Política
Gestión de Claves

1 INDICE

2 OBJETIVO

Establecer en una política las actividades necesarias para la gestión de claves y derechos de acceso de usuarios a los sistemas de información, de manera de proteger las contraseñas de desde su creación, cambio y eliminación de las mismas en el Gobierno Regional Metropolitano, manteniendo niveles de seguridad en los distintos niveles sean: usuarios normales, usuarios avanzados y administradores.

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

Jefatura de Unidad, Departamento o División.	• Autorizar el Ingreso de Nuevos Funcionarios y notificar • Solicitar la creación o eliminación de los accesos a los sistemas de información. • Notificar cualquier desvinculación de funcionarios
Funcionario designado del Departamento de Gestión de Personas.	• Solicitar los accesos a los sistemas de información. • Notificar cualquier desvinculación de funcionarios. • Recopilar y revisar los antecedentes mínimos para el inicio de trámites de ingreso y asignación de derechos de accesos provisorios.
Departamento de Informática	• Crear los accesos básicos a los nuevos funcionarios • Revisar y gestionar los permisos de accesos a los sistemas de información • Eliminar los derechos de accesos de los funcionarios que se desvinculan.
Encargado de Seguridad de la información	• Coordinar la Revisión de derechos de acceso de usuario.
Funcionarios	• Las responsabilidades de los funcionarios se describen en el punto 6.2

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.09.02.01	Registro y cancelación de registro de usuario	Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar los derechos de acceso.
A.09.02.02	Asignación de acceso de usuario	Debe existir un procedimiento formal de asignación de acceso de usuario para asignar o revocar lo derechos de acceso para todos los tipos de usuario, a todos los sistemas y servicios.
A.09.02.03	Gestión de derechos de acceso privilegiados	Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiados.
A.09.02.06	Eliminación o ajuste de los derechos de acceso	Se deben retirar los derechos de acceso de todos los empleados, y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio.
A.09.04.01	Restricción de acceso a la información	Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.
A.09.04.02	Procedimiento de inicio de sesión seguro	Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro
A.10.01.02	Gestión de claves	Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas, a través de todo su ciclo de vida.

6 DEFINICIONES

6.1 Consideraciones generales

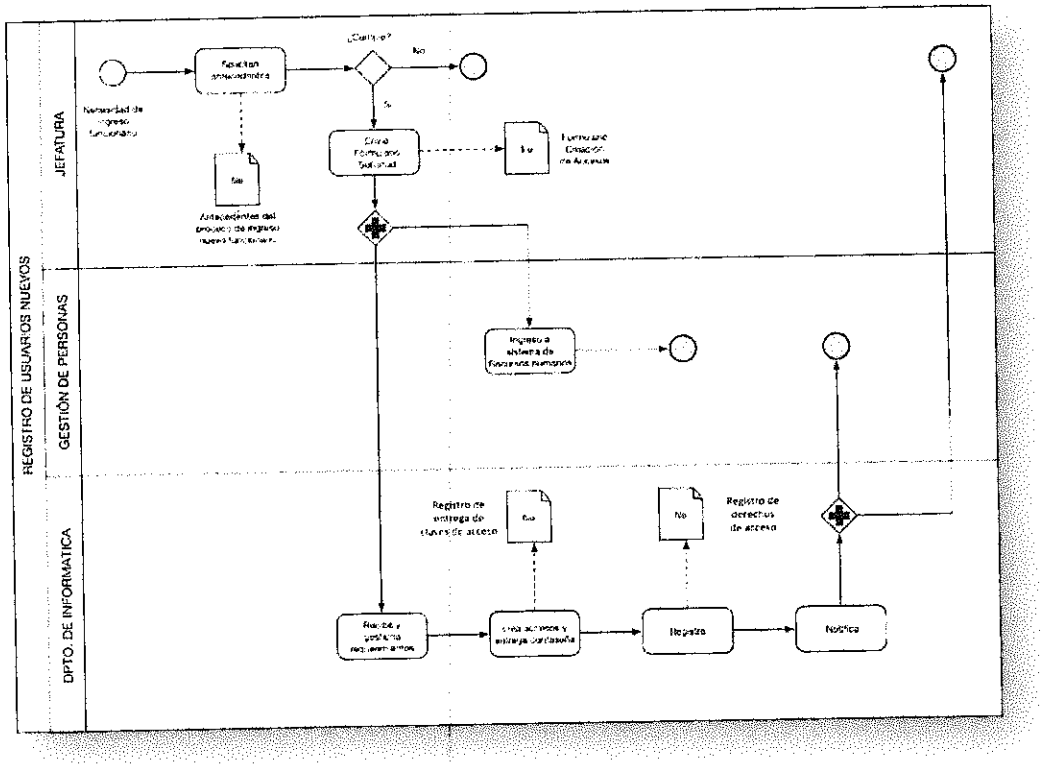
En cualquier registro de usuarios se deben utilizar ID´s únicos para permitir a los usuarios vincularse y ser responsables de sus acciones.

