SERNAC
Servicio Nacional del Consumidor

ACTUALIZA "POLÍTICA DE CONTROL DE ACCESO LÓGICO V 3.0", DEL SERVICIO NACIONAL DEL CONSUMIDOR.

RESOLUCION EX. N° 00895

SANTIAGO, 13 NOV 2019

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 Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; el Título VI de la Ley Nº 19.496 sobre Protección de los Derechos de los Consumidores; el Decreto Supremo N° 90, de 2018, que nombró a don Lucas del Villar Montt como Director Nacional del Servicio Nacional del Consumidor; la Resolución Nº 7 de 2019, de la Contraloría General de la República; y,

CONSIDERANDO:

1. Que, mediante Resolución Exenta N° 763, de fecha 27 de septiembre de 2019, se actualizó la Política General de Seguridad de la Información y sus responsables.

2. Que, de acuerdo a los objetivos de la "Política General de Seguridad de la Información" señalada en el considerando precedente, se estableció que para la implementación paulatina de un Sistema de Seguridad de la Información en el Servicio, es necesario "Complementar la Política de Seguridad de la Información, con las políticas específicas, procedimientos, instructivos, etc. que permitan articular el sistema, integrándose, tanto de manera metodológica como documental, con los sistemas de gestión existentes en la Institución".

3. Que, en la misma Resolución Exenta señalada, se constituyó el Comité de Seguridad de la Información, entre cuyas responsabilidades se estableció la de implementar y mantener el sistema de seguridad de la información en el Servicio Nacional del Consumidor.

4. Que, para la implementación de la política referida en el considerando anterior y para complementarla respecto de la seguridad de la información institucional en el acceso lógico a activos de información, recursos computacionales e instalaciones de procesamiento de información (Datacenter), se hace necesario actualizar y aprobar la "política de control de acceso lógico v 3.0".

5. Que, de acuerdo a lo que dispone la Resolución Exenta N° 73 de fecha 01 de febrero de 2018, que Establece la Jerarquía Documental y Aprueba Circuitos de Aprobación en el Servicio Nacional del Consumidor, las Políticas son intenciones y direcciones de la organización.

6. Que, conforme la resolución señalada en el considerando anterior, las Políticas serán elaborados por el Jefe del respectivo Centro de Responsabilidad, para posteriormente pasar por la revisión técnica del Subdirector respectivo y el Jefe de Planificación Estratégica y Calidad para luego ser revisados, respecto a su juridicidad, por la Fiscalía Administrativa, la que los remitirá al Director Nacional, para su aprobación mediante Resolución Exenta.

7. 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.

8. Que, conforme lo señala la normativa referida, se hace necesaria la actualización de la ya mencionada política, mediante el correspondiente acto administrativo.

9. Las facultades que confiere la ley a este Director Nacional.

RESUELVO:

1. ACTUALÍCESE Y APRUÉBASE la "Política de Control de Acceso Lógico" versión *3*.0, ***que se transcribe a continuación***:

I. DECLARACIÓN INSTITUCIONAL

El Servicio Nacional del Consumidor es la institución del Estado responsable de vigilar que se respeten los derechos de los/as consumidores/as, ***definiendo sus líneas estratégicas en cuanto a: informar, educar y proteger a los consumidores, promoviendo el cumplimiento de la normativa vigente, mediante la vigilancia y fiscalización de los mercados, en un marco técnico de eficacia y eficiencia de la acción institucional, potenciando el equilibrio y transparencia en las relaciones de consumo, a través de un SERNAC moderno y ágil al servicio de las personas, bajo el alero de la excelencia y mejora continua.***

Es en este sentido que la Dirección Nacional declara que la presente Política se aplica para definir, establecer, implementar, mantener y mejorar barreras lógicas de acceso a la información, de manera que los procedimientos que se

definan, con sus controles asociados, estén orientados a hacer oposición a las amenazas presentes e impedir que se exploten las vulnerabilidades que pudiesen tener los sistemas que mantienen activos de información y que, en consecuencia, pudieran provocar riesgos que afecten la confidencialidad, integridad y disponibilidad de la información del Servicio Nacional de Consumidor.

