Servicio Nacional del Consumidor
Ministerio de Economía, Fomento y Turismo

RESOLUCIÓN EXENTA N°

SANTIAGO,

APRUEBA PROCEDIMIENTO DE GESTIÓN Y CONTROL DE ACCESOS LÓGICOS DEL SERVICIO NACIONAL DEL CONSUMIDOR VERSIÓN 4.0.

VISTOS:

Lo dispuesto en el Decreto con Fuerza de Ley N°1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley Nº18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N°19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; el Título VI del Decreto con Fuerza de Ley N° 3, de 2019, del Ministerio de Economía, Fomento y Turismo, que fija el texto refundido, coordinado y sistematizado de la Ley Nº19.496 sobre Protección de los Derechos de los Consumidores, que establece las funciones del Servicio Nacional del Consumidor; la Resolución Exenta N° 215, de fecha 31 de marzo de 2023, que establece la jerarquía documental y los circuitos de aprobación de los mismos; el Decreto N° 91 de 2022 del Ministerio de Economía, Fomento y Turismo, que nombra a Andrés Herrera Troncoso como Director Nacional del Servicio Nacional del Consumidor; la Resolución N°7 de 2019 de la Contraloría General de la República, y

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

CONSIDERANDO:

1. Que, durante agosto de 2023, el Departamento de Tecnología e Informática actualizó el Procedimiento de Gestión y Control de Accesos Lógicos, generando la versión 4.0 del mismo, con la finalidad de establecer las definiciones que regulan el acceso a los medios compartidos de información del Servicio Nacional del Consumidor, en adelante "SERNAC", en términos de autenticación, autorización y trazabilidad, junto con reducir posibles accesos o modificaciones por parte de personas o usuario/as no autorizados/as, y que pongan en riesgo la continuidad operacional del Servicio.

2. Que, el término procedimiento, de acuerdo a la definición entregada en la Resolución Exenta N° 215, de fecha 31 de marzo de 2023, que **"Establece la Jerarquía Documental y Aprueba Circuitos de Aprobación"**, es un instrumento que describe las actividades consecutivas de un proceso, subproceso o parte de éstos, que conllevan un orden lógico de interrelación, identificando responsables de la ejecución de cada una de ellas. El procedimiento según está definición se aprueba a través de Resolución Exenta.

3. Que, de acuerdo a la resolución señalada en el considerando precedente, los procedimientos serán sometidos a una revisión de calidad por parte de la Unidad de Control de Gestión y Mejora de Procesos, después de lo cuál deberán someterse al control de legalidad de la Fiscalía Administrativa, la que los remitirá al Subdirector correspondiente, y en caso que no corresponda a una Subdirección o División, deberán ser remitidos a la Dirección Nacional, para su aprobación mediante Resolución Exenta.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

4. Que, el artículo 3 de la Ley N°19.880, que Establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado, dispone que las decisiones escritas que adopte la Administración se expresarán por medio de actos administrativos.

5. Que, de conformidad a lo anterior, por medio de la Resolución Exenta N° 160, de 25 de febrero de 2022, de SERNAC, fue aprobado el Procedimiento para la gestión y control de accesos lógicos de este Servicio en su versión 3.0, el cual debe ser dejado sin efecto, dado que es necesario incorporar la modificación consistente en que los accesos deban ser revisados y actualizados con una frecuencia de 6 meses, por consiguiente por medio del acto administrativo que se aprueba, se añade dicha periodicidad. Así las cosas, por medio del presente acto administrativo, se aprobará una nueva versión del procedimiento antedicho.

6. Las facultades que la ley confiere al Director Nacional.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

RESUELVO:

1° DÉJASE SIN EFECTO la Resolución Exenta N° 160, de fecha 25 de febrero de 2022.

