



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

NORMA DE USO IDENTIFICACIÓN Y  
AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS

Página 1 de 15

Versión: 06

Código: NOR-SSI-003

Fecha: 12/07/2019

# Norma de uso Identificación y autenticación de Sistemas Informáticos



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

NORMA DE USO IDENTIFICACIÓN Y  
AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS

Página 2 de 15

Versión: 06

Código: NOR-SSI-003

Fecha: 12/07/2019

## 1 INDICE

|      |   |    |
|------|---|----|
| 1    | INDICE .....  | 2  |
| 2    | OBJETIVO .....  | 3  |
| 3    | ALCANCE .....   | 3  |
| 4    | ROLES Y RESPONSABILIDADES .....   | 3  |
| 5    | CONTROL NORMATIVO .....   | 4  |
| 6    | IDENTIFICACION Y AUTENTICACION.....   | 5  |
| 7    | DESARROLLO DE LA NORMA .....  | 5  |
| 7.1  | Administración de la información de autenticación secreta .....                                     | 5  |
| 7.2  | Uso de la información de autenticación.....   | 5  |
| 7.3  | Sistemas de administración de claves o contraseñas .....  | 6  |
| 7.4  | Solicitud de cambio de autenticación secreta .....  | 6  |
| 7.5  | Procedimientos Documentados.....  | 6  |
| 8    | REGISTROS DE CONTROL.....   | 6  |
| 9    | Monitoreo.....  | 7  |
| 10   | PROCEDIMIENTOS DE OPERACION PARA CREACION CLAVE DE USUARIO A TRAVES DE<br>DIAGRAMAS DE FLUJOS ..... | 8  |
| 11   | PROCEDIMIENTO DE OPERACIÓN PARA CAMBIO DE CLAVE SISTEMAS A TRAVES DE<br>DIAGRAMA DE FLUJOS .....    | 9  |
|      | .....   | 9  |
| 12   | DIFUSIÓN.....   | 10 |
| 13   | REVISIÓN .....  | 10 |
| 14   | ANEXOS .....  | 11 |
| 14.1 | Formulario de creación o cambio de autenticación secreta.....                                       | 11 |
| 14.2 | Formulario solicitud cambio de contraseña.....  | 12 |
| 15   | APROBACIÓN.....   | 13 |
| 16   | REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES.....  | 14 |

Toda versión impresa de este documento se considera como Copia No Controlada



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

NORMA DE USO IDENTIFICACIÓN Y  
AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS

Página 3 de 15

Versión: 06

Código: NOR-SSI-003

Fecha: 12/07/2019

## 2 OBJETIVO

El acceso a la información de los sistemas del Gobierno Regional Metropolitano de Santiago será solo otorgado a usuarios identificados y autenticados. El Gobierno Regional Metropolitano de Santiago establecerá los procedimientos y controles para otorgar, cambiar y finalizar acceso a los sistemas de información.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también problemas jurídicos tanto nacionales como internacionales.

## 3 ALCANCE

Las normas mencionadas en el presente documento cubren el uso apropiado de los sistemas y los métodos de identificación y autenticación del Gobierno Regional Metropolitano de Santiago y aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios al Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución o que transite por la red del Gobierno Regional Metropolitano de Santiago

## 4 ROLES Y RESPONSABILIDADES

Los funcionarios deben comprender sus responsabilidades para salvaguardar los ID's de identificación (nombre de usuario) y sus contraseñas. Deberá notificar inmediatamente a un supervisor, jefe directo o Departamento de Informática si sospechan que una contraseña u otro sistema credenciales han sido comprometidos.

Los usuarios tienen la obligación de no registrar los identificadores o contraseñas en ~~paper~~

Los usuarios no deben almacenar identificadores en un computador de manera desprotegida.

Es absoluta responsabilidad del usuario al terminar su jornada laboral o al no estar frente a su computador debe cerrar su sesión de usuario.

El usuario debe configurar su computador para el uso de protector de pantalla y que este solicite contraseña para iniciar sesión nuevamente.

