DOCUMENTO ELECTRONICO

(V5) APRUEBA INSTRUCTIVO “POLITICA GENERAL DE USO DE LOS RECURSOS INFORMÁTICOS DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO” Y DEROGA RESOLUCIÓNES EXENTAS N°14.184 DEL AÑO 2016.
RESOLUCION EXENTO Nº: 12510/2017
Santiago28/09/2017

VISTOS:
Lo dispuesto en el artículo 9º del D.F.L. Nº 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley Nº 18.359, que crea el cargo de Subsecretario de Desarrollo Regional y Administrativo en el Ministerio del Interior; en el D.F.L. Nº 1-18.359, de 1985, del Ministerio del Interior, que traspasa y asigna funciones a la Subsecretaría de Desarrollo Regional y Administrativo; en la Ley Nº 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y sus modificaciones; en su Reglamento contenido en el D.S. Nº 250, de 2004, del Ministerio de Hacienda y sus modificaciones; en el D.S. N°739, de 11 de marzo del 2014, del Ministerio del Interior y Seguridad Pública, que nombra Subsecretario de Desarrollo Regional y Administrativo; la Resolución Exenta N° 14.184, de 01 de diciembre de 2016, que aprobó Instructivo “Politica General de uso de los Recursos Informáticos de la Subsecretaría de Desarrollo Regional y Administrativo”; y en la Resolución Nº 1600, de 2008, de la Contraloría General de la República.

CONSIDERANDO:
1.- Que, la gestión de la Subsecretaría de Desarrollo Regional y Administrativo debe desarrollarse en un marco de mayor expedición y transparencia.

2.- Que, entre otras obligaciones le corresponde asegurar un buen y correcto uso de los recursos y bienes que se le encuentran asignados.

3.- Que, se precisa contar con políticas que regulen el buen uso de los recursos informáticos y de la infraestructura de red existente en la Subsecretaría de Desarrollo Regional y Administrativo.

4.- Que, en dicho contexto, el presente acto administrativo viene en aprobar el instructivo interno sobre “Política General de uso de los recursos informáticos de la Subsecretaría de Desarrollo Regional y Administrativo- SUBDERE”.

5.- Que, en el proceso de actualización y mejora permanente de las normas de seguridad de la información, el presente acto administrativo viene en aprobar este nuevo instructivo que reemplaza el aprobado por Resolución Exenta N° 14.184, de 01 de diciembre de 2016.

RESUELVO:
ARTÍCULO 1°.- APRUEBASE el instructivo sobre “Política General de Uso de los Recursos Informáticos de la Subsecretaría de Desarrollo Regional y Administrativo- SUBDERE”, cuyo tenor es el siguiente:

“POLÍTICA GENERAL DE USO DE LOS RECURSOS INFORMÁTICOS DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO - SUBDERE"

1. ASPECTOS GENERALES:

La red SUBDERE y los Computadores, proporcionan acceso a recursos informáticos, dentro y fuera del ámbito de la SUBDERE, permiten la comunicación dentro de Chile y con el resto del mundo. Este privilegio acarrea responsabilidades para el personal de SUBDERE, cualquiera sea la calidad jurídica en que haya sido contratado, quienes deberán respetar los derechos de los demás usuarios, la integridad del sistema y de los recursos físicos, todo ello con el debido respeto de las leyes y regulaciones vigentes.

La presente Política se enmarca en los siguientes lineamientos:

1.1. Necesidad: Los usuarios de los recursos informáticos, de las redes de la SUBDERE serán responsables de su utilización en términos adecuados y de mantener el respeto a los demás usuarios. Esta política aporta una serie de recomendaciones y líneas de actuación para lograr el uso correcto de los recursos informáticos y la adopción de buenas prácticas.

1.2. Objetivos de la Políticas: Asegurar una infraestructura informática que facilite la realización de las misiones básicas de SUBDERE, como son la comunicación con regiones, municipalidades, las tareas administrativas de soporte interno, el apoyo a los productos estratégicos de la Subsecretaría. Los computadores, servidores y redes son tecnologías que permiten de forma eficiente el acceso y distribución de información. Como tales, se consideran una infraestructura estratégica para el desarrollo de los objetivos de la SUBDERE. Además, estas tecnologías permiten la posibilidad de acceder, copiar y compartir información con fuentes remotas. Esta política recomienda un uso apropiado de los servicios informáticos, y entregar derechos y fijar obligaciones para los usuarios o funcionarios de SUBDERE, además, norma las consecuencias del uso incorrecto de los servicios informáticos.

2. ÁMBITO DE APLICACIÓN:

2.1. Agentes a los que se aplica esta política: Será de aplicación para todo el personal de la SUBDERE, independiente de su calidad jurídica, o que se encuentren en comisión en ella, que haga uso de los recursos tecnológicos que SUBDERE les provea y que son definidos en el punto 2.2 siguiente. Además, se aplicará a cualquier otra entidad externa o proveedores que utilicen dichos recursos informáticos.

2.2. Recursos a los que se refiere esta política: Se incluyen toda las tecnologías de la información y comunicación (TIC), sistemas de información, ya sean individuales o compartidos y estén o no

conectados a las redes institucionales de la SUBDERE. Se aplicará a todos los equipos, estaciones de trabajo, notebooks, servidores, equipos de video conferencia, equipos de comunicaciones, impresoras, scanner y periféricos en general, además, de los enlaces de comunicaciones administrados directa o indirectamente por el Departamento de Informática de SUBDERE, independientemente que se use para gestión administrativa, económica, investigación, docencia u otros fines de tipo institucional.

