POLÍTICA DE SEGURIDAD
SOBRE CONTROL DE ACCESO

Subsecretaría de Desarrollo Regional y Administrativo (SUBDERE)

Código	SSI.CA.00
Versión	4.0
Fecha Aprobación	06-10-2017
Elaborado por:	Rodrigo Zúñiga, Encargado de Seguridad de la Información
Aprobado por	Consejo de Calidad, Riesgos y Seguridad de la Información
Nivel de Clasificación	Uso Interno

INDICE

CONTROL DE VERSIONES

Historia e identificación de los Cambios				
Versión	**Fecha de Revisión**	**Motivo de la revisión**	**Páginas Modificadas**	**Autor**
1	26-12-2011	Formulación Inicial	Todas	Rodrigo Zúñiga
2	26-12-2012	Modificación de punto 5.1 Control de Acceso Físico (Se agrega mención explícita a la documentación en archivadores). Se actualizan documentos de referencia.	4	Rodrigo Zúñiga
3	17-11-2016	Aprobación por parte del Consejo de Calidad, Riesgos y Seguridad de la Información, de acuerdo a la nueva estructura del Sistema de Gestión Integrado.	1	Rodrigo Zúñiga
4	01-08-2017	Se incluye secciones 6, 7 y 8 sobre revisión, difusión y registros respectivamente. Se actualiza sección 3 Documentos de referencia: actualizando Norma NCh/ISO 27001, que correspondía a 27001:2009	1, 4, 6, 7	Rodrigo Zúñiga

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

		por NCh/ISO 27001:2013 y se actualizan puntos de acuerdo a la nueva norma; se reemplaza texto información de la Política de Seguridad de la Información vigente. Se agrega logo en la portada.		

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

1. Objetivo

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos del negocio y de seguridad.

2. Alcance

Este documento se aplica a todo el alcance del Sistema de gestión de seguridad de la información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

3. Documentos de Referencia

- Decreto 83, Ministerio Secretaria General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Resolución Exenta N°14185/2016. Aprueba Política de Seguridad de la Información de la Subsecretaría de Desarrollo Regional y Administrativo, en el marco del Sistema de Mejora de la Gestión.
- Norma NCh/ISO 27001:2013, puntos A.6.2.1, A.6.2.2, A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.3 y A.11.2.4

4. Definiciones

- Encargado de Seguridad: Funcionario responsable del desarrollo de políticas de seguridad en la institución, la coordinación en la respuesta a incidentes que afecten a los activos de información institucionales y establecer puntos de enlace con encargados de seguridad de otros organismos públicos.
- Encargado de Sistema Informático: Funcionario que es responsable técnico de un Sistema Informático, incluyendo la creación de respaldos, la revisión de los niveles de seguridad, mejoras, etc.
- Responsable de autorización de derechos de acceso: Funcionario responsable administrativo de un Sistema Informático, incluyendo la responsabilidad de asignar los privilegios de acceso, autorizar modificaciones, etc. Debiera ser un Jefe de Departamento o Unidad.

5. Control de Acceso

5.1. Control de Acceso Físico

5.1.1. Acceso a las instalaciones

Está permitido el acceso a todas las instalaciones de la organización, excepto a aquellas para las cuales el privilegio debe ser concedido por una persona autorizada (instalaciones con equipos de comunicación, procesamiento o almacenamiento de información, etc.). Se prohíbe también el acceso a oficinas sin la debida autorización de alguno de los funcionarios que la ocupan.

Las zonas de acceso restringido a las que se refiere el párrafo anterior deberán estar debidamente señaladas, excepto en el caso de las oficinas.

Debe existir una persona (rol o cargo) responsable de autorizar el acceso las instalaciones de acceso restringido.

Esto incluye el acceso a dependencias externas a la SUBDERE, que prestan servicios de almacenamiento de información, a las cuales se podrá acceder, en compañía de alguno de los responsables.

5.1.2. Control de Acceso a Archivadores y documentación

El acceso a la documentación almacenada en archivadores, está restringido excepto que haya sido autorizado por el encargado de la unidad responsable de la documentación.

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

5.2. Control de Acceso a Sistemas o Servicios Informáticos

En el acceso a todos los sistemas, servicios e información está prohibido salvo que sea expresamente permitido (como aquellos descritos en la sección 5.2.2) a usuarios individuales o a grupos de usuarios.