Está absolutamente prohibido a los usuarios permitir que los sistemas recuerden las contraseñas o identificadores de sistemas. Tampoco deberán incluir el identificador en cualquier proceso de inicio de sesión automatizado. (Ej. Macros)

**Toda versión impresa de este documento se considera como Copia No Controlada**

Los Jefes de Departamento y de Unidad se asegurarán de que su personal cumpla con todas las directrices que figuran en esta política, además notificarán sin demora al Departamento de Informática la Información de las cuentas que deben ser desactivadas, y deberán reportar cualquier sospecha o violaciones compromisos de las credenciales al Departamento de Informática.

El Encargado de seguridad de la información, implementará métodos de autenticación para los sistemas de información en su cuidado, instruyendo a los usuarios en cuanto a su uso.

El Departamento de Informática preparará directrices y normas para las credenciales de usuario, con accesos restringidos según su perfil y aprobará la emisión de las credenciales.

Los desarrolladores de sistemas deben garantizar que sus sistemas soportan los procedimientos y directrices especificadas en este documento normativo

## 5 CONTROL NORMATIVO

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

| <b>Código del Control</b> | <b>Identificación del Control</b>                           | <b>Requisito de control</b>   |
|---------------------------|---|---|
| A.09.02.04                | Gestión de información secreta de autenticación de usuarios | Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.                          |
| A.09.03.01                | Uso de información de autenticación secreta                 | Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta. |
| A.09.04.03                | Sistema de gestión de contraseñas                           | Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.                                  |
| A.12.01.01                | Procedimientos de operación documentados                    | Los procedimientos de operación se deben documentar, y poner a disposición de todos los usuarios que los necesiten.                     |

|   |  |                     |
|---|--|---------------------|
| <br>GOBIERNO REGIONAL<br>METROPOLITANO DE<br><b>SANTIAGO</b> | <b>GOBIERNO REGIONAL METROPOLITANO – SSI</b><br><br><b>NORMA DE USO IDENTIFICACIÓN Y<br/> AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS</b> | Página 5 de 15      |
|   |  | Versión: 06         |
|   |  | Código: NOR-SSI-003 |
|   |  | Fecha: 12/07/2019   |

## 6 IDENTIFICACION Y AUTENTICACION

El método específico de autenticación para cada sistema deberá ser proporcional con el nivel de sensibilidad del sistema para tener acceso (es decir, mientras más sensibles sean los sistemas se deberá utilizar métodos de autenticación más fuerte). Varios métodos de autenticación (por ejemplo, uso de la contraseña) puede ser necesaria para la sensibilidad de alta - confidencialidad o de alto riesgo.

## 7 DESARROLLO DE LA NORMA

### 7.1 Administración de la información de autenticación secreta

Para todos los sistemas de información, el Departamento de Informática del Gobierno Regional Metropolitano, creará claves de autenticación secreta mediante un proceso de administración formal, previa verificación de identidad, a través del cual se individualizará al usuario, el sistema, derechos de administración sobre el sistema, definiendo si es un usuario normal, uno avanzado o uno con niveles de administrador.

Las autenticaciones secretas temporales serán creadas por defecto en la instalación inicial del sistema, y será una clave estándar, la cual deberá ser cambiada cuando el usuario inicie su próxima sesión. El usuario deberá confirmar el ingreso de su autenticación secreta, digitando dos veces su nueva autenticación secreta. Una vez cambiada la autenticación secreta deberá ingresar con su nombre de usuario y su nueva clave para de esta manera verificar la identidad del usuario en el sistema. Una vez realizado esto, deberá firmar un documento que identifica el cambio de la clave estándar por su nueva autenticación secreta.

Con lo anteriormente descrito, el usuario ya estará en condiciones de acceder al sistema con su propia clave.

### 7.2 Uso de la información de autenticación

A los funcionarios, cualquiera sea su calidad jurídica, se les hará firmar un documento que declare que las claves son personales e intransferibles.

La clave deberá tener una longitud mínima, y no podrán basarse en nombres de hijos o familiares fáciles de adivinar. La clave deberá cambiarse si se sospecha que esta ha sido comprometida o vulnerada.