II. OBJETIVO GENERAL

La presente Política tiene como objetivo controlar y gestionar el acceso lógico a: activos de información, recursos computacionales e instalaciones de procesamiento de información (Datacenter)[1]; los cuales serán restringidos sobre la base de requisitos de Seguridad de la Información y conforme a los recursos disponibles.

De acuerdo a lo anterior, SERNAC se compromete a gestionar controles para reducir los riesgos vinculados a la Seguridad de la Información, especialmente en el acceso lógico, bajo los siguientes objetivos específicos:

- Definir, establecer, implementar, controlar, mantener y mejorar los niveles de seguridad en el acceso lógico, apropiados para el resguardo de la información para las operaciones en los equipos y áreas del SERNAC.

- Definir, establecer, implementar, controlar, mantener y mejorar un sistema en el cual cada funcionario(a) declara tomar conocimiento de las políticas y procedimientos de gestión de seguridad de la información.

La finalidad es que el funcionario[2] tenga un acceso adecuado y controlado a los sistemas de información y recursos tecnológicos, validando su autentificación, autorización y auditoria.

III. ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política será de aplicación obligatoria a toda la Institución: procesos de provisión de productos estratégicos (bienes y servicios), de gestión estratégica y soporte institucional; funcionarios/as, trabajadores proveedores, clientes (tanto internos como externos) y terceros relacionados.

[1] Un Data Center es un "centro de datos" o "Centro de Proceso de Datos" (CPD). Esta definición engloba las dependencias y los sistemas asociados gracias a los cuales los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos.
[2] Entiéndase para efectos de la presente política, el concepto amplio de funcionario, independiente de su calidad jurídica y/o contractual.

Todos los funcionarios***/as y trabajadores*** de***l*** SERNAC tienen la responsabilidad de conocer y aplicar la presente política, tanto a nivel de gestión interna, como con terceros relacionados a sus funciones.

IV. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Director Nacional	Liderar la definición e implementación de la Política de Control de Acceso Lógico	1. Generar lineamientos y criterios generales. 2. Aprobar políticas institucionales. 3. Asignar recursos según se requiriera, para la gestión lógica de los activos de información institucionales.
Comité de Seguridad de la Información	Coordinar los avances en la implementación y funcionamiento de la Política y sus Procedimientos	1. Entregar asesoría al Director Nacional en materias relativas a la seguridad de los activos de información. 2. Implementar y mantener el Sistema de Seguridad de la Información. 3. Revisar periódicamente el Sistema de Seguridad de la Información, en particular a lo referente al control de accesos lógicos.
Encargado de Seguridad de la Información	Gestionar la implementación de la Política de Control de Acceso Lógico	1. Hacer gestión para la implementación, registro y control de la política de control de acceso lógico y sus procedimientos asociados. 2. Coordinar el análisis, levantamiento y documentación de los procesos de la Institución en temáticas referidas a Control de Acceso Lógico. 3. Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes, servicios en red, etc. 4. Coordinar la difusión de la presente política, según lo indicado en el punto VIII de este documento.

Oficial de Seguridad de la Información	Asesorar y apoyar en temáticas relacionadas al control de acceso lógico	1. Asesorar en forma permanente y cercana, a las distintas áreas de la Institución en temas referentes a seguridad y conducir al correcto cumplimiento de los estándares de seguridad definidos. 2. Proponer el diseño de políticas, normas y procedimientos de seguridad de la información. 3. Controlar los niveles de acceso lógico institucionales.
Jefatura de l***a Unidad Continuidad Operativa TI***	Responsable de las acciones TI implementadas	1. Velar por el fiel cumplimiento de las acciones tecnológicas implementadas por ***la Unidad Continuidad Operativa TI***, de acuerdo a los lineamientos que de esta política se pueden desprender. 2. Proponer y/o definir requisitos técnicos necesarios para la materialización de la presente política. 3. Administrar el ciclo de vida de los usuarios a nivel lógico, desde la creación de sus cuentas y accesos a los diferentes sistemas y aplicaciones, hasta la gestión de redes y servicios de red que correspondan. Esto, sin perjuicio de la gestión asociada a todos los demás roles, permisos, accesos y privilegios necesarios para sus operaciones diarias (a partir de requerimientos solicitados de forma previa).
Propietarios de los Activos de Información	Responsables de la autorización de derechos de acceso	1. Autorizar los derechos de acceso de un usuario a los sistemas y bases de datos que están bajo su gestión.
Jefaturas ***y Coordinadores/as***	Implementar las políticas y procedimientos relacionados a control de acceso lógico	1. Promover y dar cumplimiento a lo establecido en la presente Política y en las que la complementen, y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que determinen las áreas