5.2.1. Perfiles de Usuario

Cada sistema o servicio deberá contar con documentación que indique los perfiles de usuario existentes, los cargos que tienen derecho de acceso respecto a cada perfil y las funciones que pueden realizar dichos perfiles en el sistema, de acuerdo a la *Ficha de Documentación de Control de Acceso a Sistemas Informáticos* que se encuentra en el Anexo 1.

La ficha mencionada deberá ser entregada por el Encargado del Sistema Informático al Encargado de Seguridad de la Información, para ser incorporado como documento anexo a la presente política (un ejemplo de los datos a ingresar en cada campo, de encuentra disponible en el Anexo 2). En caso de no existir dicha documentación, los encargados de cada sistema informático deberán generarla en plazos acordados con el Encargado de Seguridad de la Información, estos plazos no podrán exceder de un año, luego de la fecha de aprobación de la presente política.

Esto es aplicable tanto para los sistemas o servicios internos de SUBDERE como para aquellos ofrecidos a terceros (Gobiernos Regionales, Municipios, etc.)

5.2.2. Uso de los servicios de SUBDERE

Los funcionarios de SUBDERE pueden, desde el momento de su incorporación a la institución, acceder a los siguientes sistemas o servicios:

- Navegación Web
- Correo electrónico
- Sistema de Gestión Documental
- Sistema de Cometidos
- Sistema de Liquidaciones de Sueldo
- Intranet
- Sistema de Evaluación de Desempeño
- Horario Online
- Servidor de Archivos NAS y uso de carpetas compartidas

Para cualquier otro sistema o servicio dentro de la Institución, el funcionario deberá ser autorizado de acuerdo a lo establecido en la sección 5.2.3.

Los usuarios no pueden acceder a sistemas o servicios para los cuales no cuentan con autorización.

5.2.3. Gestión de Privilegios

Debe existir una persona (rol o cargo) responsable de autorizar la concesión o eliminación de privilegios o derechos de acceso para los sistemas o servicios. La cual debe ser indicada en la *Ficha de Documentación de Control de Acceso a Sistemas Informáticos* que se encuentra en el Anexo 1

Al asignar privilegios, la persona responsable debe tener en cuenta los requerimientos de negocio y de seguridad para el acceso, como también la clasificación de la información a la que se accede con esos derechos de acceso. Deberá existir un registro de aquellos privilegios entregados a funcionarios o terceras partes.

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

El Responsable de la autorización de los derechos de acceso debiera ser el Jefe de Departamento o Unidad Responsable del sistema, o un Dueño de Proceso identificado, el cual deberá indicar a los responsables técnicos del sistema (o Encargado de Sistema Informático) la asignación de los privilegios otorgados al usuario.

Esto es aplicable tanto para los sistemas o servicios internos de SUBDERE como para aquellos ofrecidos a terceros (Gobiernos Regionales, Municipios, etc.)

5.2.4. Revisión periódica de los derechos de acceso

Los propietarios de cada sistema o servicio deben, según los intervalos definidos en la *Ficha de Documentación de Control de Acceso a Sistemas Informáticos* que se encuentra en el Anexo 1, revisar si los derechos de acceso concedidos se mantienen de acuerdo a los requerimientos de negocios y de seguridad.

Cada revisión debe ser registrada e informada al encargado de Seguridad de la información, quien deberá mantener un registro de dichas actividades.

Esto es aplicable tanto para los sistemas o servicios internos de SUBDERE como para aquellos ofrecidos a terceros (Gobiernos Regionales, Municipios, etc.)

5.2.5. Cambios de estado

Cuando se produce un cambio o finalización de empleo, el Departamento de Recursos Humanos debe informar inmediatamente al Departamento de Informática, quién a su vez informará a los encargados de sistemas o a quien autorizó los privilegios del funcionario en cuestión.

Cuando se modifican las relaciones contractuales con entidades externas que tienen acceso a sistemas o servicios, o cuando finaliza el contrato, el encargado del sistema o servicio debe gestionar de forma inmediata la revocación de los permisos de acceso.

Las personas autorizadas de asignar los privilegios, en esos casos, deben exigir, cuanto antes, la modificación o eliminación de los derechos de acceso.

En el caso de aquellos servicios o sistemas utilizados por entidades externas (diferentes a los proveedores con los que existe un contrato de por medio) como Gobiernos Regionales o Municipios, en que el Responsable de la autorización de derechos de acceso, o el Encargado de Sistema o servicio, no puedan contar con la información al momento del cambio de estado, ésta deberá solicitarse al menos como parte de la revisión periódica de derechos de acceso.