2° APRUÉBASE el Procedimiento de Gestión y Control de Accesos Lógicos versión 4.0, cuyo texto se transcribe a continuación:

1. Presentación del documento

A continuación se presentan los elementos introductorios del presente documento:

Proceso / subproceso	Gestión TI
Propósito	Establecer las definiciones que regulan el acceso a los medios compartidos de información del SERNAC, en términos de autenticación, autorización y trazabilidad. Esto, con la finalidad de reducir posibles accesos o modificaciones por parte de personas o usuario/as no autorizadas, y que pongan en riesgo la continuidad operacional del Servicio. Asimismo, este procedimiento permite dar cumplimiento a las disposiciones de los controles A.09.01.02, A.09.02.01, A.09.02.02, A.09.02.03, A.09.02.04, A.09.02.05, A.09.02.06, A.09.03.01 y A.09.04.01, sobre "Accesos a las redes y a los servicios de la red", "Registro y cancelación de registro de usuario", "Asignación de acceso de usuario", "Gestión de derechos de acceso privilegiados", "Gestión de información secreta de autenticación de usuarios", "Revisión de los derechos de acceso de usuario", "Eliminación o ajuste de los derechos de acceso", "Uso de información de autenticación secreta" y "Restricción de acceso a la información", respectivamente; de la NCh-ISO 27001.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

Alcance	Este procedimiento es aplicable a todas las personas funcionarias, independiente de su calidad jurídica, así como también, incluye a pasantes, practicantes y/o cualquier persona que tenga asignado un acceso lógico independiente de la plataforma tecnológica a la que acceda, esto también incluye cuentas genéricas asignadas a personas y/o a terceros relacionados con el Servicio. Además de todos los recursos tecnológicos e información que se encuentre contenida en ellos, tales como: carpetas y/o archivos contenidos en Google Drive, base de datos de los sistemas y aplicaciones, sistemas y aplicaciones tecnológicas, servidores, servicios, etc.
Responsables	Unidad Continuidad Operativa TI (en adelante "UCOTI"), Encargado/a de Ciberseguridad. Oficial de Seguridad de la Información. Responsable o Propietario del Activo de Información. Funcionarios y funcionarias del SERNAC. Practicantes, pasantes, terceros relacionados, y/o cualquier persona con acceso lógicos. Jefaturas y/o Coordinadores/as. Funcionarios/as requirentes.
Formato utilizado	Procedimiento versión 3.0

2. Índice

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

3. Descripción de Actividades

1. Control de acceso a la información

N°	Actividad	Descripción	Responsable
1.1	Definición de Perfiles de Usuario	El Jefe/a de la Unidad Continuidad Operativa TI, a través del Administrador/a de Base de Datos, Administrador de Plataformas y/o Administrador/a de Redes y Sistemas (según sea el caso y el perfil a asignar) y en conjunto con el Propietario de Activo de Información, deberá definir Perfiles de Usuario, que establezcan niveles de acceso a la información y su procesamiento, de acuerdo a necesidades de acceso lógico que determinen las respectivas jefaturas, en función de las tareas asignadas al cargo del funcionario.	Jefe/a Unidad Continuidad Operativa TI Administrador/a de Bases de Datos Administrador/a de Plataformas Administrador/a de Redes y Sistemas Propietario de Activo de Información
1.2	Autorización de Acceso	Para todo medio de procesamiento de información al que se necesite conceder accesos lógicos (por ejemplo: servidores, sistemas de información y aplicaciones, unidades compartidas de Google Drive, etc.), el Propietario del Activo de Información, deberá designar un responsable del recurso a compartir.	Propietario de Activo de Información Funcionarios y funcionarias propietarios de los datos

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		Para conceder permiso a terceros (externos a SERNAC)[1], debe existir una solicitud de la unidad solicitante y un documento firmado de confidencialidad de la información. Además, dicha solicitud debe ser elevada y aprobada por el Oficial de Seguridad de la Información y el Propietario del Activo de Información. Dicha solicitud, debe ser adjuntada en el ticket de Mesa de Ayuda TI solicitado para este requerimiento. Por tanto, ninguna solicitud debe ser enviada por correo, siendo el único medio la Mesa de Ayuda TI. Se excluye de este punto "Mi Unidad" de Google DRIVE asignada a cada funcionario/a, pasante, practicante, o cualquier correo electrónico genérico asignado a una persona, ya que, los permisos en aquellas carpetas y archivos es de absoluta responsabilidad de quién comparte. Esto es, al ser una herramienta colaborativa, se encuentra disponible la opción de compartir con personas de SERNAC y/o externo. Para el caso de compartir carpetas y/o archivos desde "Mi Unidad", el usuario/a debe compartir solamente a cuentas de correo electrónico conocidas evitando en todo momento dejar la información con libre	

