RESOLUCIÓN EXENTA N° 958

SANTIAGO, 10 DE NOVIEMBRE 2022

ACTUALIZA "POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS V 4.0", DEL SERVICIO NACIONAL DEL CONSUMIDOR.

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, que establece las funciones del Servicio Nacional del Consumidor; la Resolución Exenta N°658 de 27 de agosto de 2021 que establece la jerarquía documental y los circuitos de aprobación de los mismos; la Resolución Nº 7 de 2019, de la Contraloría General de la República; y

CONSIDERANDO:

1. Que, mediante Resolución Exenta N° 592, de fecha 07 de julio de 2022, 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, la implementación paulatina de un Sistema de Seguridad de la Información, requiere ser complementado con 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, durante julio de 2022 se modificó la "Política de escritorio y pantalla limpios v.3" aprobada por Resolución Exenta N° 881 de 11 de noviembre de 2019, la que se actualiza por el presente acto administrativo.

4. Que, el término Política, de acuerdo a la definición entregada en la Resolución Exenta N°658 de fecha 27 de agosto de 2021, que "Establece la Jerarquía Documental y Aprueba Circuitos de Aprobación" en el Servicio Nacional del Consumidor, es una intención y directriz de la Institución, forma de expresión formal de la Dirección Nacional que proporciona un marco de referencia para los objetivos propuestos según la materia.

5. Que, éstos, de acuerdo a la Resolución Exenta citada, serán elaborados por la Jefatura del Centro de Responsabilidad, para posteriormente pasar por la revisión técnica de la Subdirección del Centro de Responsabilidad responsable de operativizar el proceso. Luego es sometida a una revisión del Sistema de Gestión de la Calidad, a cargo de la Unidad de Control de Gestión y Mejora de Procesos, más una revisión estratégica de la Subdirección de Estrategias, Proyectos Institucionales y Servicios Usuarios. De manera posterior, se somete al control de legalidad de la Fiscalía Administrativa, área que, en caso de que se encuentren jurídicamente correctos, los remitirá al/la Director/a Nacional para su aprobación mediante Resolución Exenta.

6. Que de acuerdo a la resolución exenta antes citada, se delega en el/la Subdirector/a de Estrategia, Proyectos Institucionales y Servicios Usuarios la facultad de firmar, por orden del Director Nacional, las resoluciones exentas que aprueben políticas institucionales relacionadas a controles de seguridad de la información.

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, en consecuencia, se hace necesaria la aprobación de la ya mencionada Política mediante la correspondiente resolución.

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

RESUELVO:

1. ACTUALÍCESE la "Política de Escritorio y Pantalla Limpios" versión 4.0, 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 la protección de cualquier tipo de información de SERNAC, en cualquiera de sus formas y que puede estar contenida en escritorios, estaciones de trabajo, computadores portátiles, smartphones, medios magnéticos, dispositivos removibles (pendrive, CD, DVD, discos externos,

etc.), documentación impresa en papel y en general, cualquier tipo de información que es utilizada por los funcionarios**/as**. La finalidad es reducir accesos no autorizados, pérdida, fuga o daño de la información que es manipulada por los funcionarios***/as*** durante y después de la jornada laboral.

II. OBJETIVO GENERAL

Establecer lineamientos y normas generales que regulen la protección y el uso de pantallas y escritorios no supervisados, durante y después de la jornada laboral, entendiendo éstos como pantallas de computador y/o escritorios que permanecen sin uso y sin un funcionario***/a*** que esté vigilando y ejerciendo supervisión sobre la información que éstos contienen.

III. ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

Esta política debe ser conocida y cumplida por todos los funcionarios/as de planta, contrata y personal a honorarios del Servicio Nacional de Consumidor. También aplica a externos contratados que presten servicios y tengan acceso a información y recursos de la institución***, así como también, incluye a pasantes, practicantes y/o cualquier persona que tenga asignado un puesto de trabajo o recurso tecnológico.***
Aplica a pantallas e instalaciones de procesamiento de información, computadores portátiles, smartphones, medios magnéticos, dispositivos removibles (pendrive, CD, DVD, discos externos, etc.), documentación impresa en papel y en general, cualquier tipo de soporte de información que es utilizada por los funcionarios, ***funcionarias, terceros y cualquier persona que cuente con equipos tecnológicos y/o puesto de trabajo asignado.***

IV. ROLES Y RESPONSABILIDADES

Responsable	Rol	Funciones
Director***/a*** Nacional	Liderar la definición e implementación de la Política de Escritorio y Pantalla Limpios	1. ***Liderar el compromiso institucional con la Política de escritorio y pantalla limpios.*** 2. Generar lineamientos y criterios generales ***en materias de escritorios y pantallas limpios.*** ***3. Evaluar las propuestas y las acciones realizadas por el/la Encargado/ de Ciberseguridad para dar cumplimiento a la Política Nacional de Ciberseguridad, aplicables a la política de escritorio y pantalla limpios.***

		4. Asignar recursos, según las necesidades para la Gestión de la política de escritorio y pantalla limpios.
Comité de Seguridad de la Información	Coordinar los avances en la implementación y funcionamiento de la Política y sus Procedimientos	1. Asesorar al Director***/a*** Nacional en materias relativas a la seguridad de los activos de información ***relacionados con la política de escritorio y pantallas limpios.*** 2. Revisar periódicamente el Sistema de ***Gestión de la*** Seguridad de la Información, en particular lo referente a las pantallas y escritorios despejados. ***3. Revisar y tomar acciones sobre los incidentes y eventos de seguridad de la información referente a las pantallas y escritorios despejados, priorizados por el Comité Operativo de Seguridad de la Información.***
Encargado/a de Seguridad de la Información	Gestionar la implementación de la Política de Escritorio y Pantalla Limpios	1. Hacer gestión para la implementación, registro y control de la política de escritorio y pantalla limpios y sus procedimientos asociados. 2. Coordinar el análisis, levantamiento y documentación de los procesos de la Institución, en temáticas referidas a pantallas y escritorios despejados. 3. Coordinar la difusión de la presente política, según lo indicado en el punto VIII de este documento.
Encargado/a de Ciberseguridad	***Responsable de proponer lineamientos y asesorar técnicamente en materias de escritorio y pantalla limpios***	***1. Planificar y ejecutar acciones de difusión y concientización para lograr el entendimiento y aplicación de la presente Política por parte de todo el personal de SERNAC.*** ***2. Asesorar, el/la Director/a Nacional, en el análisis e implementación de iniciativas tendientes a dar***

		cumplimiento a la Política Nacional de Ciberseguridad, aplicables a la política de escritorio y pantallas limpios. ***3. Proponer a el/la Director/a Nacional, cambios a la normativa interna, cuando ésta incida en materias de ciberseguridad, y las modificaciones que sean necesarias para el cumplimiento de la Política Nacional de Ciberseguridad, aplicables a la política de escritorio y pantallas limpios.***
Oficial de Seguridad de la Información	Apoyar y asesorar en temáticas relacionadas a pantallas y escritorios despejados, ***junto con supervisar su cumplimiento***	1. ***Apoyar en la ejecución de acciones de difusión y concientización para lograr el entendimiento y aplicación de la presente Política por parte de todo el personal de SERNAC.*** 2. Asesorar en forma permanente y cercana, a las distintas áreas de la Institución, ***en el entendimiento e implementación de la presente Política.*** ***3. Supervisar el cumplimiento de la presente Política, registrando y coordinando el tratamiento de eventos e incidentes asociados a su incumplimiento.***
Jefatura de ***la 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.
Jefaturas ***y Coordinadores/as***	Implementar las políticas y procedimientos relacionados a pantallas y escritorios despejados	1. Promover y dar cumplimiento a lo establecido en la presente Política y en las que la complementen, velando por su aplicación en su entorno laboral, a través de los procedimientos e instrucciones que se determinen ***en***