5.3. Control de Acceso Remoto

En general, SUBDERE no provee acceso a sus Sistemas Internos desde fuera de su red, exceptuando el caso del correo electrónico, y el acceso otorgado en casos particulares mediante medios seguros, como Red Privada Virtual (VPN, por sus siglas en inglés).

En el caso de aquellos sistemas o servicios destinados a usuarios externos a la Institución, éstos se encuentran disponibles a través de Internet. Será responsabilidad de los Encargados de Dichos Sistemas de información, la aplicación de los medios de seguridad necesarios para proteger la información almacenada en ellos.

5.3.1. Acceso Remoto a Funcionarios

Aquellos funcionarios que requieran acceso remoto a los servicios de SUBDERE que sólo se encuentran disponibles en la red Interna, deberán solicitarlo al Jefe del Departamento de Informática justificando el motivo de la solicitud. El Jefe del Departamento de Informática podrá aprobar, rechazar o solicitar más antecedentes respecto de la solicitud. El acceso puede ser VPN para funcionarios en general o vía SSH (abreviación de Secure Shell, es un protocolo, y el programa que lo implementa, que permite acceder a maquinas remotas a través de una red), en el caso de los funcionarios que ejercen funciones relacionadas con Tecnologías de Información.

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

En caso de aprobar la solicitud, será responsabilidad del Administrador de la Red la generación de las credenciales de acceso, las cuales deberán ser entregadas de forma presencial al funcionario.

En el caso de los accesos vía VPN, será responsabilidad de la Unidad de Soporte la configuración de la misma en el equipo móvil (laptop, netbook, etc.) que utilizará el funcionario, así como de informar al usuario de las medidas de seguridad y buenas prácticas al ingresar a la red interna desde fuera de las instalaciones de la Institución.

Será responsabilidad del Departamento de Informática difundir e informar a los funcionarios que tengan acceso remoto a los sistemas y servicios de SUBDERE, de las medidas de seguridad que estos deben tener al realizar actividades de trabajo desde fuera de las dependencias de la Institución. Estas medidas de seguridad deberán incluir al menos las descritas en el Anexo 3 *Seguridad del Trabajo Remoto* y aplican tanto para los sistemas y servicios disponibles a través de Internet, como aquellos privados a los que se haya otorgado acceso especial (vía VPN o SSH).

Será responsabilidad de los funcionarios que tengan acceso a los sistemas o servicios de SUBDERE, el cumplimiento de las medidas de seguridad indicadas por el Departamento de Informática.

5.3.2. Computación Móvil

Será responsabilidad del Departamento de Informática difundir e informar a los funcionarios que tengan acceso a equipos móviles de la institución, de las medidas de seguridad que estos deben tomar al utilizar dichos dispositivos. Estas medidas de seguridad deberán incluir al menos las descritas en el Anexo 4. *Seguridad de los dispositivos móviles*.

Será responsabilidad de los funcionarios que tengan acceso a los dispositivos móviles, el cumplimiento de las medidas de seguridad indicadas por el departamento de Informática.

5.3.3. Acceso Remoto a Proveedores

En caso de que terceros (proveedores, consultores, etc.), por motivos de desarrollo, mantención, soporte o auditoría, tanto de sistemas, servicios, servidores o infraestructura de red, requieran acceso remoto a servidores de SUBDERE, el funcionario de SUBDERE que tenga a cargo el contrato con el tercero, deberá solicitarlo mediante la jefatura respectiva al Jefe del Departamento de Informática, quien podrá aprobar, rechazar o solicitar más antecedentes respecto de la solicitud.

En caso de aprobar la solicitud, será responsabilidad del Administrador de la Red la generación de las credenciales de acceso, quien las deberá comunicar de forma presencial al tercero en cuestión, salvo que esto no sea posible, podrán ser entregadas vía telefónica. El Administrador de Red también será responsable de que los derechos de acceso asignados sean estrictos y no permitan realizar actividades más allá que de las requeridas para el desempeño de las funciones requeridas.

Será responsabilidad de quien tenga a cargo el contrato con el tercero involucrado, informar al Departamento de Informática, la finalización del mismo, para la revocación de los derechos de acceso.

6. Revisión del presente documento

La presente política, deberá ser revisada y de ser necesario actualizada al menos una vez cada 2 años, o cuando ocurran cambios que pudieran afectar el enfoque de la Subsecretaría para la gestión de la Seguridad de la Información en relación al control de acceso físico y/o lógico.

