



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Política
ESCRITORIO Y PANTALLA DESPEJADA

Código	
POL-SSI-11	
Versión	Revisión
05 13.11.2019	05
Página 1 de 6	

POL-SSI-11
**POLÍTICA ESCRITORIO Y
PANTALLA DESPEJADA**
PRESIDENCIA DE LA REPÚBLICA

Aprobado por: Julio Maiers Hechenleitner
Director Administrativo

NOTA DE SENSIBILIDAD Y PROPIEDAD INTELECTUAL

La información contenida en este documento es de Uso Interno, de propiedad y uso exclusivo de la Presidencia de la República para los fines que establezca. Solo podrá ser modificado con la venia de las autoridades que lo han aprobado.



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
Política
ESCRITORIO Y PANTALLA DESPEJADA

Código	
POL-SSI-11	
Versión	Revisión
05	05
13.11.2019	
Página 2 de 6	

Tabla de Contenidos:

1. Objetivo.....	3
2. Alcance.....	3
3. Roles y Responsabilidades	3
4. Definiciones (contenido).....	4
5. Periodicidad de Evaluación y Revisión.....	5
6. Difusión.....	5
7. Control de Cambios.	6

 Presidencia de la República Gobierno de Chile	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Política ESCRITORIO Y PANTALLA DESPEJADA		Código POL-SSI-11	
	Versión	Revisión		
	05 13.11.2019	05		
	Página 3 de 6			

1. Objetivo.

Establecer las actividades necesarias para la protección de la información digital e impresa, mediante la implementación de mecanismos pertinentes de control, con el propósito de evitar robos, pérdida, daños, o usos indebidos de la información.

2. Alcance.

El alcance de este documento aplica a cualquier tipo de soporte de información y a todas las instalaciones de procesamiento de información y estaciones de trabajo pertenecientes a la Presidencia de la República.

3. Roles y Responsabilidades.

- **Director Administrativo.**
Responsable de liderar la implantación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), asignando los recursos técnicos y humanos necesarios para mantener activo dicho sistema, mediante la promulgación de políticas internas que indiquen lineamientos y las obligaciones de las personas (usuarios) de la institución.
- **Integrantes del Comité de Seguridad de la Información.**
Responsables de apoyar y gestionar la implementación de los requisitos de seguridad de la información del SGSI para el correcto y adecuado uso de los activos de información de la Institución.
- **Encargado de Seguridad de la Información.**
Responsable de supervisar y coordinar las actividades de monitoreo, control y evaluación del SGSI de la institución para el cumplimiento de los requisitos de seguridad de la información.
- **Coordinadores del SGSI**
Responsables de gestionar el cumplimiento de los requisitos de seguridad del SGSI vinculados a su Departamento a través de la correcta aplicación de las políticas y procedimientos asociados.
- **Usuarios (personal de institución y personal externo).**
Responsables de aplicar y cumplir las responsabilidades y/o tareas que tengan definidas en las políticas y procedimientos de seguridad de la información de la institución.

 Presidencia de la República Gobierno de Chile	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Política ESCRITORIO Y PANTALLA DESPEJADA		Código	
			POL-SSI-11	
	Versión	Revisión		
	05 13.11.2019	05		
		Página 4 de 6		

4. Definiciones (contenido).

La Dirección Administrativa de Presidencia de la República se asegura de proteger la información almacenada en los escritorios de las estaciones de trabajo e instalaciones de procesamiento de información, mediante el establecimiento de mecanismos pertinentes que aseguren la protección de la información que se encuentre disponible.

Para el logro de lo anterior, se establecen controles en función de la criticidad de información, requisitos legales y contractuales aplicables, los riesgos a los activos determinados y los aspectos culturales y conductuales propios de la institución. Para ello, se establecen los siguientes lineamientos:

- a) Las estaciones de trabajo del personal de la institución se localizan preferentemente en ubicaciones que no queden expuestas al acceso de personas externas no autorizadas.
- b) Los equipos computacionales que queden ubicados cerca de zonas de atención o tránsito de público, deben situarse de forma que las pantallas no puedan ser visualizadas por personas externas.
- c) Los computadores de escritorio y portátiles tienen configurado el estándar relativo a protector de pantalla, de forma que se active bloqueando el acceso a la estación de trabajo después de un periodo de inactividad. El primer periodo de cierre corresponderá a los 5 minutos de inactividad en el PC, tras lo cual se activará el protector de pantalla, con mensajes acordes a las buenas prácticas de seguridad.
- d) Para el desbloqueo de los computadores de escritorio y portátiles, el sistema debe solicitar nuevamente la identificación del usuario y contraseña. Si el personal está ubicado cerca de zonas de atención de público, al ausentarse de su estación de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
- e) Toda vez que el personal se ausente de su estación de trabajo, junto con bloquear sus computadores de escritorio o portátiles, deben guardar, en un lugar seguro con restricción de acceso, cualquier documento o medio de almacenamiento de información removible que contenga información confidencial.
- f) Al finalizar su jornada laboral, el personal de la institución debe cerrar sesión apagando su estación de trabajo y guardar en un lugar seguro los documentos y medios que contengan información reservada o de uso interno.
- g) En caso que se utilice una estación de trabajo para presentaciones, si éste fuera de uso común, se debe eliminar la información antes presentada.
- h) La información reservada o crítica para la institución, ya sea, en medios de almacenamiento electrónico o papel, se debe mantener guardada bajo llave (según corresponda, gabinete, cajones u otras formas de muebles de seguridad), cuando no se esté utilizando y especialmente cuando la oficina esté desocupada.