		materias de seguridad de la información y de ciberseguridad, relacionadas con la política de escritorio y pantalla limpios. 2. ***Alertar de manera oportuna y adecuada al Oficial de Seguridad y a la jefatura directa, o superior, cualquier situación que atente contra lo establecido en esta política y/o pueda poner en riesgo la continuidad de los procesos.***
Funcionarios***/as*** del SERNAC	Colaborar en la implementación y dar cumplimiento a lo establecido en la Política de Control de Escritorio y Pantalla Limpios y sus procedimientos	1. Dar cumplimiento a lo establecido en la presente Política y en las que la complementen,aplicándola 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 ***Operativo*** de Seguridad de la Información. ***2. Alertar de manera oportuna y adecuada al Oficial de Seguridad de la Información, a su jefatura directa y/o superior, cualquier situación que atente contra lo establecido en esta política o pueda poner en riesgo la continuidad de la seguridad de la información.***
Terceros relacionados[1]	Colaborar con la implementación de la Política de Escritorio y Pantalla Limpios	1. Colaborar directamente con el cumplimiento de las disposiciones, definiciones e implementación de la Política de Control de Escritorio y Pantalla Limpios, ***y otros documentos que la complementen, según***

[1] 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.

		corresponda a su relación con el Servicio.

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 escritorios y pantallas despejados, bajo las siguientes especificaciones:

5.1. Ubicación de escritorios y equipos

5.1.1. Los lugares y/o puestos de trabajo de los funcionarios de la institución, deben estar ubicados, preferentemente, donde no queden expuestos al acceso de personas externas. De esta forma, se protege tanto el equipamiento tecnológico, como los documentos que contengan información confidencial o de uso interno, que eventualmente, esté utilizando el trabajador.

5.1.2. Los escritorios, muebles y computadores ubicados cerca de zonas de atención o tránsito de público, deben situarse de tal forma que permitan proteger los activos de información institucionales y las pantallas de las estaciones de trabajo.

5.1.3. Las pantallas y documentos que deban ser visualizadas por personas externas a la institución, deberán hacerlo con autorización o supervisión adecuada, por parte de un funcionario responsable.

5.1.4. Cuando sea aplicable, en los sitios donde se almacene la información física o digital (activos de información), se debe implementar condiciones ambientales que controlen o alerten temperatura y humedad adecuadas.[2]

5.2. Escritorios de trabajo limpios

5.2.1. Los funcionarios/as deben velar porque la información con que trabajan, ya sea en formato papel o digital ***y/***o el medio que la contenga (PC, Dispositivos Móviles, etc.), no permanezcan expuestos a terceros o personal no autorizado, antes, durante y finalizada la jornada de trabajo***,*** inclusive. ***Por otra parte, cabe destacar que, existe prohibición de guardar información digital en cualquier otro medio que no sea Google Drive o sistemas asignados para dicho efecto, como por ejemplo "GIDI", quedando prohibido guardar información en pendrives, cd, discos duros de los computadores y/o cualquier otro medio físico que contenga información digital.***

5.2.2. Es responsabilidad del funcionario/a, tratándose de estaciones de trabajo, bloquear sus pantallas en caso de ausentarse de su escritorio, utilizando una clave personal para su desbloqueo y

[2] Sujeto a recursos disponibles.

evitando así, la exposición de la información ante terceras personas o funcionarios***/as*** del Servicio que no sean pertinentes (no autorizados a acceder a esa información).

5.2.3. Si el funcionario/a está ubicado cerca de zonas de atención o tránsito de público y al ausentarse de su lugar de trabajo, debe guardar también los documentos y medios físicos que contengan información de uso interno, reservado o confidencial para la institución.

5.2.4. Cuando no se necesite, cuando las oficinas estén desocupadas o al finalizar la jornada de trabajo, el funcionario/a debe guardar en un lugar seguro y resguardado (de acuerdo a las facilidades dadas por la institución), los documentos y medios que contengan información reservada, confidencial o de uso interno.

5.2.5. Los funcionarios/as deben velar que se prevenga el uso no autorizado de fotocopiadoras y otros medios tecnológicos que permitan la reproducción de información, tales como: escáner, teléfonos celulares, dispositivos o cámaras digitales, que pudiesen facilitar o permitir, el robo, pérdida o fuga de información considerada reservada, confidencial o sensible para procesos institucionales.

