notificar al Departamento de Informática.
JUNAEB dispondrá de un canal de ayuda para realizar soporte sobre trabajo con acceso remoto, para los casos en que existan problemas en la utilización correcta del acceso remoto, tanto por el método de conexión como en el equipamiento.

6. PERIODIOCIDAD DE EVALUACIÓN Y REVISIÓN

El presente documento tiene una vigencia de 3 años una vez aprobada su elaboración. Sin perjuicio de lo anterior, el documento puede ser evaluado y/o actualizado en cualquier momento, dependiendo de la necesidad de la organización por modificación en el proceso y/o seguridad de la información.

7 DIFUSION

El presente documento será difundido del portal de intranet Institucional.
Todos los usuarios de JUNAEB, tienen la responsabilidad de conocer la presente política y cumplir lo que en ella se indica.

8 CONTROL DE CAMBIOS

Nº	Cambio	Fecha	Autorizado por:
01	Elaboración inicial	24/10/2018	Jefe del Departamento de Informática

ARTÍCULO SEGUNDO: PUBLÍQUESE la presente resolución una vez que se encuentre totalmente tramitada en la sección de actos y resoluciones con efectos sobre terceros, del banner de gobierno transparente en el portal web de JUNAEB, a objeto de dar cumplimiento con lo previsto tanto en el artículo 7 de la ley N° 20.285, sobre Acceso a la Información Pública, como asimismo en el artículo 51° de su reglamento

ANÓTESE.

Junta Nacional de Auxilio Escolar y Becas
SECRETARIO GENERAL

JAIME TOHA LAVANDEROS
SECRETARIO GENERAL
JUNTA NACIONAL DE AUXILIO ESCOLAR Y BECAS

DIRECCIÓN NACIONAL DE AUXILIO ESCOLAR Y BECAS
JEFE GABINETE

/MBG/AFP/PFR/xah

DISTRIBUCIÓN:

1. Departamentos y Unidades de JUNAEB
2. Direcciones Regionales
3. Oficina de Partes

JUR N° 2648-2018