Las claves temporales deberán ser cambiadas en el primer inicio de sesión

**Toda versión impresa de este documento se considera como Copia No Controlada**



### 7.3 Sistemas de administración de claves o contraseñas

Los usuarios deberán ser forzados al uso de claves secretas o contraseñas, de manera de mantener su información resguardada

El Departamento de Informática les permitirá a los usuarios cada cierto tiempo cambiar sus propias contraseñas, permitiéndoles confirmar las nuevas claves y evitar errores de digitación.

El sistema deberá mantener un registro para evitar claves o contraseñas utilizadas con anterioridad.

Todos estos procedimientos deberán quedar documentados y a disposición de los funcionarios en cualquier momento.

### 7.4 Solicitud de cambio de autenticación secreta

Para el cambio de clave de un funcionario cuando este no esté presente, o se vea imposibilitado de hacerlo personalmente, deberá ser solicitado por su jefatura directa mediante correo electrónico el que debe ser respaldado además con la solicitud formal del cambio de clave mediante el formulario Solicitud Cambio de Contraseña

### 7.5 Procedimientos Documentados

Todos estos procedimientos, así como las demás Políticas, reglamentos, y normas deberán quedar documentados de manera electrónica en la Intranet del Servicio, quedando a disposición de todos los usuarios para cuando ellos lo requieran.

## 8 REGISTROS DE CONTROL

El Departamento de Informática deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.09.02.04 Informe de creación y mantención de usuarios
- A.09.03.01 Informe de usuarios con recepción de clave secreta conforme
- A.09.04.03 Informe de cambio de claves al inicio de la primera sesión, haciendo hincapié en Sistema de gestión de claves de calidad
- A.12.01.01 Informe de publicación de procedimientos en Intranet

El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

|   |   |                     |
|---|---|---------------------|
|  | <b>GOBIERNO REGIONAL METROPOLITANO – SSI</b><br><br><b>NORMA DE USO IDENTIFICACIÓN Y<br/>AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS</b> | Página 7 de 15      |
|   |   | Versión: 06         |
|   |   | Código: NOR-SSI-003 |
|   |   | Fecha: 12/07/2019   |

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.

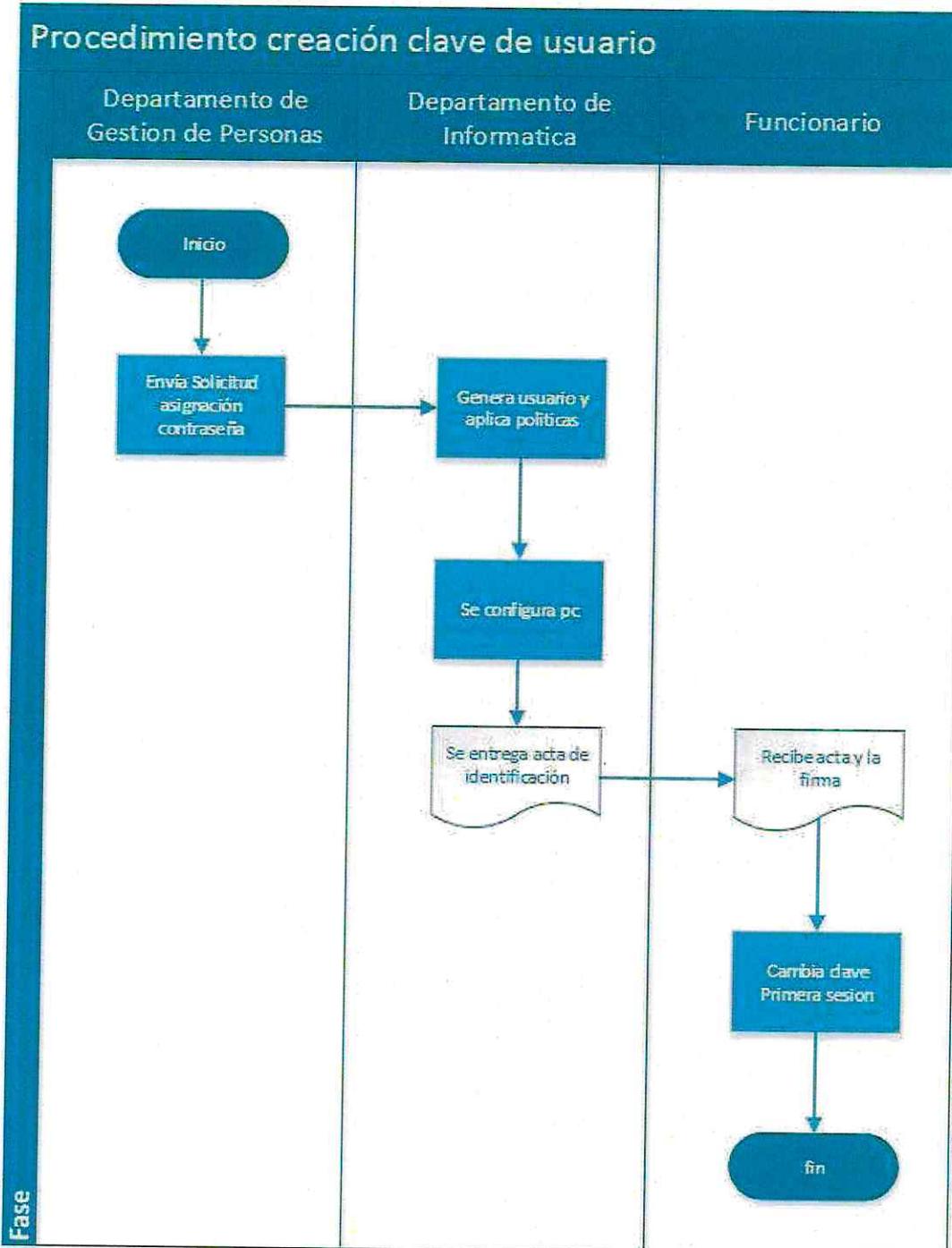
Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable)