2.3. Aspectos legales: Se aplicarán las leyes y normativa chilena, en relación con la protección de datos personales, propiedad intelectual y sobre uso de herramientas Informáticas, así como aquellas que se aprueben en el futuro sobre la materia. Por todo ello, la SUBDERE podrá ser requerida por los órganos administrativos o contralores pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco jurídico definido por las siguientes Leyes y Decretos Supremos:

• Ley 19.223 (publicada el 07/06/1993) que Tipifica Figuras Penales Relativas a la Informática, que al efecto señala.
• Artículo 1° "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena del presidio menor en su grado medio a máximo.
Si como consecuencia de estas conductas se afectasen los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo".

• Artículo 2° "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en el sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio".
• Artículo 3° "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".
• Artículo 4° "El que maliciosamente revele o difunda datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable técnico o administrativo del sistema de información, la pena aumentará en su grado".

• Ley Nº 17.336 (D.O. 02/10/1970): Sobre Propiedad Intelectual, se debe considerar que toda la información que se genera en el servicio es de propiedad de la SUBDERE.
• Ley Nº 19.628 (D.O. 28/08/1999): Sobre la protección de la vida privada o protección de datos de carácter personal.
• Ley Nº 19.812 (D.O. 13/06/2002): Que modifica Ley Nº 19.628: Sobre protección de la vida privada.
• Ley Nº 19.799 (D.O. 12/04/2002): sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
• Ley N°18.168 (D.O. publicada 02/10/1982) Ley General de Telecomunicaciones.
• Ley Nº 19.880 (D.O. 29/05/2003): sobre Bases de los Procedimientos Administrativos, se refiere a acceso a información personal y privacidad.
• Ley N °19.927 (D.O. 14/01/2004) Ley contra la Pedofilia.

Decretos Supremos

• Decreto Supremo Nº 83/2004 que Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad del Documento Electrónico.
• Decreto Supremo Nº 93/2006, que Aprueba norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
• Decreto Supremo N°14, de 27 de febrero de 2014, que Modifica el Decreto N°181, que aprueba el reglamento de la Ley N°19799, sobre documentos electrónicos, firma electrónica y certificación de dicha firma y deroga los Decretos que indica.
• Norma Chilena de Seguridad NCH 27002:2013, que hace referencia a los controles de la seguridad informática.

2.4 Actualización de la Política: Esta política se actualizará cada tres años. El fundamento de la presente actualización de este documento normativo, se vincula con la separación de los controles de infraestructura como el Data center, servidores, equipos de comunicaciones, servicios que proveen terceros etc. que de acuerdo a la recomendación de la norma 2007.

3. ROLES Y RESPONSABILIDADES:

3.1. Responsable Administrativo del Equipamiento a su cargo: Es el funcionario o alumno en práctica a quien la SUBDERE le asigna un bien informático al momento de ingresar o acceder a la institución. El usuario debe firmar un acta de recepción con los bienes asignados.

3.2. Administrador de Sistemas: Es el responsable de la gestión y administración de los sistemas a su cargo y de supervisar el cumplimiento de la política de uso de los mismos. Será normalmente el responsable técnico informático que está a cargo del sistema.

3.3. Responsable Administrativo de los recursos informáticos de la SUBDERE es el Jefe del Departamento de Informática.

3.4. Usuarios: Todo funcionario independiente de su calidad jurídica o alumnos en práctica de la SUBDERE que utilice los recursos informáticos de la institución.

3.5. Responsable de seguridad: Será quien se encarga de dirigir las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma.

3.6. Consultor externo: se considera a empresas de desarrollo, de servicio de comunicaciones, consultor que por la naturaleza de sus actividades debe tener acceso a los servicios informáticos de manera remota o directamente en las dependencias de SUBDERE.

4. POLITICAS DE CONTROL DE ACCESO. (A.09.01.01)

El objetivo es limitar el acceso a la información y a las instalaciones físicas o lógicas donde se procesa la información, para ello se entregan una serie de recomendaciones que regulan el buen uso, disponibilidad y nivel de servicio de los recursos informáticos, se fijan las reglas de control de información, los derechos y restricciones de acceso para los roles o privilegios de cada usuario que manejan los activos de información de su responsabilidad estimando los riesgos de seguridad asociados.

Para SUBDERE los controles de acceso son lógicos y físicos estos se integran de manera adecuada considerando que la información que circula al interior de la institución es cercano al 100% de tipo digital, los activos de información original siempre son archivados y resguardado por la Oficina de Partes, entidad funcional que cumple entre otros el rol de frontera entre SUBDERE y el medio ambiente externo a la institución.

Se debe considerar que SUBDERE mantiene segregación en el uso de las herramientas informáticas

implementadas, es decir, un rol determinado tiene asignado los privilegios que le corresponde al rol de acuerdo a las necesidades de acceso de información, existe coherencia entre el derecho de acceso a la información y la clasificación de los activos de información respecto de los sistemas y redes que maneja SUBDERE.

La unidad de redes de SUBDERE maneja la administración de los derechos de acceso para el entorno distribuido a nivel nacional y segmentado por tipo de red, es decir, para cada red regional maneja segmentación propia y en el nivel central esta segmentado por cada división, esto permite mayor control y en el caso de incidente se pueden aislar él o los problemas (bajar) de inmediato sin comprometer a toda la organización, con esto se logra administrar los tipos de conexiones disponibles. El control de acceso basado en roles es el enfoque que SUBDERE utiliza para el acceso a sistemas que manejan activos de información.

La política de control de acceso se relaciona y se respalda con los procedimientos que maneja el departamento de informática para aplicar en concordancia con procedimientos como “Revisión Derechos de Acceso”, “Gestión Privilegios de Sistemas”, “Gestión Derecho Acceso”, “Procedimiento de Ingreso y Egreso”, procedimientos, controles y recomendaciones que forman parte de la presente política general de recursos informáticos.