Es responsabilidad de los Administradores de Sistemas mantener un registro formal de todas las personas registradas para usar el servicio, de manera de asegurarse de que las IDs de usuarios redundantes no se emitan a otros usuarios.

El Departamento de Informática deberá eliminar o deshabilitar inmediatamente las IDs de los usuarios que han dejado de ser parte del Gobierno Regional Metropolitano.

6.2 Asignación de acceso de usuarios

La creación de los accesos de nuevos funcionarios (correo electrónico, active Directory, estaciones de trabajo, acceso a sistemas), se debe realizar de acuerdo al siguiente flujo.



La Jefatura de la Unidad, Departamento o División es responsable de solicitar los accesos básicos para los nuevos funcionarios mediante el **Formulario de solicitud para creación / eliminación de accesos**[1]

La Unidad de Soporte del Departamento de Informática es responsable de la creación de los accesos básicos de ingreso, que incluye:

- Creación de correo Electrónico.
- Creación de usuario en Active Directory
- Creación de usuario en sistemas necesarios
- Habilitación de estación de trabajo

La entrega de las contraseñas temporales de ingreso se realiza mediante el **Registro de entrega de claves de acceso**[2], que es firmado por el funcionario que lo recepciona, quedando una copia en poder de soporte y otra en poder del funcionario.

En el registro de entrega de claves de acceso se proporciona un enunciado con las responsabilidades implicadas en el uso de los sistemas de información del Gobierno regional Metropolitano[3].

Las condiciones de uso incluyen:

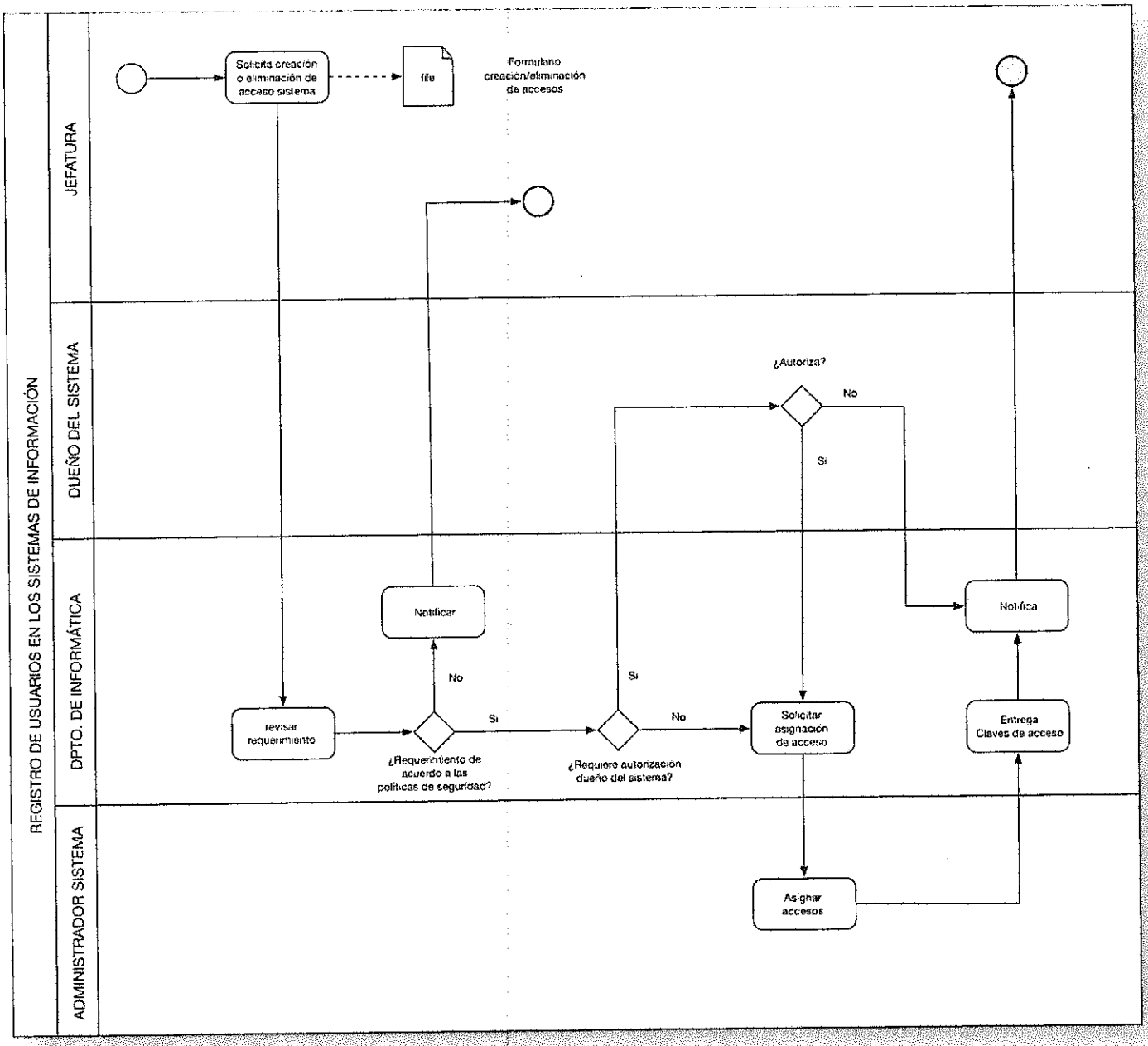
- Mantener confidenciales las claves secretas.
- Cumplir con lo establecido en las Políticas y Procedimientos del Sistema de Seguridad de la Información, en lodo lo que sea de su competencia.
- No divulgar información pertinente al Gobierno Regional Metropolitano.
- Entender la responsabilidad funcionaria, aún fuera de las dependencias de trabajo y fuera del horario normal de trabajo.

