

# Política de Escritorios y pantallas limpias

- Equipo de usuario desatendido
- Política de escritorio y pantalla limpios

1 INDICE

<b>1</b>	<b>INDICE .....</b>	<b>2</b>
<b>2</b>	<b>OBJETIVO .....</b>	<b>3</b>
<b>3</b>	<b>ALCANCE .....</b>	<b>3</b>
<b>4</b>	<b>ROLES Y RESPONSABILIDADES .....</b>	<b>3</b>
<b>5</b>	<b>CONTROL NORMATIVO SSI .....</b>	<b>4</b>
<b>6</b>	<b>DEFINICIONES .....</b>	<b>4</b>
6.1	Impresoras limpias.....	4
6.2	Escritorio limpio.....	4
6.3	Pantalla limpia .....	5
6.4	Escritorio desentendido.....	5
<b>7</b>	<b>DIFUSIÓN .....</b>	<b>6</b>
<b>8</b>	<b>PERIODICIDAD DE EVALUACION Y REVISIÓN .....</b>	<b>6</b>
<b>9</b>	<b>FORMALIZACION EXTERNA .....</b>	<b>6</b>
<b>10</b>	<b>REGISTRO, REVISION Y ACTUALIZACION HISTORICO .....</b>	<b>7</b>
<b>11</b>	<b>FORMALIZACIÓN.....</b>	<b>8</b>

- Equipo de usuario desatendido
- Política de escritorio y pantalla limpios

## 2 OBJETIVO

El presente documento tiene por finalidad proteger toda la información institucional que pudiere estar accesible en los puestos de trabajo asignados a los usuarios internos del Servicio, que se considere importante para el logro de la misión y objetivos institucionales, independiente de la forma en que dicha información este almacenada o contenida.

## 3 ALCANCE

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios para el Gobierno Regional Metropolitano.

## 4 ROLES Y RESPONSABILIDADES

El Departamento de Informática es responsable de velar el cumplimiento de esta política.

El funcionario es el responsable del orden de su puesto de trabajo y de la administración todos los activos de información que formen parte de sus tareas sean estas de carácter crítico, confidenciales o sensibles, de manera de evitar vulnerabilidades y que puedan comprometer al Servicio.

Cada jefatura es responsable por la Seguridad de la Información en sus grupos de trabajo y deberá instruir a cada funcionario sobre la importancia en el manejo de los activos de información.



- **Equipo de usuario desatendido**
- **Política de escritorio y pantalla limpios**

## 5 CONTROL NORMATIVO SSI

La siguiente política tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.11.02.08	Equipo de usuario desatendido	Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.
A.11.02.09	Política de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.

## 6 DEFINICIONES

Una política de escritorio despejado/pantalla despejada reduce el riesgo del acceso al personal no autorizado, la pérdida o daño de la información durante y fuera de las horas laborales normales.

### 6.1 Impresoras limpias

Se Considerará el uso de impresoras con función de código PIN, validado por Tarjeta Personal de manera que los originadores sean los únicos que puedan obtener sus impresiones y solo al estar al lado de la impresora.

### 6.2 Escritorio limpio

La información sensible o crítica para el Servicio, es decir, en medios de almacenamiento electrónico (pendrive) o papel, no se deberá dejar sobre los escritorios, se deberá mantener guardada bajo llave (idealmente en una caja fuerte o gabinete u otras formas de muebles de seguridad) cuando no se necesite, especialmente cuando la oficina esté desocupada.

No se deberá dejar en la pantalla Post it con las claves del equipo u otra información sensible.

No deberán dejarse carpetas con información sensible sobre los escritorios, de manera que puedan ser accedidas por personas no autorizadas a la información que contienen.

No se deberá consumir alimentos ni bebidas cerca de los equipos computacionales.

- **Equipo de usuario desatendido**
- **Política de escritorio y pantalla limpios**

No se deberá tener sobre el escritorio elementos que pudiesen dañar los activos de información como tazas de café, refrescos o líquidos en general.

### 6.3 Pantalla limpia

Se deberían mantener desconectados a los computadores y terminales o protegidos con un mecanismo de bloqueo de pantalla y teclado mediante una contraseña, token o mecanismo de autenticación de usuario similar cuando se deja sin supervisar y se debería proteger con bloqueos de tecla, contraseñas u otros controles cuando no está en uso.

No se permitirá que el usuario solo apague su pantalla no sin antes dejar el sistema bloqueado.

Deberá considerarse un protector de pantalla automático con tiempo determinado, en el entendido que el usuario podría olvidarse de activar su protector de pantalla cuando no en su escritorio.

### 6.4 Escritorio desentendido

Cada vez que el usuario se ausente de su escritorio o lugar de trabajo deberá bloquear su equipo a fin de proteger el acceso a archivos o datos almacenados en él.