4.1. ACESO A REDES Y SERVICIOS DE RED. (A.09.01.02)

Los usuarios sólo tienen acceso a las redes y a los servicios, sistemas o plataformas en los que cuenta con autorización específica, esta política cubre a todas las redes, con sus segmentaciones y servicios asociados.

4.1.1 Es requisito y obligatorio para todos los usuarios de SUBDERE la autenticación de usuario (login/password) para acceder a los distintos servicios de red y sistemas locales y de gestión interna.

4.1.2. Los usuarios deben respetar la integridad de los recursos y sistemas de informáticos. Para ello se difunden una serie de recomendaciones, mediante políticas, procedimientos o instructivos.

4.1.3. La Unidad de Redes del Departamento de Informática de SUBDERE tiene la responsabilidad y obligación del monitoreo del uso de servicio de red. Seguridad perimetral, seguridad en la navegación, inspección en el caso de detectar operaciones de tráfico anómalo.

4.1.4. La Unidad de Redes del Departamento de Informática de SUBDERE administra herramientas de acceso con los requisitos de autenticación del usuario para acceder a los distintos servicios, niveles y sistemas de la red SUBDERE.

4.1.5. La Unidad de Redes del Departamento de Informática de SUBDERE administra servicios de privilegios especiales como VPN, Redes inalámbricas WIFI corporativas, aplicando procedimientos para la asignación de privilegios en las oficinas regionales y central en el Edificio Moneda Bicentenario. Uso de las VPN es uso exclusivo de los jefes de División y Departamento.

En caso de necesidad de algún funcionario para el desempeño de sus labores, el acceso a este servicio deberá ser solicitado por su jefe directo, mediante correo electrónico institucional, o memorándum a través del SGDOC, o ticket de mesa de ayuda. Es de responsabilidad del solicitante informar el retiro de los accesos o privilegio solicitado.

El jefe del Departamento de Informática revisará e instruirá para su aprobación y/o rechazo a la Unidad de Redes y Seguridad.

4.1.6. El Departamento de Informática cuenta con un procedimiento de alta y baja de funcionarios donde se establece al usuario a quién se le permite acceder a que redes, servicios y nivel de privilegio, el acceso por defecto es sistemas internos y navegación estándar.

4.1.7. Está prohibido instalar computadores o cualquier otro dispositivo de propiedad privada en la red de datos de SUBDERE. Salvo excepciones que serán autorizadas por el jefe del Departamento de Informática.

4.1.8. Todas las conexiones a los servicios de red no autorizadas y no seguras, pueden afectar a toda la organización por ello se identifican los accesos en especial a las aplicaciones o servicios sensibles para el servicio.

4.2. RESPONSABILIDAD DE LOS USUARIOS. (A.09.03.01)

El usuario es el responsable de proteger su información de autenticación, por lo que es necesario que el funcionario adopte las políticas, procedimientos e instructivos de la organización en el uso de información institucional. Todo usuario o funcionario que haya sido autorizado a usar una cuenta mediante un sistema de (login/password) será responsable de mantenerla en secreto y no darla a conocer, el entregar la credencial de acceso a terceros es una falta. Es el usuario el que siempre será responsable de lo que se ejecute en desde su cuenta, en el uso de la red, sistemas, correo electrónico institucional u otras. Los funcionarios deberán evitar tener recursos compartidos (archivos, directorios, carpetas, etc.) sin el mecanismo de seguridad necesarios y disponibles en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

4.2.2. Sobre Contraseñas Adecuadas

4.2.1. Debe contener al menos 8 caracteres y no más de 64. Se recomienda combinar números y letras en mayúscula y minúscula, de preferencia no repetir los mismos caracteres. La contraseña distingue mayúsculas y minúsculas, por ello deberá de recordar las letras que escribe en mayúscula. En caso de incluir caracteres que no sean alfa-numéricos se debe validar que el sistema lo permite.

4.2.2. Nunca utilice una contraseña que resulte fácil de averiguar cómo su fecha de nacimiento, o el nombre de sus hijos, familiares o mascota. Su contraseña no debe contener su nombre de correo electrónico, sus apellidos o la respuesta a su pregunta secreta. Tampoco se deben de utilizar derivados de estos, ni datos personales fáciles de indagar.

4.2.3. Nunca escriba su contraseña en papel. Elija una contraseña que pueda recordar (la contraseña debe ser fácil de recordar para no tener que escribirla, es deseable que se pueda escribir sin necesidad de mirar el teclado.

4.2.4. No utilice palabras de diccionario en ningún idioma. En la actualidad existen muchos programas para develar claves, que basan su ataque en técnicas de diccionario y de fuerza bruta.

4.2.5. Nunca envíe su contraseña por correo electrónico o en un mensaje instantáneo (tampoco mencionarla en una conversación telefónica, ni faltar a la discreción).

4.2.6. No se recomienda poner la misma contraseña de acceso a todos los sistemas. Esto es, una contraseña para los sistemas internos que no debería ser la misma para otras actividades personales o de correo personal. Por ejemplo, correo electrónico, Clave única del Registro Civil, entidades Bancarias etc.

4.2.7. Procure no mantener sus contraseñas indefinidamente. Trate de cambiarlas con cierta regularidad, se recomienda cada 60 días.

4.2.8. Existen varias maneras de plantear una contraseña que no sea débil. Por ejemplo, utilice las primeras letras de una frase u oración que no sea tan conocida (puede combinarla con números, letras, o bien, puede elegir palabras sin sentido pero que sean pronunciables, Ejemplo (1Ejemp.,#)

4.2.9. Como política una contraseña para acceder a la red o un sistema admitirá un número limitado de intentos y se bloqueará. En caso de que esto suceda debe enviar un aviso al administrador solicitando una credencial transitoria.