[1] Documento de acuerdo de confidencialidad y no divulgación disponible en: https://docs.google.com/document/d/1j-hyXWxI_k-rwtF8l0N1iIODHb_t1A4c2qCH0_ZIGoQ/edit#>

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		acceso, a excepción que esta sea información accesible a cualquier personas, como por ejemplo, una encuesta.	
1.3	Accesos no autorizados	La Jefatura de la Unidad de Continuidad Operativa TI tiene las facultades de suspender o eliminar los accesos a cualquier persona que signifique riesgo en la confidencialidad, integridad o disponibilidad de la información y deberá comunicarlo al Encargado de Ciberseguridad y al Oficial de Seguridad de la Información, para su tratamiento y eventual sanción. Esto incluye a "Mi unidad" en Google Drive de cualquier funcionario y funcionaria, cuenta de pasantes y/o prácticas profesionales y/o cualquier cuenta genérica asignadas a personas, donde la Jefatura de la Unidad de Continuidad TI tiene la facultad de quitar dichos permisos si estos ponen en riesgo a la seguridad del Servicio. Dichos permisos mal ejecutados, pueden ser informados por cualquier funcionario o funcionaria, por Auditorías Internas, por revisiones de la Mesa de Ayuda, o por cualquier persona involucrada con dicha información.	Jefatura Unidad Continuidad Operativa TI Oficial de Seguridad de la Información Encargado de Ciberseguridad Funcionarios/as requirentes Jefaturas y/o Coordinadores/as

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		Cualquier intento de acceso que no esté autorizado, ya sea a equipos, servidores, aplicaciones, unidades compartidas de Google Drive u otra información, será considerado como una falta grave, por lo que debe reportarse de inmediato al Encargado de Ciberseguridad y al Oficial de Seguridad de la Información y a las jefaturas inmediatas. Si la falta es considerada como un atentado a la integridad, confidencialidad y disponibilidad de los activos de información de la institución, ya sea en menor o mayor grado, se procederá a investigar dentro del marco del estatuto administrativo y se aplicarán las sanciones administrativas que correspondan, sin perjuicio de las denuncias penales o demandas civiles que procedan por la vía judicial.	

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

2. Administración de accesos lógicos

N°	Actividad	Descripción	Responsable
2.1	Proceso de alta de personas usuarias	El/la funcionario/a requirente solicitará acceso lógico a un Activo de Información, a través de un requerimiento efectuado a la Mesa de Ayuda TI (ticket). La Jefatura de la Unidad Continuidad Operativa TI deberá aprobar o rechazar las solicitudes que hayan sido escaladas, previa consulta al Propietario del Activo de Información, esta consulta no deberá superar las 48 horas desde la solicitud. La Mesa de Ayuda TI gestionará el requerimiento y analizará si requiere nivel de escalamiento o tratamiento inmediato, una vez asignado como observador al administrador/a de plataformas correspondiente. El/la Administrador/a de plataformas tendrá la responsabilidad de asignar un determinado perfil de acceso al Usuario Requirente, en base a los requerimientos de la unidad que lo solicite y lo indicado por el propietario del activo.	Funcionarios/as requirentes Agentes Mesa de Ayuda TI Jefe/a Unidad Continuidad Operativa TI Propietario de Activo de Información

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		Una vez aprobada la implementación, el Agente de la Mesa de Ayuda TI, según corresponda, deberá notificar al solicitante que su solicitud ha sido implementada o que se ha desestimado, y los motivos, esta información estará contenida en el mismo ticket, y el plazo para informar no deberá superar las 48 horas desde que se tiene una respuesta del Propietario del Activo de Información.	
2.2	Solicitud de usuarios nuevos	Cuando ingresen nuevos usuarios a la institución, se procederá a la asignación de equipamiento (PC o Notebook, según corresponda), un Agente de la Mesa de Ayuda TI realizará el perfilamiento de dicho equipo según las características de la solicitud, concediendo los privilegios de acceso lógico necesarios para la realización de sus tareas. El Administrador/a de Redes y Sistemas, según corresponda, dará acceso lógico a Activos de Información, según indique el requerimiento en base a un perfil de usuario ya definido. Los accesos iniciales para cualquier usuario nuevo son: Cuenta de correo, cuenta de dominio, cuenta de control de asistencia.	Administrador/a de Redes y Sistemas Agentes Mesa de Ayuda TI Administrador/a de plataformas