 Presidencia de la República Gobierno de Chile	SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Política ESCRITORIO Y PANTALLA DESPEJADA		Código	
			POL-SSI-11	
	Versión	Revisión		
	05 13.11.2019	05		
				Página 5 de 6

- i) Las impresoras ubicadas en atención o tránsito de público, deben estar protegidas de acceso no autorizado. Cualquier información que va a ser impresa en cualquier impresora, debe ser retirada de ella en forma inmediata, evitando el acceso a esta información por personas no autorizadas.
- j) Cuando sea posible y se trate de información reservada, debe implementarse el control de impresión con el uso de clave por usuario.
- k) Disponer de un fondo de pantalla único para todos los usuarios.
- l) Los funcionarios deben mantener el puesto de trabajo libre de documentos considerados críticos, idealmente despejado y limpio. Por otra parte, no deben dejar notas y papeles con las claves de acceso pegados en la pantalla o en lugares de fácil acceso por terceras personas.
- m) Para las instalaciones de procesamiento de información se deben mantener protegidos con un mecanismo de bloqueo de pantalla y teclado mediante contraseña, según sea aplicable.

5. Periodicidad de Evaluación y Revisión.

Los lineamientos y alcances contenidos en esta política son susceptibles de mejorar continuamente, por lo tanto, son factibles de someter a modificaciones, actualizaciones y cambios periódicos tendientes a mantenerla vigente y aplicable de acuerdo con las condiciones en que la institución se encuentre.

Sin perjuicio de lo anterior, se establece que la periodicidad ordinaria de revisión de esta política es anual.

6. Difusión.

La presente política y sus lineamientos estratégicos están disponibles al personal bajo el control de la Presidencia de la República y terceros, según corresponda.

El mecanismo de difusión de esta política es:

- Publicación en la Intranet institucional.
- Publicación en el Portal de transparencia institucional.

7. Control de Cambios.

Versión	Fecha	Principales revisiones y/o modificaciones	Nº de revisión	Elaborado por	Revisado por	Aprobado por (responsable del documento)
01	31.03.2016	Versión inicial.	01	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
02	26.12.2016	-Actualización de documento según requerimientos de NCh-ISO 27001:2013. -El presente documento se aprueba bajo Resolución Exenta N° 2487, con fecha 26/12/2016.	02	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
03	07.11.2017	-Se actualiza codificación de este documento, se reemplaza "POL-TIC-04" por "POL-SSI-05", producto de una nueva forma de identificar los documentos (todas las páginas, encabezado del documento) -Se incorporan las tablas "Objetivo y Productos estratégicos y Procesos Críticos en ámbito de aplicación del PMG-SSI PRESIDENCIA" y "Alcance de Dominios y Controles de Seguridad de la Información asociados a este documento" (páginas 3 y 4, sección 2.-Alcance o Ámbito de Aplicación. <u>-Se incorpora en página 4 la sección 4.- Materias que aborda el documento.</u> -Se posiciona al final del documento la tabla de Historial de versiones (control de cambios) incorporando en columna "Principales Modificaciones" el texto (Página / Sección) y se crea una nueva columna denominada "Motivo del Cambio", (página 8 / sección 10.- Historial de versiones (control de cambios). -El presente documento se aprueba bajo Resolución Exenta N° 2080, con fecha 07.11.2017	03	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
04	19.11.2018	- Ajuste a Sección alcance, página 3. -El presente documento se aprueba bajo Resolución Exenta N° 2001, con fecha 19.11.2018	04	Encargado de Seguridad de la Información.	Depto. de TIC.	Director Administrativo
05	13.11.2019	Se ajusta nombre codificación y contenido de política según los requisitos del control NChISO27001 A.11.2.9 y un nuevo orden establecido para el SGSI institucional. -El presente documento se aprueba bajo firma electrónica del Director Administrativo	05	Encargado de Seguridad de la Información.	Jefatura Depto. de TIC.	Director Administrativo