Respecto de las claves, se debería exigir al usuario seguir las prácticas de la organización en el uso de información de autenticación o clave secreta, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad. (Para mayor información respecto la autenticación de claves, por favor referirse al Procedimiento de gestión de claves).

La clave de acceso deberá ser requerida cada vez que el equipo se encienda, se bloquee, se reinicie o se active el protector de pantalla.

- Equipo de usuario desatendido
- Política de escritorio y pantalla limpios

## 7 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

## 8 PERIODICIDAD DE EVALUACION Y REVISIÓN

La siguiente Política será revisada, evaluada y/o actualizada según corresponda y aprobada su vigencia una vez al año por el Comité de Seguridad de la Información, en cuanto a su funcionamiento y correcta aplicación en la Institución.

## 9 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política de escritorios y pantallas limpias.



- Equipo de usuario desatendido
- Política de escritorio y pantalla limpios

## 10 REGISTRO, REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08-16	Creación Documento
02	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. <ul style="list-style-type: none"> <li>• Se incorpora control normativo SSI</li> <li>• Se incorpora registro de control</li> </ul>
03	Mauricio Marín	todas	27-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.
04	Mauricio Marin V.	6	2-08-2018	Se agrega en Registro de Control el siguiente párrafo: En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo. Se cambia título 6 por Definiciones. Se cambia título 7 por Registro de Operación y se señala que el informe de revisión será de manera anual. Se cambia título 9 por periodicidad de evaluación y revisión
05	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
06	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
07	Carlos Hernández	6	17-11-2021	Se agrega capítulo 9 formalización externa
08	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI  
CONTROLES NCh-ISO 27001

- Equipo de usuario desatendido
- Política de escritorio y pantalla limpios

Página 8 de 8


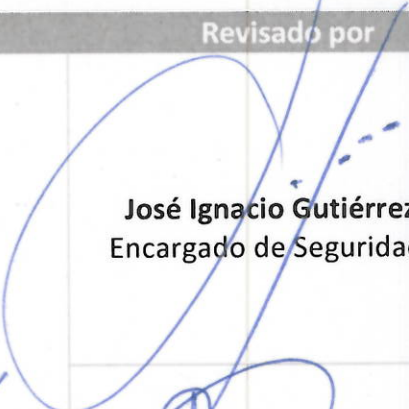
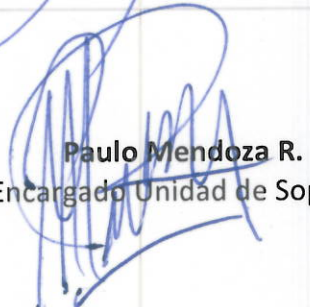


Versión: 08/21

A.11.02.08

A.11.02.09

Fecha: 23/11/2021

## 11 FORMALIZACIÓN

Elaborado por	Revisado por	Aprobado por
 <b>Carlos Hernández A.</b> Analista Departamento de Informática	 <b>José Ignacio Gutiérrez G.</b> Encargado de Seguridad SSI	
	 <b>Paulo Mendoza R.</b> Encargado Unidad de Soporte	 <b>Mayuri Reyes T.</b> Presidente Comité de Seguridad
	 <b>Carolina Hidalgo M.</b> Jefa Departamento Planificación y Control Institucional	



**ACTA DE REUNION: Comité de Seguridad de la Información**

<b>Objetivo</b>	Situación SSI año 2021
<b>Fecha y Hora</b>	23-11-2021, 15:00
<b>Lugar</b>	Sala de Reunión 2° Piso

**PUNTOS DE LA REUNION**

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
  - a. Caída de Switch piso 5 - 13 de septiembre 2021
  - b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
  - a. Switch
  - b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

**Aprobación los siguientes documentos**

1. Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio
2. Manual de gestión de archivos
3. Norma de acceso a la Red
4. Norma de Eliminación de Activos
5. Norma de la Seguridad de la información para la Gestión de Proyectos
6. Norma de Outsourcing
7. Norma de Trabajo Remoto
8. Norma de uso identificación y autenticación
9. Norma de uso de instalación legal de software
10. Norma de reutilización y devolución de activos
11. Plan de Continuidad
12. Plan de emergencia Institucional
13. Política clasificación de activos
14. Política de acceso físico
15. Política de correo electrónico e Internet
16. Política de Derechos de propiedad Intelectual
17. Política de desarrollos de sistemas

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

#### DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.



**Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas**

**Silvana Torres entrega información**

- **Acerca del expurgo de documentos**
- **2022 se enviará soporte en papel a archivo nacional**
- **Se está digitalizando documentación antigua**
- **Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808**

**José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando**

**Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI**

**Se aprueban políticas y documentación SSI**

**Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes**





GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

ACTA DE ASISTENTES  
COMITÉ DE SEGURIDAD DE LA  
INFORMACION

Página 1 de 1

Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
09	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	IAF	
11			
12			
13			