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
2.3	Solicitud de modificación para usuarios y usuarias por movimiento interno	En caso de modificación de perfiles de usuarios existentes en la institución, si requiere revocación y/o asignación de nuevos permisos de acceso, se debe levantar la solicitud según lo señalado en la actividad 4 "Proceso de alta de usuarios". Las modificaciones deberán ser implementadas por el Administrador/a de Redes y Sistemas y/o Administradores/as de Plataformas, según corresponda, dicha actividad no debe superar las 48 horas desde el plazo establecido en la solicitud. Será responsabilidad del Departamento de Personas levantar el ticket en la mesa de ayuda, solicitando movimiento interno, para, la revocación de los acceso a sistemas, esto ya sea por motivo de cese del cargo o nuevas funciones. Lo anterior se comprenderá entre las actividades asociadas a la entrega del cargo.	Funcionarios/as requirentes Agentes Mesa de Ayuda TI Propietario de Activo de Información Administrador/a de Redes y Sistemas Departamento de Personas Administradoras/es de Plataformas

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

3. Otorgamiento de accesos especiales y/o privilegiados

N°	Actividad	Descripción	Responsable
3.1	Acceso a Base Datos, aplicaciones especializadas, Información de alto nivel u otros	La solicitud de acceso a bases de datos, aplicaciones especializadas, información de alto nivel u otros, por parte usuarios no pertenecientes a la Dirección Nacional, Unidad de Desarrollo TI, Unidad Continuidad Operativa TI, deberá ser levantada por la Jefatura solicitante, a través de una solicitud a la Mesa de Ayuda TI, quien lo comunicará a la Jefatura de la Unidad Continuidad Operativa TI. La Jefatura de la Unidad Continuidad Operativa TI deberá pedir justificación de la solicitud y la temporización del acceso, para gestionar su aprobación o rechazo con el Propietario del Activo de Información y del Subdirector que corresponda, dicha gestión se debe dar en un marco de 48 horas, independiente las autorizaciones puedan superar ese plazo. De ser aprobada, se procederá a derivar al Administrador/a de Redes y Sistemas su gestión, quién habilitará una cuenta de usuario especial que cuente con los privilegios especiales solicitados, una vez autorizado los accesos, se dispondrá de 48 horas para su implementación, evitando así que se mezclen las labores cotidianas con los permisos especiales solicitados	Jefatura de la Unidad solicitante Jefe/a Unidad Continuidad Operativa TI Administrador/a de Redes y Sistemas

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		de forma temporal, cumpliendo de esta forma lo solicitado por la norma. Se solicitará que el usuario que reciba este acceso temporal, notifique y firme un documento de confidencialidad y conformidad de accesos.	

4. Revisión y revocación de accesos

N°	Actividad	Descripción	Responsable
4.1	Revisión	Los Propietarios de los activos de información son los responsables finales de la operatividad de los privilegios de acceso a las fuentes de información de la institución, por lo que deberá revisar los derechos de acceso: • Después de cambios o movimientos internos en la institución, que afecten permisos de usuarios/as sobre dichos sistemas. • Las cuentas y permisos, se revisarán cada 6 meses a solicitud del Administrador de Plataformas, a través de una solicitud por mesa de ayuda, en donde se entregará planilla con los usuarios y usuarias existentes, revisión que se realizará en conjunto entre el Administrador de Plataformas y el propietario del activo, con la finalidad que sólo existan	Propietarios de los activos de información Jefe/a Unidad Continuidad Operativa TI Administradores/as de plataformas

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		usuarios/as vigentes y con sus correspondientes servicios. Esto, de acuerdo a especificaciones y solicitudes que realice el Jefe/a de la Unidad Continuidad Operativa TI, quien es el responsable de verificar el cumplimiento de la revisión periódica de los accesos lógicos otorgados. Dicha solicitud se pedirá por ticket de Mesa de Ayuda TI, esto para ir actualizando los distintos perfiles. La respuesta debe ser entregada a través del ticket a la Jefatura de la Unidad Continuidad Operativa TI, esto es, por la confidencialidad de los datos.	
4.2	Revocación	Cuando el funcionario/a, pasante o personal externo, termina su relación laboral con SERNAC, por cualquiera que fuera el motivo, todos los permisos asignados a su acceso deben ser revocados. Es responsabilidad de la Unidad de Gestión del Personal informar oportuna y formalmente las desvinculaciones, para poder hacer valer las normas de seguridad de la información. Dicha notificación deberá ser enviada a través de un ticket en la Mesa de Ayuda TI, este puede ser	Funcionarios y funcionarias de la Unidad de Gestión del Personal Mesa de Ayuda TI Administrador/a de Plataformas. Administrador/a de Redes y Sistemas Jefe/a Unidad Continuidad Operativa TI