## 9 Monitoreo

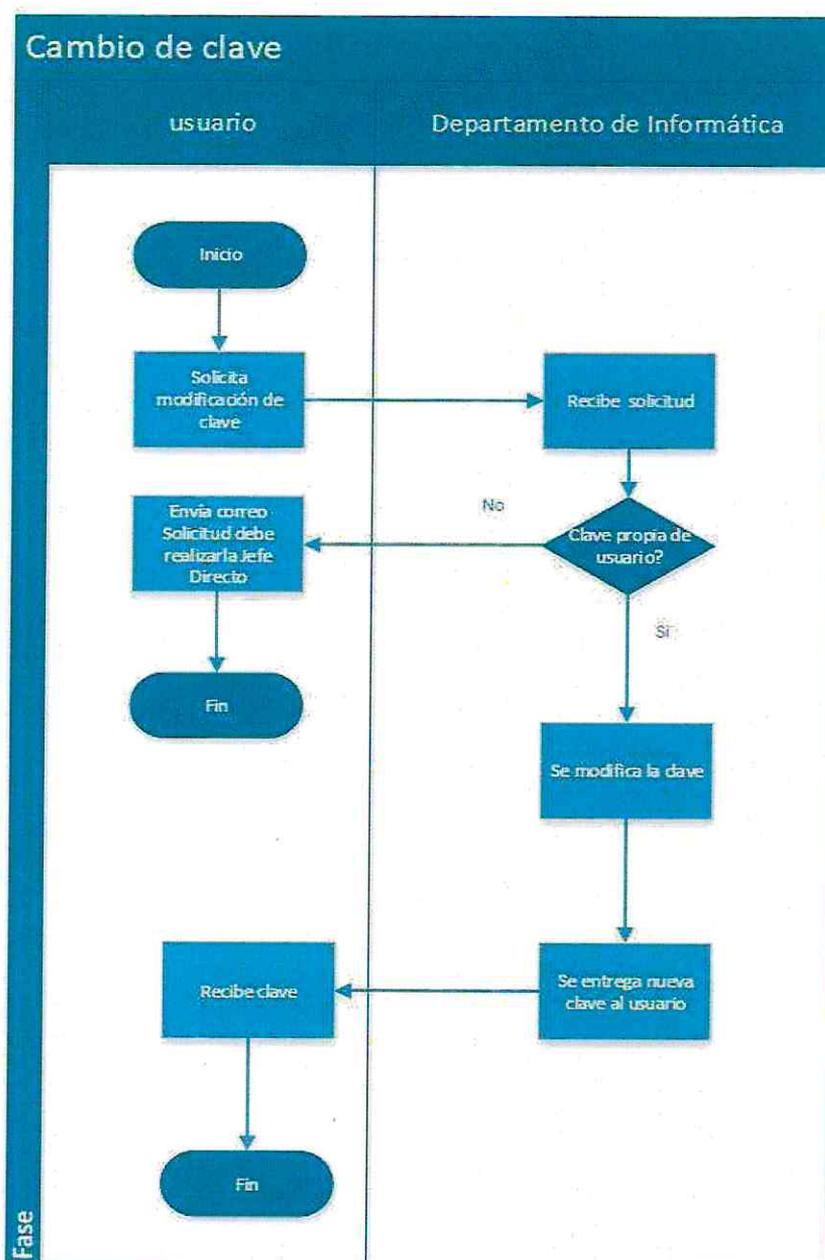
El Departamento de Informática controlará la identificación y autenticación de los usuarios de los sistemas informáticos provistos por el Gobierno Regional Metropolitano de Santiago, evitando el mal uso de la infraestructura disponible.