La creación de accesos se registra en la Planilla de **Registro de Derechos de Acceso**[4].

[1] Ver anexo 1 con formato de registro.
[2] Ver anexo 2 con formato de registro.
[3] Los requerimientos de seguridad para el uso de correo electrónico y la gestión de contraseñas, están definidos en la Política de Correo Electrónico, Norma de uso identificación y autentificación y la Política de la seguridad informática.
[4] Ver anexo 3 con formato de registro.

6.3 Gestión de derechos de acceso privilegiados

La creación o eliminación de accesos privilegiados a los sistemas de información se debe realizar de acuerdo al siguiente flujo:



6.4 Eliminación o ajuste de derechos de acceso

La Jefatura de la Unidad, Departamento o División es responsable de solicitar la creación o eliminación de los accesos a los sistemas de Información mediante el **Formulario de solicitud de creación/eliminación de accesos** firmado.

El Departamento de Informática es responsable ante cualquier solicitud de ajuste de derechos de acceso de chequear que el nivel de acceso solicitado es apropiado para el propósito institucional y que sea consistente con la Política(s) de Seguridad de la Organización.

En caso de ser necesario se debe solicitar la autorización de acceso del usuario a los sistemas, al propietario para su uso y/o acceso.

Las claves secretas temporales deben ser proporcionadas a los usuarios de una manera segura.

6.5 Restricción de acceso a la información

Cada jefe de Departamento será el encargado de definir los niveles de restricción de acceso a la información según las funciones o roles necesarios para cada funcionario.
Éstos deben ser informados al Departamento de Informática para de esta forma controlar los inicios de sesión seguros para los distintos sistemas.