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		dirigido desde cualquier funcionario/a de la Unidad de Gestión del Personal. Una vez recibido el requerimiento en la Mesa de Ayuda TI, se debe incluir al administrador de plataformas, al administrador de redes y sistemas, y a un agente de mesa de ayuda TI, para de esta forma asegurar la correcta limpieza de todas las plataformas en donde pudiera contenerse una cuenta asociada al funcionario o funcionaria, pasante o personal externo desvinculado del Servicio o que haya renunciado. Para asegurar que la revisión se realiza de forma correcta, en el ticket, se deberá registrar que la persona fue debidamente eliminada del o los sistemas. Por tanto, en el caso de que la persona o cuenta no exista en el sistema, de igual forma debe informar indicando la no existencia de esta, esto para dejar registro de la actividad, esta revocación debe ser realizada de forma inmediata y no superando un día desde el aviso o asignación del ticket.	Agentes de Mesa de Ayuda TI

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
4.3	Revocación de accesos a proveedores o terceros relacionados.	Es responsabilidad del Propietario de los activos de información, notificar formalmente el término de contrato y/o servicio de algún proveedor o tercero relacionado con accesos a los sistemas dentro del mismo día hábil de término del contrato y/o servicio, para poder hacer valer las normas de seguridad de la información. Dicha notificación deberá ser enviada a través de un ticket en la Mesa de Ayuda TI, este debe ser dirigido por el Propietario del Activo que solicita la baja de la cuenta asociada. Una vez recibido el requerimiento en la Mesa de Ayuda TI, se debe incluir al administrador de plataformas, al administrador de redes y sistemas, y a un agente de mesa de ayuda TI, para de esta forma asegurar la correcta limpieza de todas las plataformas en donde pudiera contenerse una cuenta asociada al proveedor o al tercero relacionado a dar de baja. Para asegurar que la revisión se realiza de forma correcta, en el ticket, se deberá registrar que la persona y/o empresa fue debidamente eliminada del o los sistemas. Por tanto, en el caso de que la persona y/o empresa no exista en el sistema, de igual forma debe informar indicando la no existencia de esta, esto para dejar registro de la actividad.	Propietarios de los activos de información Agentes de Mesa de Ayuda TI Mesa de Ayuda TI Administrador/a de Redes y Sistemas Administrador/a de Plataformas.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

N°	Actividad	Descripción	Responsable
		Esta revocación debe ser realizada de forma inmediata y no superando un día desde el aviso o asignación del ticket.	

4. Registros de calidad

Nombre Registro	Almacenado por	Tiempo de Retención	Medio de soporte	Lugar de almacenamiento	Disposición Final
Ticket Mesa de Ayuda TI	Plataforma Mesa de Ayuda	Indefinido	Digital	Plataforma Mesa de Ayuda	Histórico
Documento de confidencialidad firmado	Unidad Continuidad Operativa TI	Indefinido	Digital	Google Drive	Histórico

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

5. Definiciones de conceptos

Concepto	Definición
Activo de Información	Activo que tiene valor para la institución y que, por tanto, debe protegerse.
Acceso a funcionarios/as a activos de información	Acceso de funcionarios/as a la información que necesitan para el desarrollo legítimo de sus funciones y actividades dentro de la Institución, de acuerdo a privilegios y accesos basados en las necesidades de las áreas y aprobadas por el propietario de los activos.
Acceso lógico	Acceso a recursos tecnológicos, a través de claves de ingreso, elaboradas bajo lenguaje de programación.
Control de acceso lógico	Consiste en la verificación de si una entidad (persona, sistema, servidor, etc.) que solicita acceso lógico a un recurso tecnológico (sistemas, dispositivos, bases de datos, comunicaciones, etc.), tiene los derechos necesarios para hacerlo, en términos de autenticación, autorización y trazabilidad. Con esto, se debe permitir únicamente el ingreso a los usuarios debidamente autorizados.
Requerimiento de acceso lógico	Solicitud, a través de ticket a la Mesa de Ayuda TI, que recibe la Unidad Continuidad Operativa TI, para permitir acceso lógico permanente, eventual o por períodos de tiempo, a las redes, sistemas y bases de datos que contengan activos de información de la institución.
Requerimiento de acceso lógico de terceros	Requerimiento de acceso que involucra a personas o entidades externas al SERNAC.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