		responsables, el Encargado de Seguridad de la Información, el Oficial de Seguridad y/o el Comité de Seguridad de la Información.
Funcionarios del SERNAC	Colaborar en la implementación y dar cumplimiento a lo establecido en la Política de Control de Acceso Lógico y sus procedimientos	1. Dar cumplimiento a lo establecido en la presente Política y en las que la complementen y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que determinen las áreas responsables, el Encargado de Seguridad de la Información, el Oficial de Seguridad y/o el Comité de Seguridad de la Información.
Terceros relacionados[3]	Colaborar con la implementación de la Política de Control de Acceso Lógico	1. Colaborar directamente con el cumplimiento de las disposiciones, definiciones e implementación de la Política de Control de Acceso Lógico, según corresponda.
Mesa de Ayuda ***TI***	Gestionar técnicamente el control de acceso lógico[4]	1. Gestionar y/o escalar los requerimientos de acceso lógico.

V. DEFINICIÓN Y NORMATIVAS VIGENTES

La presente política es parte integral de la documentación del Sistema de Seguridad de la Información de la Institución, y está orientada a formular las directrices generales que permitan minimizar el impacto de las amenazas y riesgos que pudiesen estar presentes, en materia de Control de Acceso Lógico, bajo las siguientes especificaciones:

- Quienes utilicen los servicios de información son responsables por su cuenta de usuario y contraseña para el uso y acceso a los recursos informáticos. La Mesa de Ayuda ***TI*** se comunicará por escrito a los usuarios las condiciones básicas de uso de sus cuentas y contraseñas al serles asignadas.

- Las cuentas de usuario contarán con los privilegios mínimos necesarios para acceder a los diferentes sistemas del SERNAC, coherentes con el desarrollo de las funciones asignadas.

[3] Personas, partes o actores externos al Servicio Nacional del Consumidor, y que se relacionan en él en el cumplimiento de condiciones contractuales, de convenios de servicio, en la gestión de áreas de negocio, entre otros.
[4] Podrá haber excepciones, según condiciones contractuales de gestión de plataformas.

- Se debe efectuar la implementación de controles de accesos mediante técnicas de autentificación, autorización y contabilidad, basados en el Protocolo de Seguridad Informática AAA (Authentication, Authorization y Accounting).

- Queda prohibida la utilización de la infraestructura tecnológica del SERNAC para obtener acceso lógico no autorizado a la información, a otros sistemas de información de SERNAC, o de terceros.

- Queda prohibido proporcionar a personal externo, información de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del SERNAC.

- Queda prohibido que usuarios externos o visitantes hagan conexión lógica con sus propios dispositivos a la red de SERNAC, salvo que sea autorizado expresamente por el ***Jefe/a de Continuidad Operativa TI***, quien se reserva el derecho de realizar las revisiones que estime pertinentes a los dispositivos de los usuarios, previo a otorgar la autorización. Lo anterior, para validar los requisitos técnicos de seguridad para el ingreso a la red. Este tipo de conexiones será limitado y temporal, pudiendo ser revocado sin mediar previo aviso.

- Se deben revocar en forma inmediata los derechos de acceso lógico a aquellos usuarios que se desvinculan del SERNAC en forma permanente. Esto, previa notificación ***del Departamento*** Gestión y Desarrollo de Personas.

- Se debe asegurar que la información se mantenga bajo rigurosos mecanismos de seguridad, cuando se utiliza para su procesamiento y/o instalación y equipamiento de procesamiento remoto, con y sin conexión.