6.6 Procedimiento de inicio de sesión seguro

Los controles de inicio de sesión son una forma de implementar la función de la autenticación de usuario de manera de impedir el acceso no autorizado a los sistemas de información.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final o cancelación de los derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Con todo lo anterior, el Departamento de Informática controlará el acceso a los sistemas computacionales a través de IDs únicas, provistas de sus respectivas claves para cada usuario permitiendo el inicio de sesión a los sistemas o aplicaciones mediante confrontación y validación de éstas con los perfiles del Active Directory

Algunas medidas a tener en cuenta para el inicio de sesión seguro:

- No mostrar la contraseña
- Proteger contra intentos de inicio de sesión fallidos
- Proteger contra intentos de inicio de sesión forzado
- Deshabilitar autocompletar

6.7 Gestión de contraseñas del usuario

Es responsabilidad de todos los funcionarios cumplir con los siguientes requerimientos:

6.7.1 Características de contraseñas

- Las contraseñas temporales deben ser proporcionadas a los usuarios de una manera segura, no se deben utilizar mensajes de correo electrónico de terceros o no protegidos (sin texto).
- Las contraseñas de acceso creadas por el usuario deben ser difíciles de adivinar por terceros y ser sólo de su conocimiento personal, quedando prohibida su divulgación, así como mantener anotada su clave de acceso en un lugar visible.
- Los sistemas de información deben validar la robustez de las contraseñas de los usuarios.
- Las contraseñas de acceso de los usuarios deben contar con un archivo histórico, debidamente encriptado, con el objetivo de no permitir reutilizar una clave de acceso utilizada recientemente.
- Las contraseñas nunca deberían ser almacenadas de una forma desprotegida (ej. Contraseñas almacenadas en el navegador, post-it, cuadernos, etc.).
- Toda contraseña predeterminada debe ser cambiada después de la instalación de los sistemas o software.

6.7.2 Cambio de las contraseñas

- La contraseña temporal de una cuenta de usuario, se creará expirada, de modo de obligar su cambio durante el **Primer Acceso** [5].
- Los usuarios deben cambiar su contraseña de acceso con la frecuencia establecida por la Unidad de Soporte, como mínimo esta será cada 3 meses y será establecida por GPO

en Active Directory

- Las contraseñas deben ser únicas para cada funcionario y deben cumplir, a lo menos, con los siguientes requisitos:
  - Debe contener 8 caracteres como mínimo.
  - No debe contener: los nombres o apellidos del funcionario, el user name o nombre de usuario, el nombre de la institución o unidad funcional.
  - No debe contener palabras completas.
  - Contener al menos un carácter de las siguientes categorías.

Categoría	Ejemplo
Letras Mayúsculas	A, B, C
Letras Minúsculas	A, b, c
Números	0,1,2,3,4,5,6,7,8,9
Símbolos	“, -, %, $, ¡, ¿.....

Ejemplo de Contraseña segura: **“J0Ab77c3**

Para el buen uso de este procedimiento, se establecerá una GPO que obligue al cumplimiento de lo antes indicado

6.7.3 Intentos Fallidos

- **El número de intentos erróneos de acceso a una cuenta, debe estar limitado según se indique en el estándar definido por la Unidad de Soporte del Departamento de Informática.** Los intentos fallidos establecidos por GPO es de 3 intentos
- De cumplirse el número de intentos fallidos definido, la cuenta debe quedar bloqueada, siendo los únicos autorizados para su desbloqueo la Unidad de Soporte del Departamento de Informática.
- Toda reasignación de contraseña debe ser solicitada por el Jefe directo del usuario titular de la cuenta mediante correo electrónico además deberá firmar el formulario existente.
- El Departamento de informática llevara un registro de estas solicitudes.

[5] Ver anexo 5

6.8 Revisión de derechos de acceso de usuarios

La administración de los perfiles radica en los usuarios encargados de los sistemas de información y las jefaturas de División correspondiente.

Para administrar los accesos a los sistemas de información se definirán perfiles de acceso asignables a grupos de usuarios que, por su responsabilidad en la organización, presenten necesidades de accesos equivalentes.

- El Encargado de Seguridad de la información es responsable de que se efectúe la revisión de los derechos de acceso de acuerdo a los siguientes lineamientos:
- Se debe revisar los derechos de acceso de los usuarios cada seis meses.
- Las autorizaciones para derechos de acceso con privilegios especiales se deben revisar a intervalos de tres meses.
- Se debe chequear la asignación de privilegios para asegurar que no se hayan obtenido privilegios no autorizados.
- Chequeo de IDs de usuario y cuentas redundantes.
- Revisión después de cualquier cambio, como un ascenso, democión o término de contrato.

Los Usuarios Encargados de alguna aplicación deben revisar en forma periódica los perfiles de usuarios del personal vigente y solicitar al Jefe del Departamento de Informática la actualización de éstos cada vez que ocurra un cambio en la definición de funciones.