5.2.6. Los funcionarios***/as*** deben velar que no se exponga la información y sus medios de procesamiento y***/o*** almacenamiento, a un posible deterioro o pérdida causada por consumo de alimentos, bebidas y/o el consumo de cigarrillo, velas e inciensos, estufas eléctricas o a gas, etc., que estén cerca o sobre las estaciones de trabajo o dichos medios. ***Es por ello que, para evitar este tipo de situaciones, existe prohibición de guardar información en medios físicos. Toda información institucional debe estar en la nube de Google Drive y/o en sistemas habilitados para dichos efectos***.

5.2.7. Estará prohibido el consumo de alimentos y bebidas al interior de las instalaciones de procesamiento de información (Data Centers o Salas de Servidores), así como en aquellas dependencias donde se mantenga o trabaje con documentos reservados o confidenciales que sean críticos para la operación de la institución. Será responsabilidad de cada jefatura asegurar que estas disposiciones se cumplan por las personas a su cargo.

5.2.8. No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.

5.2.9. El usuario***/a*** no tiene permitido manipular las estaciones de trabajo y los computadores portátiles.

5.2.10. Queda prohibido instalar cualquier tipo de software que no sean los debidamente licenciados y autorizados por UCOTI. Es por ello que, solo el personal autorizado de UCOTI puede instalar software y manipular las estaciones de trabajo para este efecto.

5.3. Pantallas limpias y cierre de sesión por inactividad

5.3.1. Los/as funcionarios/as deben velar por que la información dispuesta en las pantallas de los equipos de trabajo no quede expuesta a terceros o personal no autorizado, antes, durante y finalizada la jornada de trabajo, inclusive, cuando ésta no esté siendo utilizada.

5.3.2. ***Los/as funcionarios/as*** no deberá***n*** almacenar documentación ***y/***o información reservada o confidencial, en el escritorio de Windows (pantalla inicial) de la estación de trabajo, ***como tampoco en ninguna carpeta interna del computador, ya sea "descargas", "mis documentos" y/o cualquier carpeta creada por el/la funcionario/a. Por tanto, todo computador institucional debe estar libre de archivos institucionales***. Para esto, se han disponibilizado carpetas habilitadas en la nube ***de Google Drive*** y se ha entregado capacitación respecto a su uso.

5.3.3. Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active ante un tiempo de inactividad. El primer periodo de cierre corresponderá a un tiempo máximo de 3 minutos de inactividad en la estación de trabajo.

5.3.4. La pantalla de autentificación de la red de la institución debe requerir solamente la identificación de la cuenta usuario de dominio y su contraseña, y no entregar otra información.

5.3.5. Para desactivar el protector de pantalla y volver al modo normal de funcionamiento de la estación de trabajo, el sistema solicitará nuevamente la contraseña de dominio para ingresar ***a***l equipo.

5.3.6. Cada vez que los funcionarios/as se ausenten de su lugar de trabajo, deben bloquear su estación de forma manual con el fin de proteger el acceso a las aplicaciones y servicios de la institución. Para ambientes Windows, esto se realiza a través de la combinación de las teclas "Control" + "Alt" + "Supr" o "Inicio" + "L". Esto es responsabilidad única y exclusiva de cada usuario.

5.3.7. Una vez que el***/la*** funcionario***/a*** ha***ya*** terminado su jornada laboral, deberá apagar su estación de trabajo con la precaución de guardar toda información reservada o confidencial que pudiese estar sobre su escritorio físico.

5.3.8. Se deberá procurar no pegar autoadhesivos ni figuras en las pantallas.

5.3.9. Los***/as*** funcionarios***/as*** deben preocuparse por mantener sus equipos y estaciones de trabajo en buenas condiciones de limpieza externa.

5.3.10. La autenticación del usuario debe ser requerida toda vez que el equipo de trabajo se encienda, reinicie, bloquee o después de aparecer el protector de pantalla.