7. Difusión

La Difusión de la presente política será responsabilidad de los departamentos de Administración e Informática de SUBDERE en relación al acceso físico y lógico respectivamente, quienes realizaran todas las gestiones y

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

acciones que requiera esta política, la que debe ser conocida y asumida por todos los funcionarios de la SUBDERE a quienes aplica.

El mecanismo de difusión a utilizar corresponderá a notificación vía correo electrónico y la publicación del presente documento en la intranet Institucional.

8. Gestión de registros guardados en base a este documento

Nombre del registro	Responsable	Tiempo	Medio de Soporte	Lugar	Disposición
Ficha de Documentación de Control de Acceso a Sistemas Informáticos	Encargado de la Unidad TI a cargo del sistema	Permanente	Digital	Carpeta con documentación de la Unidad TI a cargo del sistema	Permanente

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

Anexo 1. Ficha de Documentación de Control de Acceso a Sistemas Informáticos

Nombre del sistema (si es web, incluir la url)	
Tipo de Sistema(tipo de usuarios a los que presta servicios)	[ ] Interno (los usuarios son solo funcionarios de SUBDERE) [ ] Interno-Externo (funcionarios SUBDERE y externos, ej.: GORES, Municipios, etc.) [ ] Externo (sólo usuarios externos ej.: Municipios, ciudadanos en general, etc.)
Rol autorizado a conceder o eliminar derechos de acceso	
Periodicidad de la Revisión de derechos de acceso	
Fecha de Revisión de la presente ficha	

Perfil de Usuario	***Cargos Asociados***	***Permisos***

Método de implementación técnica de control de acceso	

Observaciones	

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

Anexo 2. Ejemplo de llenado de Ficha de Documentación de Control de Acceso a Sistemas Informáticos

Nombre del sistema (si es web, incluir la url)	[ejemplo: Sistema de evaluación del Desempeño (http://sed.subdere.gov.cl)]
Tipo de Sistema(tipo de usuarios a los que presta servicios)	[x] Interno (los usuarios son solo funcionarios de SUBDERE) [ ] Interno-Externo (funcionarios SUBDERE y externos, ej.: GORES, Municipios, etc.) [ ] Externo (sólo usuarios externos ej.: Municipios, ciudadanos en general, etc.)
Rol autorizado a conceder o eliminar derechos de acceso	[Jefe de Departamento de RRHH]
Periodicidad de la Revisión de derechos de acceso	ejemplo: Cada periodo de evaluación: -Primera Evaluación de Desempeño [marzo] -Segunda Evaluación de Desempeño [agosto] -Pre- Calificación [septiembre] -Calificación [septiembre] -Evaluación de honorarios [noviembre]
Fecha de Revisión de la presente ficha	[01-12-2011]

Perfil de Usuario	***Cargos Asociados***	***Permisos***
[Administrador]	[Funcionario Responsable del Proceso de Evaluación del desempeño]	• Gestión (Crear, Ver, Modificar , Eliminar) de periodos de calificación (Primera y Segunda Evaluación, Pre-Calificación, Calificación y Evaluación de honorarios) • Asignar Evaluadores y Pre-Calificadores
[Evaluador]	[Jefes de Unidades de Desempeño]	• Evaluar funcionarios, tanto en la Primera y Segunda Evaluación, Pre- Calificación y Evaluación de honorarios.
…	…	…

Método de implementación técnica de control de acceso	[Ejemplo:] • Nombre de usuario y contraseña • Token con clave dinámica sincrónica • Firma electrónica avanzada • etc.

Observaciones	[ej.: Sistema sólo disponible desde la red interna de SUBDERE.]

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional

Anexo 3. Seguridad del Trabajo Remoto

El Trabajo Remoto significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización, esto incluye el acceso a herramientas o servicios públicos como el correo electrónico o el acceso a sistemas mediante accesos especiales como VPN.

Al realizar actividades de trabajo desde fuera de la Institución, se deben tener presente las siguientes recomendaciones:

- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de Trabajo Remoto.
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Procurar no realizar actividades prohibidas por las normas o políticas de la institución.

Anexo 4. Seguridad de los dispositivos móviles

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento y procesamiento de datos.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil que contiene información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Se debe evitar la conexión de los equipos móviles a redes públicas, ya que la información transmitida podría ser vista por otros usuarios (incluyendo claves de acceso, correos electrónicos, etc.)

Este documento es de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a la Intranet Institucional