4.3. SISTEMA DE CONTROL DE ADMINISTRACION DE CONTRASEÑAS. (A.09.04.03)

SUBDERE cuente con sistema de administración de contraseñas interactivo y que garantiza contraseñas de calidad, encriptado mediante protocolo Kerberos, este sistema centralizado de contraseñas permite forzar el uso de IDs de usuarios y contraseña individual (login/password), además, permite que cada usuario pueda seleccionar y cambiar su propia contraseña, es responsabilidad de cada usuario mantener contraseñas robustas.

El sistema obliga al usuario a cambiar sus contraseñas al primer inicio se sesión, además, como parte de la política SUBDERE impone a cambiar en intervalos regulares cada 90 días, el sistema permite no mostrar en la pantalla los caracteres mientras se ingresan o se accede al dominio SUBDERE, permite almacenar y transmitir contraseñas en forma protegida.

Se debe considerar que los sistemas internos se SUBDERE se autentifican contra un servicio de control y administración de contraseñas utilizando las potencialidades técnicas y de administración que maneja el Active Directory, no obstante, en SUBDERE los servicios como correo y algunas aplicaciones que manejan contraseñas de manera individual cumplen técnicamente como establece la norma y las presentes políticas.

Asegurarse que su cuenta sea cerrada o bloqueada al final de cada sesión. Bloquear cuando no se encuentre en su estación de trabajo (presionar teclas Windows L simultáneamente)

Las contraseñas de acceso entregada por el Departamento de Informática para red, correo institucional o sistemas, son genéricas, es responsabilidad del usuario cambiarla y generar una contraseña segura en el primer ingreso (Ver 4.2.2. Sobre Contraseñas Adecuadas)

4.3.1 Sobre accesos no autorizados y suplantación de identidad.

Los usuarios no deben tratar de conseguir accesos a sistemas o recursos a los que no estén autorizados y asignados los privilegios respectivos, tampoco permitir o facilitar que otros lo hagan. Los sistemas de uso compartidos proporcionan mecanismos para proteger los datos e información privada, ante posibles consultas no autorizadas. Los intentos de saltarse estos mecanismos para conseguir accesos a información calificada como personal o privada supondrán una violación de esta política e incluso del marco legal señalado en el apartado 2.3. Aspectos Legales.

Los administradores de sistemas pueden acceder, por motivos de mantenimiento y/o de seguridad, a las bases de datos de sus sistemas, sólo con la finalidad de permitir revisar log de registro, detectar, analizar y seguir las trazas de una determinada sesión o conexión, el administrador no debe modificar datos o transacciones que afecten la integridad, confidencialidad e integridad de la información.

En cualquier caso, el administrador de sistemas tiene el deber de guardar secreto sobre el contenido de los archivos de los usuarios, no estando autorizado para permitir que terceros puedan acceder a los mismos ni difundir o publicar datos personales.

El administrador sólo podrá entregar credenciales de acceso a información institucional y que sea solicitada formalmente por (Jefes de División, Departamento o Unidad) de funcionarios que están bajo su bajo su cargo, debiendo formalizar mediante expediente o correo electrónico. Será responsabilidad del Jefe del Departamento de Informática registrar el privilegio asignado temporalmente al jefe o a quien él indique la entrega de credenciales de acceso.
Cualquier defecto o anomalía que se descubra se debe reportar al Departamento de Informática SUBDERE, esta es la entidad encargada de investigar y proponer soluciones al problema.

5. LOS ADMINISTRADORES DE SISTEMAS Y SUS RESPONSABILIDADES:

Cada miembro de esta Subsecretaría es responsable del equipamiento y recursos asignado por SUBDERE, pero existen recursos como (servidores, aplicaciones, bases de datos, red, equipos de comunicaciones) cuya explotación es compartido por un grupo de usuarios. Estos recursos son de responsabilidad del Departamento de Informática, Unidad de Redes (que asumirá competencias organizativas) y un administrador o responsable técnico del sistema, que será nombrado por el encargado de la unidad de desarrollo, él responsable técnico se encargará de las tareas técnicas y del funcionamiento del recurso en cuestión.

5.1. La administración de los recursos informáticos corresponderá al Departamento de Informática, cumpliendo el rol de Administrador de redes para los recursos informáticos globales de la SUBDERE. El administrador del sistema (en este caso, el Departamento de Informática gestor de los recursos informáticos globales) deberá organizarse y realizar las acciones y esfuerzos necesarios para:

- Prevenir y evitar robos, pérdidas o cualquier daño físico a los componentes del sistema.
- Respetar todos los acuerdos y licencias relativos al hardware y software que sean aplicables al sistema.
-Tratar la información almacenada en el sistema de la forma apropiada y adoptar las precauciones y medidas para proteger la seguridad de los datos, red y equipos según lo especificado en el marco legal vigente y los compromisos adquiridos.
- Dar publicidad a las distintas políticas y recomendaciones de uso de servicios.
- Garantizar los procedimientos de recuperación de la información y del sistema en los servidores bajo su responsabilidad.
- Implantar y hacer cumplir en su ámbito de actuación la política y normas generales, así como las particulares de ámbito de sus competencias.
- Mantener actualizados y seguros los sistemas bajo su responsabilidad.
- Colaborar con otros administradores de sistemas de otras entidades o redes (ejemplo otros ministerios), para resolver los problemas causados desde máquinas bajo el dominio SUBDERE.
- Todo funcionario de SUBDERE que utilizan sistemas informáticos debe reportar incidentes de seguridad, utilizando medios como teléfono, e-mail, mesa de ayuda o personalmente al Jefe del Departamento de Informática o al oficial de seguridad de la información.