Lo descrito anteriormente, se realiza con el fin de proporcionar información para el caso de revisiones.

10 PROCEDIMIENTOS DE OPERACION PARA CREACION CLAVE DE USUARIO A TRAVES DE DIAGRAMAS DE FLUJOS



## 11 PROCEDIMIENTO DE OPERACIÓN PARA CAMBIO DE CLAVE SISTEMAS A TRAVES DE DIAGRAMA DE FLUJOS



|   |   |                     |
|---|---|---------------------|
| <br><b>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</b> | <b>GOBIERNO REGIONAL METROPOLITANO – SSI</b><br><br><b>NORMA DE USO IDENTIFICACIÓN Y AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS</b> | Página 10 de 15     |
|   |   | Versión: 06         |
|   |   | Código: NOR-SSI-003 |
|   |   | Fecha: 12/07/2019   |

## 12 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.

## 13 REVISIÓN

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

|   |   |                     |
|---|---|---------------------|
| <br><b>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</b> | <b>GOBIERNO REGIONAL METROPOLITANO – SSI</b><br><br><b>NORMA DE USO IDENTIFICACIÓN Y AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS</b> | Página 11 de 15     |
|   |   | Versión: 06         |
|   |   | Código: NOR-SSI-003 |
|   |   | Fecha: 12/07/2019   |

## 14 ANEXOS

### 14.1 Formulario de creación o cambio de autenticación secreta



**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS  
DEPARTAMENTO DE INFORMÁTICA**



**ACTA DE ENTREGA DE IDENTIFICACIÓN**

Acta de entrega de Identificación

**IDENTIFICACIÓN DE FUNCIONARIO**

Nombre de Funcionario: \_\_\_\_\_ RUN: \_\_\_\_\_

Departamento: \_\_\_\_\_ Fecha de Entrega: / / \_\_\_\_\_

Nombre de Usuario: \_\_\_\_\_

Clave de acceso: \_\_\_\_\_

Mediante el presente la persona anteriormente individualizada toma conocimiento según lo establecido en la Política Gestión de Claves de este Gobierno Regional. Que deberá hacer cambio de la clave entregada en el siguiente inicio de sesión, que esta tendrá una duración de tres meses, que pasado este tiempo deberá crear nueva contraseña la cual no puede ser igual a las últimas diez utilizadas, deberá ser alfanumérica, deberá tener una longitud mínima de ocho caracteres, deberá considerar el uso de mayúsculas y minúsculas, además de caracteres especiales.