6. Consideraciones

- Los centros de responsabilidad que tienen activos de información a su cargo, en donde sean propietarios de los activos de información, deben ceñirse a este procedimiento, con el fin de solicitar y registrar las autorizaciones correspondientes.

- Información mínima a incorporar en el requerimiento a Mesa de Ayuda, según el tipo de solicitud:

  a. **Solicitudes de acceso lógico:** Los requerimientos o solicitudes de acceso lógico, deberán ser siempre a través de la Plataforma de Mesa de Ayuda TI y contener, a lo menos, la siguiente información:

     i. Nombre del equipo solicitante y la jefatura o coordinador/a.
     ii. Nombre completo del usuario requirente.
     iii. Detallar requerimiento de acceso lógico y/o indicar perfil de usuario a asignar. Esto es, sistema de información o aplicación al que necesita otorgar o cambiar el acceso.
     iv. Fundamento de la solicitud para aprobación.

  b. **Solicitud de revocación temporal de acceso lógico a cuentas con accesos a los sistemas:** Los requerimientos o solicitudes de revocación temporal de acceso lógico, a funcionarios/as, pasantes, practicantes, empresas, y/o terceros relacionados que aún no han sido informados como desvinculados por la Unidad Gestión del Personal o informados como término de contrato, deberán ser siempre a través de la Plataforma de Mesa de Ayuda TI e informado por la Jefatura directa del funcionario/a en cuestión o el Propietario del activo del sistema, debiendo contener a lo menos, la siguiente información:

     i. Nombre completo del funcionario/a, pasantes, practicantes, empresas, y/o terceros relacionados que se le revocarán los permisos de forma temporal.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

ii. Detallar el motivo, los cuales pueden ser, por ejemplo: Licencias Médicas, sumario administrativo que ordene dicha revocación y/o semejante, renuncia, término de contrato anticipado, gestión de multas contractuales y, en caso de cuentas con permisos más elevados (administradores con mayor acceso), el motivo se podría fundar en desvinculaciones informadas con semanas de anticipación y que el funcionario/a se encuentre haciendo uso de vacaciones o días administrativos, entre otros fundamentos.

c. Información de desvinculaciones: Ticket a Mesa de Ayuda TI desde la Unidad Gestión del Personal, indicando a lo menos:

i. Nombre completo funcionario/a desvinculado.
ii. Fecha de desvinculación.
iii. Centro de Responsabilidad al cual pertenece.

- Toda solicitud de acceso a recursos y/o activos de información, debe ser debidamente solicitada en base a este procedimiento y fundamentado de acuerdo a los lineamientos establecidos en la Política de Control de Acceso Lógico.

- En las situaciones en que un/a administrador/a de plataformas se encuentre fuera de UCOTI, éste será incluido en el ticket como observador, esto para que preste solución a la plataforma que le toque administrar. Esta canalización, le corresponde al agente de la mesa de ayuda TI, pero la solución final la entrega el/la administrador/a que se encuentra a cargo del sistema. Para el caso de el/la administrador/a integrante de UCOTI se asigna en el requerimiento como Agente[2] o como Observador[3], dependiendo de la plataforma a administrar o la característica del ticket.

[2] Agente de Mesa de Ayuda es el técnico a cargo del ticket, quién debe velar por el cierre de este, sea quién de la solución final o no.
[3] Observador de Mesa de Ayuda, es un actor dentro del ticket, puede autorizar, dar solución, opinar, y/o solo mirar que ocurre con el ticket o cualquier acción que considere dentro del mismo, pero no dar cierre al ticket, esta función es del agente.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

- El Encargado/a de Ciberseguridad asume la gestión de los riesgos asociados a la ciberseguridad, incluyendo las actividades orientadas a la protección preventiva de las infraestructuras tecnológicas y sus datos, la detección de vulnerabilidades, anomalías e incidentes, la mitigación del impacto de los mismos, así como la respuesta y recuperación oportuna frente a incidentes que les puedan afectar.