Las medidas de seguridad se dimensionarán en función de la importancia de los recursos que se quieran proteger. Para cumplir esta política, el administrador del sistema cuenta con medios restringidos (herramientas y personal) con estos recursos, se deben tomar medidas que garanticen el buen funcionamiento de los recursos informáticos. El administrador de redes de SUBDERE es el responsable técnico de redes. Este profesional puede suspender los privilegios de acceso o conexión

si lo estima necesario o apropiado para mantener la operación y disponibilidad de los sistemas o la red.

5.2. El Responsable de Seguridad es un funcionario de SUBDERE, designado mediante resolución como Oficial de Seguridad, quien se encarga de proponer las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma:

- Interpretación de la política: Será responsable de la interpretación de esta política, de la resolución de los problemas y conflictos con las políticas y otras situaciones especiales.
- Cumplimiento de la política: en los casos en que se produzcan violaciones a esta política, el Responsable de seguridad estará autorizado para trabajar en colaboración con las correspondientes unidades administrativas para su resolución.
- Control y monitorización: será el responsable de diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas, del cumplimiento y ajuste a esta política.
- Responsable del Programa de Mejoramiento a la Gestión de Seguridad de la información (PMG SSI)
- Para asuntos legales derivados del incumplimiento de estas normas se consultará con la Asesoría Jurídica con la Fiscalía de la SUBDERE.

6. CORREO ELECTRONICO. (A.13.02.01)

La Subsecretaria entrega este servicio a los funcionarios para comunicarse, en calidad de usuarios internos y de ellos con usuarios, terceros externos a la Subdere. La vigencia de la cuenta de correo comprende el periodo de compromiso de trabajo con la institución. Este es un servicio externalizado o contratado, por el que se pagan licencias anuales por cada funcionario, en conformidad a la normativa aplicable. Una vez completado el proceso de activación del servicio de correo, el usuario se responsabiliza de mantener la confidencialidad de su contraseña, y de todas las actividades que se efectúen por el uso de ésta. Se debe considerar que el correo electrónico es vulnerable en la medida que no se conserven las medidas de seguridad y buenas prácticas en el uso de este medio de comunicación. (Ver 4.2.2. Sobre Contraseñas Adecuadas)

El Departamento de Informática tiene como obligación aplicar una política de respaldo de las comunicaciones según lo señalado en el artículo 6 del Decreto Supremo Nº83, que aprueba norma técnica sobre eficiencia de las comunicaciones electrónicas entre órganos de la Administración del Estado, que en lo sustancial señala: “Deberá quedar constancia de la transmisión y recepción de las comunicaciones efectuadas por medios electrónicos e identificarse el remitente, destinatario, fecha y hora de las mismas con la finalidad de asegurar la constancia de la transmisión y recepción ”. Este respaldo y archivo de los correos electrónicos será por un plazo de hasta 10 años después de cerrada la cuenta de correo, para lo cual se utiliza un sistema de archiving de los correos, por medio de un proceso de identificación y movimiento de datos inactivos fuera del sistema de producción que permite almacenar la información de forma eficiente y proporcionan recuperaciones rápidas en caso de ser necesario.

La capacidad de la casilla de correo asignada es de 30 GB, con la capacidad para adjuntar archivos de hasta 25 GB, además, cuenta con el servicio de Google Driver con capacidad de 30Gb y otros utilitarios de apps google incluidos en la casilla electrónica y la agenda institucional, la cual es administrada por cada funcionario.

El servicio de correo electrónico institucional es administrado por la, Unidad de Redes que entrega las contraseñas de acceso, monitoreo del servicio, se ocupa del uso eficiente y del resguardo de las buenas prácticas.

6.1. El usuario deberá notificar inmediatamente al Departamento de Informática de cualquier uso no autorizado de su contraseña o cuenta o de cualquier otra falla de seguridad. La notificación puede realizarse por mesa de ayuda, telefónicamente, o por correo electrónico.

6.2. Es responsabilidad del funcionario leer diariamente el correo y responder si corresponde, el usuario para sus actividades personales, comerciales, o políticas no debe utilizar el correo electrónico institucional. Para ello, la SUBDERE entrega las facilidades de no bloquear los servicios de correo tipo WEB MAIL.

6.3. El funcionario responsable en el uso del correo electrónico no puede utilizar este medio para él envió de correos difamatorios, hostigamiento o acoso, compras, ventas no autorizadas, el envío de mensajes con contenido fraudulento, ofensivo, obsceno, amenazante, enviar SPAMS (correo basura), enviar anexos (attachments) que pudieran contener información nociva para otro usuario como virus o pornografía, cartas encadenadas o mensajes excesivamente voluminosos.

6.4. Listas de Correo: Los servicios de mensajería masiva o foros de discusión son herramientas que facilitan la difusión de información a varios interlocutores de una sola vez. El uso de correos masivos está restringido como privilegio especial, el administrador o moderador de este tipo servicios es el Departamento de Informática, para esto la SUBDERE dispone de una lista de correo cerrada, que están bajo el dominio de @SUBDERE.GOV.CL, que contiene las cuentas de correo de quienes trabajan en la institución.

6.5. Se debe considerar que algunos tipos de archivos adjuntos recibidos en el correo electrónico pueden ser peligrosos, en especial los ejecutables o .exe que en su apertura o instalación pueden generar problemas de seguridad al equipo asignado como a la red SUBDERE en general.

6.6. Del Buen Uso del correo, es responsabilidad del funcionario lo siguiente:

1. Depurar y limpiar su casilla de correo, el espacio disponible no es infinito, debe periódicamente limpiar para que exista espacio disponible, el correo electrónico no es un repositorio para guardar documentos del tipo word, pdf, excel, etc.)
2. El empleo de su cuenta es para fines propios del trabajo de la SUBDERE.
3. Leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo (INBOX), El uso de un lenguaje apropiado en sus comunicaciones.
4. Respetar las reglas de “Conducta en Internet” para las comunicaciones.
5. No permitir que otras personas hagan uso de su cuenta de correo o suplantar a otra persona o funcionario.
6. No debe instalar software como clientes de correos.