\_\_\_\_\_  
FIRMA FUNCIONARIO

|   |   |                     |
|---|---|---------------------|
| <br><b>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</b> | <b>GOBIERNO REGIONAL METROPOLITANO – SSI</b><br><br><b>NORMA DE USO IDENTIFICACIÓN Y AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS</b> | Página 12 de 15     |
|   |   | Versión: 06         |
|   |   | Código: NOR-SSI-003 |
|   |   | Fecha: 12/07/2019   |

## 14.2 Formulario solicitud cambio de contraseña



**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS  
DEPARTAMENTO DE INFORMÁTICA**



**SOLICITUD CAMBIO DE CONTRASEÑA**

**DATOS SOLICITANTE**

Nombre de Funcionario: \_\_\_\_\_ RUN: \_\_\_\_\_  
 Departamento: \_\_\_\_\_ Fecha de Solicitud: \_\_\_\_/\_\_\_\_/\_\_\_\_

Mediante el presente la persona anteriormente individualizada, solicita al Departamento de Informática gestionar el cambio de contraseña para el funcionario sr(a) \_\_\_\_\_.

De acuerdo a lo establecido en la Política Gestión de Claves de este Gobierno Regional.

\_\_\_\_\_  
FIRMA SOLICITANTE



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

NORMA DE USO IDENTIFICACIÓN Y  
AUTENTICACIÓN DE SISTEMAS INFORMATICOS

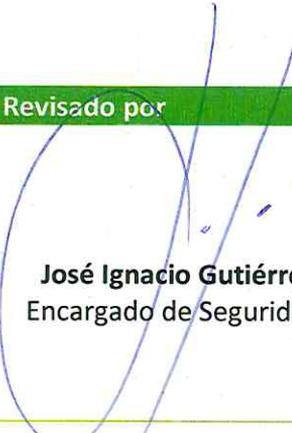
Página 13 de 15

Versión: 06

Código: NOR-SSI-003

Fecha: 12/07/2019

## 15 APROBACIÓN

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

## 16 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

| Versión | Autor             | Página o secciones | Fecha Modificación | Motivo  |
|---------|-------------------|--------------------|--------------------|---|
| 01      | Carlos Hernández  | todas              | Agosto 2011        | Creación  |
| 02      | Carlos Hernández  | todas              | Diciembre 2016     | <ul style="list-style-type: none"> <li>• Cambio diseño</li> <li>• Se incorpora periodicidad de evaluación</li> <li>• Se incorpora periodicidad de revisión</li> <li>• Se incorpora Roles y responsabilidades</li> </ul>   |
| 03      | Mauricio Marín    | todas              | 24/10/ 2017        | <p>Actualización y Modificación de documento para cumplimiento a directrices de la red de expertos SSI.</p> <ul style="list-style-type: none"> <li>• Se incorpora control normativo SSI</li> <li>• Se incorpora registro de control</li> <li>• Agrega anexos de creación modificación clave de usuarios</li> <li>• Agrega flujogramas de procedimientos de</li> </ul> |
| 04      | Mauricio Marin V. | 6                  | 1/08/2018          | <p>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.</p>  |



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

NORMA DE USO IDENTIFICACIÓN Y  
AUTENTIFICACIÓN DE SISTEMAS INFORMATICOS

Página 15 de 15

Versión: 06

Código: NOR-SSI-003

Fecha: 12/07/2019

|    |                 |       |            |   |
|----|-----------------|-------|------------|---|
| 05 | Mauricio Marin  | 6     | 3/12/201   | Se agrega el título de Procedimientos Documentados                  |
| 06 | Matias Benitez. | Todas | 12-07-2019 | Comité de la seguridad de la información aprueba revisión año 2019. |

Toda versión impresa de este documento se considera como Copia No Controlada



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

## ACTA DE REUNIÓN COMITÉ DE SEGURIDAD DE LA INFORMACION

Página 1 de 3

Fecha 12/07/2019

### ACTA DE REUNIÓN: Comité Seguridad de la Información

|               |                                     |
|---------------|-------------------------------------|
| Objetivo:     | Situación SSI primer semestre 2019. |
| Fecha y Hora: | 12 de Julio de 2019 10:00 horas     |
| Lugar:        | Sala de Reunión 6º Piso             |

### PUNTOS DE LA REUNIÓN

- Bienvenida
- Actualización de Controles SSI, correspondiente a cada departamento.
- Cumplimiento SSI 2019 primer semestre.
- Vulnerabilidades primer semestre 2019.
- Phishing GORE.
- Afiche SSI
- Revisión documentación vigente.