- Todos los contratos de confidencialidad o no divulgación, convenios, acuerdos o cualquier otra forma que relacione las actividades con terceros, deben tener definidos, establecidos, implementados y mantenidos los controles, requerimientos de seguridad y compromisos formales de confidencialidad y/o no divulgación apropiados a cada caso, otorgando los privilegios de acceso lógico restringidos para su funcionamiento estricto, hasta que sean verificados todos los antecedentes y acciones de resguardo necesario.

- Queda estrictamente prohibido otorgar derechos de acceso lógico a terceros, salvo excepciones autorizadas por el ***Jefe/a de Continuidad Operativa TI***, quien además deberá monitorearlas y controlarlas.

- Se otorgará acceso lógico sólo a la información que necesitan los funcionarios para realizar sus tareas, partiendo de la base que las distintas tareas/roles se traducen en distintos aspectos que se deberían conocer y, por lo tanto, en distintos perfiles de acceso.

- Sólo se otorgará acceso lógico a las instalaciones de procesamiento de información (equipos TI, aplicaciones, etc.) necesarias para realizar la tarea/rol/trabajo de los funcionarios y demás trabajadores de SERNAC.

- ***Los accesos con más alto privilegio tanto como ROOT o Administrador, deben ser restringidos y controlados por la Unidad Continuidad Operativa TI, dado su alto riesgo en la continuidad operacional de las distintas plataformas tecnológicas y servidores.***

A objeto de dar cumplimiento a la presente Política, el Servicio definirá los procedimientos e instrucciones de trabajo específicas que permitan asegurar la correcta implementación y cumplimiento de los principios aquí señalados.

Éstas y las demás definiciones relacionadas con la Seguridad de la Información, se encontrarán disponibles en la Documentación Técnica y Legal del Sistema, ubicada en el Gestor Documental de la aplicación web de gestión de la Institución, o su equivalente vigente.

VI. RELACIÓN CON OTRAS POLÍTICAS INSTITUCIONALES

La presente Política se aplicará de manera complementaria con las demás políticas internas y gubernamentales definidas para el Servicio, así como otros documentos pertinentes del SERNAC. Toda la documentación que forme parte del Sistema de Seguridad de la Información, se desarrollará bajo los criterios, formatos y metodologías existentes en el marco del Sistema de Gestión Institucional, siendo de carácter complementario, el desarrollo del presente sistema.

Especial relación ha de aplicarse con la Política de Gestión de la Calidad, la de Gestión de Riesgos y la General de Seguridad de la Información.

VII. REVISIONES

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política será revisada al menos una vez por año por parte del Comité de Seguridad de la Información, proponiendo a la Dirección Nacional, las mejoras a implementar ***o la mantención de ésta.***

La forma de verificar la realización de esta revisión, será el acta del Comité de Seguridad de la Información, de la sesión correspondiente.

VIII. MECANISMOS DE DIFUSION DE LA POLÍTICA

La difusión de la presente política se realizará mediante comunicaciones internas, informando a todos los funcionarios y trabajadores del SERNAC, las políticas vigentes, su lugar de

almacenamiento e invitándolos a revisarlas como parte de sus responsabilidades. Junto a esto, los documentos serán publicados en el gestor documental institucional y en el Registro de publicación de actos y resoluciones con efectos sobre terceros, del sitio web institucional, según corresponda.

2°. DÉJESE, sin efecto lo establecido en la Resolución Exenta N°941 del 28 de diciembre de 2018, y todas las anteriores que se hayan dictado en materia de Política de Control de Acceso Lógico.

3°. PUBLÍQUESE en el gestor documental de la aplicación web de gestión, para su control y uso.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE

SERVICIO NACIONAL DEL CONSUMIDOR
DIRECTOR NACIONAL

LUCAS DEL VILLAR MONTT
DIRECTOR NACIONAL
SERVICIO NACIONAL DEL CONSUMIDOR

SERNAC
Servicio Nacional del Consumidor

ACTUALIZA "POLÍTICA DE CONTROL DE ACCESO LÓGICO V 3.0", DEL SERVICIO NACIONAL DEL CONSUMIDOR.