07. CUENTAS DE USUARIOS:

7.1. Todo funcionario de la SUBDERE, en cualquier calidad de contratación, posee credenciales de acceso para el ingreso a la red de SUBDERE, sistemas, Correo Electrónico. El Departamento de Informática asigna las credenciales de acceso, previa autorización por parte del Departamento de Recursos Humanos, vía expediente electrónico (SGDOC) con la información requerida para el ingreso y egreso de los funcionarios de SUBDERE, la información de la credencial es comunicada directamente al usuario y se devuelve el expediente al Departamento de Recursos Humanos.

7.2. De la password o clave secreta: Al momento de crear al usuario, se asigna una clave genérica por defecto. El funcionario está obligado en su primer ingreso a cambiarla por una clave de su conveniencia.

7.3. El Departamento de Informática de SUBDERE mantiene un sistema centralizado de credenciales, cada credencial tiene una vigencia 90 días, el sistema informa al funcionario cuando la contraseña está por vencer, si el funcionario la cambia se extiende por otros 90 días, el sistema no permitirá utilizar la misma credencial en el tiempo. De esta manera se obliga a los usuarios a que realicen este cambio de forma periódica para mantener una buena práctica sobre la seguridad de las cuentas.

7.4. En el evento que el usuario olvide su credencial de acceso, debe solicitar el cambio a la unidad de redes. El administrador cambiará a una nueva credencial genérica e informará al usuario, es responsabilidad del usuario cambiarla la primera vez que la use. El Departamento de Informática no tiene acceso a la password que utiliza el usuario, pudiendo cada usuario cambiarla por una nueva password.

En el caso que otro funcionario solicite el cambio de credencial, el Departamento de Informática denegará dicha solicitud, salvo que se cuente con la autorización formal del Jefe del funcionario, la solicitud debe ser realizada por correo, mesa de ayuda o expediente electrónico.

08. RESPALDO DE INFORMACIÓN. (A.12.03.01)

Es responsabilidad del Departamento de Informática de la SUBDERE tomar las acciones necesarias y pertinentes para resguardar los activos de información y generar las políticas, procedimientos y/o manuales que se encuentran en el documento denominado “Procedimiento de Respaldo de Información y Sistemas”. Este documento fue creado en el año 2011 y revisado con versiones posteriores, en este momento está actualizado al año 2016, y publicado en la intranet institucional.

La SUBDERE posee un espacio de almacenamiento para que los usuarios respalden la información de trabajo, para este objeto se implementó un volumen en la red para todos los usuarios que están en el dominio o red SUBDERE.
Este se encuentra etiquetado como volumen Z: (doble click en Mi Pc). En esta carpeta (Z:) los usuarios tendrán la responsabilidad de ingresar todos los documentos que son de importancia para su trabajo cotidiano.

El Departamento de Informática respaldará en forma periódica dicha carpeta, no obstante el usuario podrá pedir un respaldo de su información en medio magnético para su propio resguardo.

Será tarea de cada usuario respaldar en DVD ó CD la información respectiva. Para tal efecto cada PC posee un grabador de DVD para estas tareas y los equipos cuentan con un software para ayudar a respaldar, en caso de dudas se puede pedir ayuda al Departamento de Informática unidad de soporte vía mesa de ayuda.

Quedan excluidos todos los archivos del tipo mp3 o algún otro formato de música o imágenes, como fotografías y cualquier archivo que no sea de índole institucional. En esta instancia el usuario podrá identificar ante el Departamento de Informática si existe algún archivo de este tipo que no corresponda a música sino a una grabación de otra índole, en cuyo caso no se procederá a borrar este material.
La Unidad de Redes dentro de sus atribuciones generará periódicamente escaneos sobre estos volúmenes en busca de archivos con formatos que no correspondan.

Respecto a los respaldos de servidores, sistemas, bases de datos, carpeteas compartidas es responsabilidad del Departamento de Informática aplicar el procedimiento de respaldo vigente en ese documento se especifican la manera que es abordado este tópico de manera puntual.

09 SERVICIO DE NAVEGACIÓN WEB:

SUBDERE, entrega las herramientas necesarias para que los usuarios naveguen por internet a sitios nacionales o Internacionales en el marco de sus labores habituales.

9.1. El Departamento de Informática tiene como función monitorear el tráfico en red hacia y desde internet, en razón de la misión de velar por un buen servicio y la correcta utilización de la red por parte de los usuarios. Como resultado de este trabajo se pueden detectar situaciones donde se encuentre tráfico que supere los márgenes de bajada o subida de información, o tráfico anómalo. En tal evento se adoptan medidas para garantizar un servicio web expedito y disponible para toda la Subdere. En el caso de detectar uso inadecuado del servicio se procederá a tomar las siguientes medidas.

1.- Notificar la incidencia al usuario o responsable del sistema y usuario final.
2.- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.
3.-- Con el permiso del responsable de seguridad y la debida justificación, inspeccionar archivos o dispositivos de almacenamiento del usuario implicado.
4.- Informar a la Jefatura Superior del usuario sobre lo sucedido.