5.4. Protección de impresora

5.4.1. Cualquier información reservada o confidencial que va a ser impresa, debe ser retirada de inmediato, evitando el acceso a esa información por personas no autorizadas.

5.4.2. Las impresoras ubicadas en lugares de tránsito o de atención de público, deben estar protegidas de acceso no autorizado, a través del uso de credenciales de acceso.

5.4.3. Para resguardo de los puntos anteriores, se implementa la opción "impresión segura", en la cual se debe ingresar una contraseña en la impresora antes de que el documento enviado salga impreso, de no ingresar dicha contraseña, el documento quedará en cola sin ser liberado. ***Cabe destacar que, este punto solo puede ser liberado por situaciones excepcionales que así lo requieran, como por ejemplo, COVID 19, donde las personas deben evitar manipular equipos comunes para evitar contagios. Siempre teniendo la claridad del punto 5.4.1, donde se debe retirar la documentación obligatoriamente de forma inmediata.***

5.5. Salas y pizarras limpias

5.5.1. En las reuniones en que se utilicen pizarras o material visual, los responsables de dichas reuniones deberán asegurarse de que éstas queden limpias de la información y datos expuestos en ellas.

5.5.2. Cuando se utilicen estaciones de trabajo de uso común para realizar presentaciones, se debe eliminar toda la información expuesta y/o presentada.

5.5.3. Las salas o áreas de reuniones, salas de conferencias y de capacitación, deben quedar limpias de todo el material utilizado.

5.5.4. Al finalizar los eventos o reuniones que precisan equipos de proyección, audio o computación, quienes hayan hecho uso de los mismos deben asegurarse de apagarlos por completo y devolverlos donde corresponda, si se han utilizado mediante préstamo interno de equipos.

5.5.5. Se considera como sala de reunión virtual la plataforma de Google MEET, siendo la herramienta debidamente licenciada y facilitada por SERNAC para las reuniones virtuales, quedando prohibido cuando el anfitrión sea SERNAC utilizar otras salas de reuniones virtuales, tales como, Zoom, Teams, etc. En los casos en que SERNAC es invitado a alguna sala virtual, se puede conectar sin problemas a través de su navegador de internet.

5.5.6. Al utilizar Google MEET, se deben considerar y aplicar todos los resguardos necesarios para compartir información, adjuntar link y/o cualquier otro mecanismo

similar, si bien es una sala virtual, se debe tener los mismos resguardos que en una sala de reuniones física.

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 de 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 ***de la jefatura de continuidad operativa TI***, 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 DIFUSIÓN DE LA POLÍTICA

La difusión de la presente política se realizará mediante comunicaciones internas, informando a todos los funcionarios**/as** 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°881 de 11 de noviembre de 2019, y todas las anteriores que se hayan dictado en materia de Política de Escritorio y Pantalla Limpios.

3°. PUBLÍQUESE en el repositorio documental para su control y uso.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE
"Por orden del Director Nacional"

FELIPE VELÁSQUEZ SOLÍS
JEFE SUBDIRECCIÓN ESTRATEGIA, PROYECTOS INSTITUCIONALES Y SERVICIOS USUARIOS
SERVICIO NACIONAL DEL CONSUMIDOR

VVC/JOT/PHP
Distribución:
Dirección Nacional - Subdirección de Fiscalización - Subdirección Nacional - Subdirección Jurídica e Interpretación Administrativa - Subdirección de Procedimientos Voluntarios Colectivos - Departamento de Juicios - Subdirección de Consumo Financiero - Subdirección de Estudios Económicos y Educación - Subdirección de Estrategia, Proyectos Institucionales y Servicios Usuarios - Direcciones Regionales - Departamento de Gestión y Desarrollo de Personas - Departamento de Administración y Finanzas - Departamento de Operaciones y Servicios Logísticos - Departamento de Comunicaciones Estratégicas y Relacionamiento Institucional - Fiscalía Administrativa - Auditoría Interna - Unidad de Control de Gestión y Mejora de Procesos - Oficina de Partes.