RESOLUCION EX. Nº 00895

SANTIAGO, 13 NOV 2019

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 Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado; el Título VI de la Ley Nº 19.496 sobre Protección de los Derechos de los Consumidores; el Decreto Supremo N° 90, de 2018, que nombró a don Lucas del Villar Montt como Director Nacional del Servicio Nacional del Consumidor; la Resolución Nº 7 de 2019, de la Contraloría General de la República; y,

CONSIDERANDO:

1. Que, mediante Resolución Exenta N° 763, de fecha 27 de septiembre de 2019, se actualizó la Política General de Seguridad de la Información y sus responsables.

2. Que, de acuerdo a los objetivos de la "Política General de Seguridad de la Información" señalada en el considerando precedente, se estableció que para la implementación paulatina de un Sistema de Seguridad de la Información en el Servicio, es necesario "Complementar la Política de Seguridad de la Información, con las políticas específicas, procedimientos, instructivos, etc. que permitan articular el sistema, integrándose, tanto de manera metodológica como documental, con los sistemas de gestión existentes en la Institución".

3. Que, en la misma Resolución Exenta señalada, se constituyó el Comité de Seguridad de la Información, entre cuyas responsabilidades se estableció la de implementar y mantener el sistema de seguridad de la información en el Servicio Nacional del Consumidor.

4. Que, para la implementación de la política referida en el considerando anterior y para complementarla respecto de la seguridad de la información institucional en el acceso lógico a activos de información, recursos computacionales e instalaciones de procesamiento de información (Datacenter), se hace necesario actualizar y aprobar la "política de control de acceso lógico v 3.0".

5. Que, de acuerdo a lo que dispone la Resolución Exenta N° 73 de fecha 01 de febrero de 2018, que Establece la Jerarquía Documental y Aprueba Circuitos de Aprobación en el Servicio Nacional del Consumidor, las Políticas son intenciones y direcciones de la organización.

6. Que, conforme la resolución señalada en el considerando anterior, las Políticas serán elaborados por el Jefe del respectivo Centro de Responsabilidad, para posteriormente pasar por la revisión técnica del Subdirector respectivo y el Jefe de Planificación Estratégica y Calidad para luego ser revisados, respecto a su juridicidad, por la Fiscalía Administrativa, la que los remitirá al Director Nacional, para su aprobación mediante Resolución Exenta.

7. 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.

8. Que, conforme lo señala la normativa referida, se hace necesaria la actualización de la ya mencionada política, mediante el correspondiente acto administrativo.

9. Las facultades que confiere la ley a este Director Nacional.

RESUELVO:

1. ACTUALÍCESE Y APRUÉBASE la "Política de Control de Acceso Lógico" versión *3.0*, ***que se transcribe a continuación***:

I. DECLARACIÓN INSTITUCIONAL

El Servicio Nacional del Consumidor es la institución del Estado responsable de vigilar que se respeten los derechos de los/as consumidores/as, ***definiendo sus líneas estratégicas en cuanto a: informar, educar y proteger a los consumidores, promoviendo el cumplimiento de la normativa vigente, mediante la vigilancia y fiscalización de los mercados, en un marco técnico de eficacia y eficiencia de la acción institucional, potenciando el equilibrio y transparencia en las relaciones de consumo, a través de un SERNAC moderno y ágil al servicio de las personas, bajo el alero de la excelencia y mejora continua.***

Es en este sentido que la Dirección Nacional declara que la presente Política se aplica para definir, establecer, implementar, mantener y mejorar barreras lógicas de acceso a la información, de manera que los procedimientos que se

definan, con sus controles asociados, estén orientados a hacer oposición a las amenazas presentes e impedir que se exploten las vulnerabilidades que pudiesen tener los sistemas que mantienen activos de información y que, en consecuencia, pudieran provocar riesgos que afecten la confidencialidad, integridad y disponibilidad de la información del Servicio Nacional de Consumidor.

II. OBJETIVO GENERAL

La presente Política tiene como objetivo controlar y gestionar el acceso lógico a: activos de información, recursos computacionales e instalaciones de procesamiento de información (Datacenter)[1]; los cuales serán restringidos sobre la base de requisitos de Seguridad de la Información y conforme a los recursos disponibles.