9.2. Una de las medidas que se adoptan es el bloqueo de sitios que presentan inseguridad y que no guardan relación con el trabajo de la SUBDERE o representan problemas de seguridad. Los sitios o páginas web bloqueadas por defecto son:

1.- Sitio que permiten streaming, música, radios y televisión en línea.
2.- Bajar y subir archivos a la red Internet (MEGA, jdownloader).
3.- Sitios del tipo P2P (Utorrent, FyerWayer).
4.- Ver Vídeos o televisión en línea o diferido.
5.- Juegos en Línea, ver pornografía.
6.- Sitios que permitan; Messenger, Chat, blogs, sitios de intercambio social, redes sociales
7.- Sitios que salten políticas de seguridad antes descritas.

9.3. En el evento que una página o sitio WEB esté bloqueada y el usuario requiera utilizarla de manera excepcional o permanente, el jefe directo del funcionario deberá solicitar al Jefe del Departamento de Informática, la asignación de un privilegio especial el cual será registrado convenientemente.

9.4. Está restringido el uso de radio, televisión u otros semejantes. Su uso se encuentra limitado de acuerdo a las funciones profesionales de cada funcionario con la finalidad de mantener expedito la utilización de internet, dado que el servicio de internet comparte un ancho de banda limitado por la simultaneidad de su uso por todos los funcionarios a nivel central y regional, siendo los enlaces internacionales los que tienen mayor costo y por ello son más limitados.

9.5. Si el Departamento de Informática identifica acciones no adecuadas a un usuario, tiene la facultad de restringir todo su acceso vía Web, situación que será notificado al Jefe de la División de Administración y Finanzas y al Jefe directo del funcionario.

10. SOPORTE Y SOFTWARE INSTALADO EN LOS EQUIPOS:

La SUBDERE entrega computadores de escritorio o notebook 100% operativos para las tareas cotidianas de los usuarios. La unidad de soporte del Departamento de Informática realiza entrega registrando en un acta el detalle de los bienes y software instalados.

Está prohibido que los usuarios o personas que NO pertenezcan al Departamento de Informática instalen software sin autorización. El Departamento de Informática en su tarea de monitoreo puede detectar software no licenciados, en ese caso se procederá a desinstalar dicho software en forma inmediata e informar a las respectivas jefaturas.

En el caso de requerirse la instalación de un software específico, la jefatura directa del funcionario deberá plantearlo al Jefe del Departamento de Informática para establecer si procede la petición.

10.1 De los Sistemas que Funcionan al interior del Servicio.
Los sistemas online que proporciona la SUBDERE pueden ser utilizados bajo las normas de navegación vía WEB, por lo tanto, estos pueden ejecutarse con el Browser FireFox, o Internet Explorer, Chrome.

11. TAREAS Y FUNCIONES DEL DEPARTAMENTO DE INFORMÁTICA:

Las principales funciones del Departamento de Informática son:

1.- Monitoreo constante del tráfico en la red nivel central y redes regionales.
2.- Administración y monitoreo del servicio de correo electrónico institucional.
3.- Administración y monitoreo del servicio de video conferencia.
4.- Soporte a usuarios en el ámbito informático en general.
5.- Soporte a usuarios respecto a la administración de servicio de telefonía. (Instalación, habilitación, cambios y registro de programación de teléfonos IP)
6.- Apoyar en uso de sistemas o sitios WEB que SUBDERE habilite o desarrolle.

11.1. Soporte de usuarios a nivel de Hardware y Software

El Hardware de la Subsecretaria (equipos físicos), en un alto porcentaje, se encuentran en arrendamiento, en especial, el equipamiento de escritorio (computadores). Es por ello que el Departamento de Informática opera como un soporte de primer nivel, en calidad de validador de un funcionamiento incorrecto, procediendo el encargado de la Unidad de Soporte informático a contactarse con la empresa prestadora del servicio y coordinara la visita para reparar el desperfecto.

12. POLÍTICAS DE SEGURIDAD SUBDERE:

12.1. Alcance y Campo de Aplicación

Este documento complementa las Políticas de Seguridad de la Información institucional vigente, según lo dispuesto en los respectivos decretos supremos e instructivos que forman el cuerpo jurídico donde se establecen normas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado.
Las exigencias y recomendaciones previstas en esta norma, tienen por finalidad garantizar estándares de seguridad en el uso, almacenamiento, acceso y distribución de los documentos electrónicos entre los órganos de la Administración del Estado. Se establecen las indicaciones respecto de los sistemas informáticos, con énfasis en el procedimiento de autorización, instalación o modificación de los sistemas; indicaciones y acciones desarrolladas de uso de red y otras normas.

12.2. EQUIPOS DE USUARIOS NO SUPERVISADOS. (A.11.02.08)

Todo equipo institucional se protege del uso no autorizado mediante el acceso de contraseña para el ingreso a la red de SUBDERE. Se cuenta con un servicio centralizado de credenciales de acceso donde se pueden generar políticas de seguridad de acceso a la red SUBDERE.

Sin perjuicio de lo anterior, todos los usuarios de SUBDERE deberán procurar que el equipo institucional asignado, cuando no esté supervisado o atendido, se mantenga bajo una protección adecuada.

Es responsabilidad del usuario finalizar las sesiones activas cuando concluya una actividad, salvo que maneje un mecanismo de protección si el equipo es desatendido.

Se recomienda que al moverse de su puesto de trabajo pulsar simultáneamente las teclas (Windows L) el equipo será bloqueado automáticamente.

Es obligación de los usuarios cerrar sesión en las aplicaciones o servicios de redes cuando no se requiera utilizarlos o deban alejarse de su puesto de trabajo.

No obstante y para mayor protección, el Departamento de Informática de SUBDERE para la implementación del control de seguridad entrega los equipos configurados para que de manera automática activen el modo hibernación en el caso que se encuentren inactivos.

12.3. POLITICAS DE ESCRTORIO DESPEJADO Y PANTALLA DESPEJADA. (A.11.02.09)

El contar con un escritorio despejado o limpio reduce el riesgo de acceso al personal no autorizado. Respecto a la pérdida o daño de la información, dentro o fuera de la jornada laboral, es crucial proteger la información institucional reservada.