- Funcionarios y funcionarias del SERNAC, practicantes, pasantes, terceros relacionados, y/o cualquier persona con acceso lógicos son responsables de velar por el fiel cumplimiento y protección de los accesos entregados a su persona. Esto es, no divulgar información contenida en dichos sistemas o aplicaciones, como tampoco, facilitar sus accesos a terceros, ya sean estos, funcionarios, funcionarias, jefaturas y/o cualquier tercero, tales como, pasante, proveedores, etc. Manteniendo siempre el control de dicho acceso asignado.

7. Referencias

- Política General de Seguridad de la Información.
- Norma Chilena ISO 27001:2013.
- Norma Chilena ISO 27002:2013.
- Política de Control de Acceso Lógico.
- Norma Chilena ISO 9001:2015.
- Instructivo sobre Gestión de Contraseñas.
- Instructivo de Atención de Requerimientos de Usuarios.
- Instructivo de Administración y Gestión de Plataformas.
- Decreto N°83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

8. Control de Cambios

Nombre sección	Descripción del cambio
1. Presentación del documento	Se modifica el alcance incorporando a pasantes, practicantes y/o cualquier persona que tenga asignado un acceso lógico.
	Se incorpora responsabilidades del Encargado/a de Ciberseguridad
3. Descripción de actividades	Se indica que toda solicitud de acceso debe remitirse mediante Mesa de Ayuda. Se mencionan especificaciones de acceso para "mi unidad". Se precisa actividad respecto a suspender o eliminar los accesos a cualquier persona que ponga en riesgo la seguridad de la información institucional. Se incorporan precisiones en la actividad de proceso de alta de personas usuarias. En la actividad de "Solicitud de usuarios nuevos" se agrega responsabilidad del Administrador de Plataformas y se precisan accesos iniciales para cualquier persona usuaria nueva. Se indica que los permisos y cuentas serán revisados cada 6 meses. En revocación de los permisos se menciona que aplican también para pasantes y personal externo, junto con describir más detalles de cómo se realiza. Se incorpora actividad de "Revocación de accesos a proveedores o terceros relacionados".
6. Consideraciones	Incorporación de nuevas consideraciones y precisiones en otras.

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223

3° ANÓTENSE al margen de la Resolución Exenta N°160 de fecha 25 de febrero de 2022, el número y fecha del presente acto administrativo.

4° PUBLÍQUESE por la Unidad de Control de Gestión y Mejora de Procesos, en el Repositorio Documental institucional vigente el presente acto administrativo para su control y uso.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE

FIRMA ELECTRÓNICA AVANZADA · GOBIERNO DE CHILE

Firmado por:
Andrés Eugenio Herrera Troncoso
Director Nacional
Fecha: 27-03-2024 17:34 CLT
Servicio Nacional del Consumidor

ANDRÉS HERRERA TRONCOSO
DIRECTOR NACIONAL
SERVICIO NACIONAL DEL CONSUMIDOR

ACS/LMD/JOT/RGM/CAV/DBY/CSA/CPR/SLG/VVC
EXPEDIENTE: 16424
Distribución:

- Distribución:
- Gabinete
- Departamento de Comunicaciones Estratégicas
- Fiscalía Administrativa
- Auditoría Interna
- Coordinación de Género e Inclusión
- Coordinación Regional
- Direcciones Regionales SERNAC
- Subdirección Jurídica
- Subdirección de Fiscalización
- Subdirección de Consumo Financiero
- Subdirección de Procedimientos Extrajudiciales de Resolución de Conflictos Colectivos
- Subdirección de Estrategias y Servicios a la Ciudadanía
- División de Gestión y Desarrollo Institucional
- Unidad de Control de Gestión y Mejora de Procesos
- Oficina de Partes y Gestión Documental

Este documento ha sido firmado electrónicamente de acuerdo con la ley N° 19.799
Para verificar la integridad y autenticidad de este documento ingrese al siguiente link:
https://doc.digital.gob.cl/validador/ITMW2J-223