De acuerdo a lo anterior, SERNAC se compromete a gestionar controles para reducir los riesgos vinculados a la Seguridad de la Información, especialmente en el acceso lógico, bajo los siguientes objetivos específicos:

- Definir, establecer, implementar, controlar, mantener y mejorar los niveles de seguridad en el acceso lógico, apropiados para el resguardo de la información para las operaciones en los equipos y áreas del SERNAC.

- Definir, establecer, implementar, controlar, mantener y mejorar un sistema en el cual cada funcionario(a) declara tomar conocimiento de las políticas y procedimientos de gestión de seguridad de la información.

La finalidad es que el funcionario[2] tenga un acceso adecuado y controlado a los sistemas de información y recursos tecnológicos, validando su autentificación, autorización y auditoria.

III. ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política será de aplicación obligatoria a toda la Institución: procesos de provisión de productos estratégicos (bienes y servicios), de gestión estratégica y soporte institucional; funcionarios/as, trabajadores proveedores, clientes (tanto internos como externos) y terceros relacionados.

[1] Un Data Center es un "centro de datos" o "Centro de Proceso de Datos" (CPD). Esta definición engloba las dependencias y los sistemas asociados gracias a los cuales los datos son almacenados, tratados y distribuidos al personal o procesos autorizados para consultarlos y/o modificarlos.
[2] Entiéndase para efectos de la presente política, el concepto amplio de funcionario, independiente de su calidad jurídica y/o contractual.

Todos los funcionarios/***as y trabajadores*** de***l*** SERNAC tienen la responsabilidad de conocer y aplicar la presente política, tanto a nivel de gestión interna, como con terceros relacionados a sus funciones.

IV. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Director Nacional	Liderar la definición e implementación de la Política de Control de Acceso Lógico	1. Generar lineamientos y criterios generales. 2. Aprobar políticas institucionales. 3. Asignar recursos según se requiriera, para la gestión lógica de los activos de información institucionales.
Comité de Seguridad de la Información	Coordinar los avances en la implementación y funcionamiento de la Política y sus Procedimientos	1. Entregar asesoría al Director Nacional en materias relativas a la seguridad de los activos de información. 2. Implementar y mantener el Sistema de Seguridad de la Información. 3. Revisar periódicamente el Sistema de Seguridad de la Información, en particular a lo referente al control de accesos lógicos.
Encargado de Seguridad de la Información	Gestionar la implementación de la Política de Control de Acceso Lógico	1. Hacer gestión para la implementación, registro y control de la política de control de acceso lógico y sus procedimientos asociados. 2. Coordinar el análisis, levantamiento y documentación de los procesos de la Institución en temáticas referidas a Control de Acceso Lógico. 3. Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes, servicios en red, etc. 4. Coordinar la difusión de la presente política, según lo indicado en el punto VIII de este documento.

Oficial de Seguridad de la Información	Asesorar y apoyar en temáticas relacionadas al control de acceso lógico	1. Asesorar en forma permanente y cercana, a las distintas áreas de la Institución en temas referentes a seguridad y conducir al correcto cumplimiento de los estándares de seguridad definidos. 2. Proponer el diseño de políticas, normas y procedimientos de seguridad de la información. 3. Controlar los niveles de acceso lógico institucionales.
Jefatura de l***a Unidad Continuidad Operativa TI***	Responsable de las acciones TI implementadas	1. Velar por el fiel cumplimiento de las acciones tecnológicas implementadas por ***la Unidad Continuidad Operativa TI***, de acuerdo a los lineamientos que de esta política se pueden desprender. 2. Proponer y/o definir requisitos técnicos necesarios para la materialización de la presente política. 3. Administrar el ciclo de vida de los usuarios a nivel lógico, desde la creación de sus cuentas y accesos a los diferentes sistemas y aplicaciones, hasta la gestión de redes y servicios de red que correspondan. Esto, sin perjuicio de la gestión asociada a todos los demás roles, permisos, accesos y privilegios necesarios para sus operaciones diarias (a partir de requerimientos solicitados de forma previa).
Propietarios de los Activos de Información	Responsables de la autorización de derechos de acceso	1. Autorizar los derechos de acceso de un usuario a los sistemas y bases de datos que están bajo su gestión.
Jefaturas ***y Coordinadores/as***	Implementar las políticas y procedimientos relacionados a control de acceso lógico	1. Promover y dar cumplimiento a lo establecido en la presente Política y en las que la complementen, y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que determinen las áreas