En especial cuando las oficinas son visitadas por proveedores, consultores, clientes, personal de limpieza o compañeros de trabajo, para este caso, se considera como una buena práctica mantener su escritorio lo más limpio y organizado posible. Si está desordenado, es muy probable que usted no se dé cuenta de que falta algo. Se recomienda siempre guardar los documentos de importancia y en especial materiales de almacenamiento, como discos externos portátiles, pendrive, notebook, laptops, IPDAs, etc. en un lugar seguro en cajones bajo llave. En el caso que se utilice Notebook se recomienda asegurarlo físicamente con candados para evitar robos. Se recomienda como buena práctica el no publicar datos sensibles que pueden vulnerar su seguridad en el uso de PC, por ejemplo, nombre de usuario, passwords, direcciones IP, contratos.

Al finalizar la jornada de trabajo es obligación del usuario apagar el equipo asignado y tomar unos minutos para juntar y asegurar todo lo considerado como material sensible o reservado.

El funcionario no debe consumir alimentos o bebidas en los puestos de trabajo, dado el riesgo que involucra para los equipos y su información en el caso de derramar liquido en los dispositivos.

13. LAS CONSECUENCIAS DEL MAL USO DE LOS RECURSOS:

13.1. Los usuarios, cuando se les solicite, deben colaborar con los administradores de sistemas, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.

13.2. En el caso que los administradores de redes o sistemas (generales o locales) detecten un mal uso de los recursos informáticos o que se considere un riesgo de seguridad de la información o que infrinjan las normas legales vigentes, deben tomar las siguientes medidas para proteger el servicio y los otros funcionarios:

13.2.1. Suspender o restringir el acceso o uso de los servicios de manera inmediata mientras dure la investigación técnica que permita definir el alcance de la infracción. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.

13.2.2 Notificar la incidencia al usuario o responsable del sistema, informar las implicancias técnicas, jurídicas y/o administrativas. Con el permiso del responsable de seguridad, inspeccionar archivos o dispositivos de almacenamiento del usuario implicado, Informar a la Jefatura superior correspondiente de lo sucedido.

13.2.3. Los usuarios que sean sorprendidos en prácticas de navegación no acordes al trabajo, y/o tratando de vulnerar los dispositivos de seguridad de la institución para lograr accesos no autorizados, serán sancionados con la restricción total de navegación en su equipo (no incluye correo electrónico), previo informe al jefe directo del funcionario.

13.5. Medidas disciplinarias: en caso que fuera necesario, corresponderá al Jefe de Servicio la adopción de medidas disciplinarias, previo procedimiento administrativo, hacia los usuarios infractores de esta política, una vez informado por el Responsable de Seguridad y el Jefe del Departamento de Informática.

ARTÍCULO 3°.- Déjese sin efecto la resolución exenta N°14184/2016, de fecha 01/12/2016, de esta subsecretaría.

ARTÍCULO 4°.- La difusión de las políticas de Uso de los recursos Informático y de Infraestructura de Red de La Subsecretaría de Desarrollo Regional y Administrativo. Será de responsabilidad del Departamento de Informática de SUBDERE gestionar la difusión de estas políticas las que deben ser conocidas y acatadas por todos los funcionarios de la SUBDERE a quienes se les aplica, se utilizará para este medio Correo Masivos y la publicación del documento en la intranet Institucional.

ARTÍCULO 5°.- Control de versión
00 Febrero de 2010 versión inicial autorizada por resolución N°774/2010 de 20/02/2010.
01 Diciembre de 2011 actualizada resolución N°12574/2011 de 14/12/2011.
30 Julio de 2017 actualiza resolución N°14184/2016, de 01/12/2016, se revisa el 100% del documento.

Se incorporaron los siguientes puntos:

4. POLITICAS DE CONTROL DE ACCESO. (A.09.01.01)
4.1. ACESO A REDES Y SERVICIOS DE RED. (A.09.01.02)
4.2. RESPONSABILIDADDES DE LOS USUARIOS. (A.09.03.01)
12.6. EQUIPOS DE USUARIOS NO SUPERVISADOS. (A.11.02.08)
12.6. POLÍTICA DE ESCRITORIO DESPEJADO y PANTALLA DESPEJADA. (A.11.02.09)

Se eliminar los siguientes puntos:

12.4 Seguridad Acceso a Data Center.
12.5. Seguridad de Servicios Informáticos.
12.7. Seguridad de clima de Data Center.
12.8. Seguridad Respecto a la Energía Eléctrica.

Se sustituyeron los siguientes puntos:

Punto 4 “Políticas de Uso” por 4. POLITICAS DE CONTROL DE ACCESO: (09.01.01)
El título “POLITICA DE USO DE LOS RECURSOS INFORMÁTICOS E INFRAESTRUCTURA DE LA RED DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO” por “POLITICA GENERAL DE USO DE LOS RECURSOS INFORMÁTICOS DE LA SUBSECRETARÍA DE DESARROLLO REGIONAL Y ADMINISTRATIVO”

COMUNÍQUESE Y ANÓTESE

RICARDO CIFUENTES LILLO
Subsecretario
Gabinete

RCL/ / EJA/ NFF/ JAAB/ JOM/ AVO/ JHR/ RHR/ psj

DISTRIBUCION:
Jefe de Division - Division de Administración y Finanzas
Jefe Division - Division de Desarrollo Regional
Jefe Division - Division de Municipalidades
Jefe Division - Division de Politicas y Estudios
NIEVES DURAN - Jefa Unidad - Oficina de Partes, Archivo y Centro Documental
RICHARD HECTOR VILLARROEL - Asesor - Gabinete