### DESARROLLO DE LA PRESENTACIÓN

Se le recuerda al Comité los controles comprometidos para dar cumplimiento a PMG-SSI 2019. También se informa la fecha de entrega al departamento de informática (18 al 24 de Julio 2019) y cuando se tiene que hacer el reporte a la red de expertos (Primera semana de Agosto).

Implementación de plataforma <https://onlyoffice.gobiernosantiago.cl> , para hacer la entrega de controles. La cual Carlos Hernández envió una invitación al correo electrónico de los integrantes del comité.

Sebastián Benussi enviará modificación de "Procedimiento de Controles de Auditorías de Sistemas de la Información".

En el Segundo semestre 2019, se trabajará en la unificación del "Manual de Gestión de Archivos", "Política Manejo de activos", "Política clasificación de activos" y "Norma de Eliminación de Activos" del Departamento Gestión Documental.

Se exponen las vulnerabilidades presentadas durante el primer semestre del 2019; corte de luz, FTP y Central telefónica.

Se informó del Phishing enviado a los funcionarios y se evidenció los resultados que se obtuvieron en este ejercicio.

Se presentó Afiche SSI implementado en el mes de julio.

Revisión de documentación SSI vigente:

- Política de correo electrónico e Internet
- Política de dispositivos móviles
- Política de Derechos de propiedad Intelectual



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

## ACTA DE REUNIÓN COMITÉ DE SEGURIDAD DE LA INFORMACION

Página 2 de 3

Fecha 12/07/2019

- Política Gestión de Personas
- Instructivo correctivo preventivo
- Manual de gestión de archivos
- Norma de acceso a la Red
- Norma de la Seguridad de la información para la Gestión de Proyectos
- Norma de Outsourcing
- Norma de Trabajo Remoto
- Norma de uso identificación y autenticación
- Norma de uso de instalación legal de software
- Norma de reutilización y devolución de activos
- Plan de emergencia Institucional
- Política clasificación de activos
- Política de acceso físico
- Política de desarrollos de sistemas
- Política de escritorios y pantallas limpias
- Política de gestión de incidentes de seguridad
- Política de gestión de la capacidad
- Política de la seguridad informática
- Política de respaldo de la información
- Política general de seguridad de la información
- Política gestión de claves
- Política manejo de activos
- Política sobre el uso de controles criptográficos
- Procedimiento de control de las vulnerabilidades técnicas
- Procedimientos de Auditoria de Sistemas de Información
- Protocolo y control de tratamiento de SSI



GOBIERNO REGIONAL  
METROPOLITANO DE  
SANTIAGO

## ACTA DE REUNIÓN COMITÉ DE SEGURIDAD DE LA INFORMACION

Página 3 de 3

Fecha 12/07/2019

### Asistencia a Reunión Comité Seguridad de la Información



Asistentes Comité de Seguridad de la Información

Página 1 de 1

Fecha: 12/07/2019

|    | Nombre              | Unidad                                | Firma |
|----|---------------------|---------------------------------------|-------|
| 1  | Jose Gutierrez      | Departamento de Informática           |       |
| 2  | Alejandro Segura    | Div. Administracion y Finanzas        |       |
| 3  | Fernando Fuenzalida | Departamento Juridico                 |       |
| 4  | Carolina Hidalgo    | Planificacion y Control Institucional |       |
| 5  | Jennifer Lueiza     | Depto. De Gestion de Personas         |       |
| 6  | Sebastian Benussi   | Depto. Auditoria Interna              |       |
| 7  | Juan Catalan        | Depto. De Servicios Generales         |       |
| 8  | Silvana Torres      | Depto. De Gestion Documental          |       |
| 9  | Ariel Lagos         | Depto. De Gestion de Personas         |       |
| 10 | Carlos Hernandez    | Departamento de Informática           |       |
| 11 | Matías Benítez      | Departamento de Informática           |       |
| 12 |                     |                                       |       |
| 13 |                     |                                       |       |
| 14 |                     |                                       |       |
| 15 |                     |                                       |       |