		responsables, el Encargado de Seguridad de la Información, el Oficial de Seguridad y/o el Comité de Seguridad de la Información.
Funcionarios del SERNAC	Colaborar en la implementación y dar cumplimiento a lo establecido en la Política de Control de Acceso Lógico y sus procedimientos	1. Dar cumplimiento a lo establecido en la presente Política y en las que la complementen y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que determinen las áreas responsables, el Encargado de Seguridad de la Información, el Oficial de Seguridad y/o el Comité de Seguridad de la Información.
Terceros relacionados[3]	Colaborar con la implementación de la Política de Control de Acceso Lógico	1. Colaborar directamente con el cumplimiento de las disposiciones, definiciones e implementación de la Política de Control de Acceso Lógico, según corresponda.
Mesa de Ayuda ***TI***	Gestionar técnicamente el control de acceso lógico[4]	1. Gestionar y/o escalar los requerimientos de acceso lógico.

V. DEFINICIÓN Y NORMATIVAS VIGENTES

La presente política es parte integral de la documentación del Sistema de Seguridad de la Información de la Institución, y está orientada a formular las directrices generales que permitan minimizar el impacto de las amenazas y riesgos que pudiesen estar presentes, en materia de Control de Acceso Lógico, bajo las siguientes especificaciones:

- Quienes utilicen los servicios de información son responsables por su cuenta de usuario y contraseña para el uso y acceso a los recursos informáticos. La Mesa de Ayuda ***TI*** se comunicará por escrito a los usuarios las condiciones básicas de uso de sus cuentas y contraseñas al serles asignadas.

- Las cuentas de usuario contarán con los privilegios mínimos necesarios para acceder a los diferentes sistemas del SERNAC, coherentes con el desarrollo de las funciones asignadas.

[3] Personas, partes o actores externos al Servicio Nacional del Consumidor, y que se relacionan en él en el cumplimiento de condiciones contractuales, de convenios de servicio, en la gestión de áreas de negocio, entre otros.
[4] Podrá haber excepciones, según condiciones contractuales de gestión de plataformas.

- Se debe efectuar la implementación de controles de accesos mediante técnicas de autentificación, autorización y contabilidad, basados en el Protocolo de Seguridad Informática AAA (Authentication, Authorization y Accounting).

- Queda prohibida la utilización de la infraestructura tecnológica del SERNAC para obtener acceso lógico no autorizado a la información, a otros sistemas de información de SERNAC, o de terceros.

- Queda prohibido proporcionar a personal externo, información de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del SERNAC.

- Queda prohibido que usuarios externos o visitantes hagan conexión lógica con sus propios dispositivos a la red de SERNAC, salvo que sea autorizado expresamente por el ***Jefe/a de Continuidad Operativa TI***, quien se reserva el derecho de realizar las revisiones que estime pertinentes a los dispositivos de los usuarios, previo a otorgar la autorización. Lo anterior, para validar los requisitos técnicos de seguridad para el ingreso a la red. Este tipo de conexiones será limitado y temporal, pudiendo ser revocado sin mediar previo aviso.

- Se deben revocar en forma inmediata los derechos de acceso lógico a aquellos usuarios que se desvinculan del SERNAC en forma permanente. Esto, previa notificación ***del Departamento*** Gestión y Desarrollo de Personas.

- Se debe asegurar que la información se mantenga bajo rigurosos mecanismos de seguridad, cuando se utiliza para su procesamiento y/o instalación y equipamiento de procesamiento remoto, con y sin conexión.

- Todos los contratos de confidencialidad o no divulgación, convenios, acuerdos o cualquier otra forma que relacione las actividades con terceros, deben tener definidos, establecidos, implementados y mantenidos los controles, requerimientos de seguridad y compromisos formales de confidencialidad y/o no divulgación apropiados a cada caso, otorgando los privilegios de acceso lógico restringidos para su funcionamiento estricto, hasta que sean verificados todos los antecedentes y acciones de resguardo necesario.

- Queda estrictamente prohibido otorgar derechos de acceso lógico a terceros, salvo excepciones autorizadas por el ***Jefe/a de Continuidad Operativa TI***, quien además deberá monitorearlas y controlarlas.

- Se otorgará acceso lógico sólo a la información que necesitan los funcionarios para realizar sus tareas, partiendo de la base que las distintas tareas/roles se traducen en distintos aspectos que se deberían conocer y, por lo tanto, en distintos perfiles de acceso.

- Sólo se otorgará acceso lógico a las instalaciones de procesamiento de información (equipos TI, aplicaciones, etc.) necesarias para realizar la tarea/rol/trabajo de los funcionarios y demás trabajadores de SERNAC.

- ***Los accesos con más alto privilegio tanto como ROOT o Administrador, deben ser restringidos y controlados por la Unidad Continuidad Operativa TI, dado su alto riesgo en la continuidad operacional de las distintas plataformas tecnológicas y servidores.***

A objeto de dar cumplimiento a la presente Política, el Servicio definirá los procedimientos e instrucciones de trabajo específicas que permitan asegurar la correcta implementación y cumplimiento de los principios aquí señalados.

Éstas y las demás definiciones relacionadas con la Seguridad de la Información, se encontrarán disponibles en la Documentación Técnica y Legal del Sistema, ubicada en el Gestor Documental de la aplicación web de gestión de la Institución, o su equivalente vigente.

VI. RELACIÓN CON OTRAS POLÍTICAS INSTITUCIONALES

La presente Política se aplicará de manera complementaria con las demás políticas internas y gubernamentales definidas para el Servicio, así como otros documentos pertinentes del SERNAC. Toda la documentación que forme parte del Sistema de Seguridad de la Información, se desarrollará bajo los criterios, formatos y metodologías existentes en el marco del Sistema de Gestión Institucional, siendo de carácter complementario, el desarrollo del presente sistema.

Especial relación ha de aplicarse con la Política de Gestión de la Calidad, la de Gestión de Riesgos y la General de Seguridad de la Información.

VII. REVISIONES

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política será revisada al menos una vez por año por parte del Comité de Seguridad de la Información, proponiendo a la Dirección Nacional, las mejoras a implementar ***o la mantención de ésta.***

La forma de verificar la realización de esta revisión, será el acta del Comité de Seguridad de la Información, de la sesión correspondiente.

VIII. MECANISMOS DE DIFUSION DE LA POLÍTICA

La difusión de la presente política se realizará mediante comunicaciones internas, informando a todos los funcionarios y trabajadores del SERNAC, las políticas vigentes, su lugar de

almacenamiento e invitándolos a revisarlas como parte de sus responsabilidades. Junto a esto, los documentos serán publicados en el gestor documental institucional y en el Registro de publicación de actos y resoluciones con efectos sobre terceros, del sitio web institucional, según corresponda.

2°. DÉJESE, sin efecto lo establecido en la Resolución Exenta N°941 del 28 de diciembre de 2018, y todas las anteriores que se hayan dictado en materia de Política de Control de Acceso Lógico.

3°. PUBLÍQUESE en el gestor documental de la aplicación web de gestión, para su control y uso.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE

SERVICIO NACIONAL DEL CONSUMIDOR
DIRECTOR NACIONAL

LUCAS DEL VILLAR MONTT
DIRECTOR NACIONAL
SERVICIO NACIONAL DEL CONSUMIDOR

SERVICIO NACIONAL DEL CONSUMIDOR
FISCALIA ADMINISTRATIVA

SERVICIO NACIONAL DEL CONSUMIDOR
JEFA
Departamento Gestión y Desarrollo

ALR/JOT/PHP/MG/RMA/vc
R.J.:5250
Distribución:
- Gabinete
- Fiscalía Administrativa
- Auditoría Interna
- Unidad de Control de Gestión y Mejoramiento de Procesos.
- Direcciones Regionales.
- Subdirección Nacional.
- Subdirección Jurídica.
- Subdirección Estrategia y Proyectos Institucionales.
- Depto. Administración y Finanzas.
- Oficina de Partes.