6.9 Eliminación de derechos

La Jefatura del Área involucrada es responsable de informar cualquier desvinculación o movimientos de funcionarios mediante el Formulario de solicitud para creación/eliminación de accesos. (anexo 6)

Esta notificación debe ser enviada en simultáneamente a:

- Departamento de Gestión de Personas.
- Departamento de Informática.

Ante el informe de desvinculación de algún funcionario, el Departamento de Informática es responsable de gestionar la recuperación de los activos asignados al funcionario. Entre otros, se encuentran:

- Equipamiento

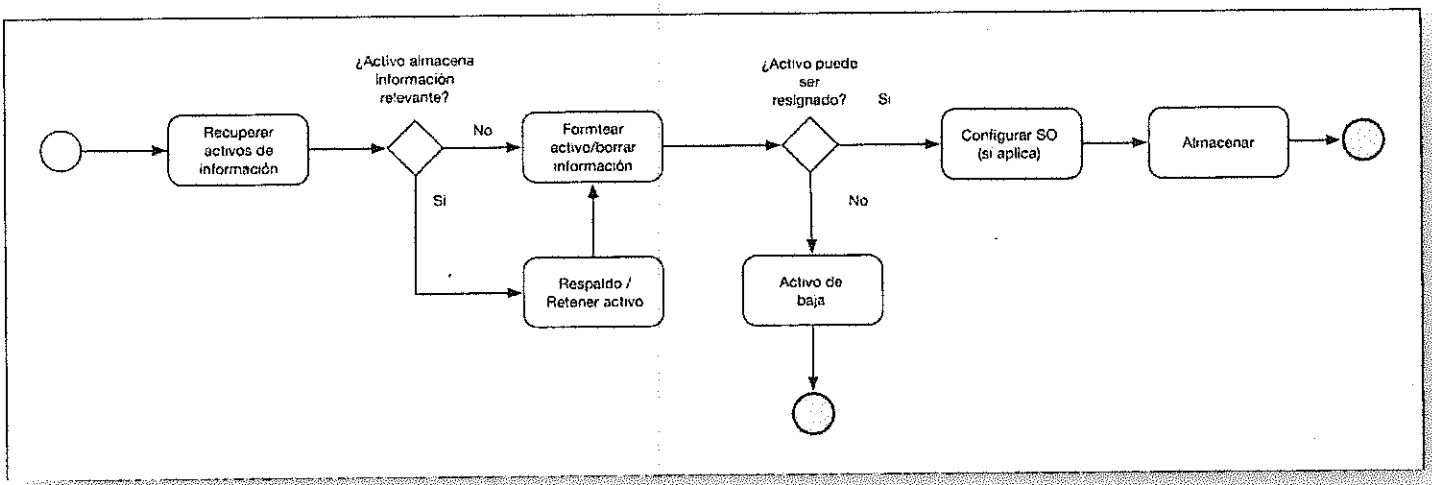
- Teléfonos móviles
- Tablets
- Pendrives
- Notebook

Los activos recuperados deben ser informados a la Unidad de Inventario del Departamento de Servicios Generales.

El Departamento de Informática es responsable de eliminar los derechos de acceso a los sistemas de información (cambio de contraseñas, eliminación de usuario según sea requerido). El Departamento de Informática además es responsable de eliminar los derechos de las tarjetas de acercamiento.
Junto con recuperar los activos de información asignados al funcionario. Entre otros, se encuentran:

- Discos Duros.
- CD - DVD de respaldos.
- Software.
- Manuales.
- Cualquier Información almacenada en medios electrónicos.

La recuperación de activos de información se realizará de acuerdo al siguiente modelo:



7 ANEXOS

7.1 ANEXO 1: Formulario de solicitud de asignación de contraseña

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

SOLICITUD ASIGNACIÓN CONTRASEÑA

DATOS SOLICITANTE

Nombre de Funcionario:_____ RUN:_____

Departamento:_____ Fecha de Solicitud:__/__/_____

Mediante el presente la persona anteriormente individualizada, solicita al Departamento de Informática gestionar la creación de usuario para el funcionario.

Nombre completo_____
Run:_____
División/Departamento:_____
Calidad Jurídica:_____
Cargo:_____
Fecha de Ingreso:_____
Fecha de Egreso _____

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

_____
FIRMA SOLICITANTE

7.2 ANEXO 2: Registro de acta de entrega de identificación:

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 ultimas 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.

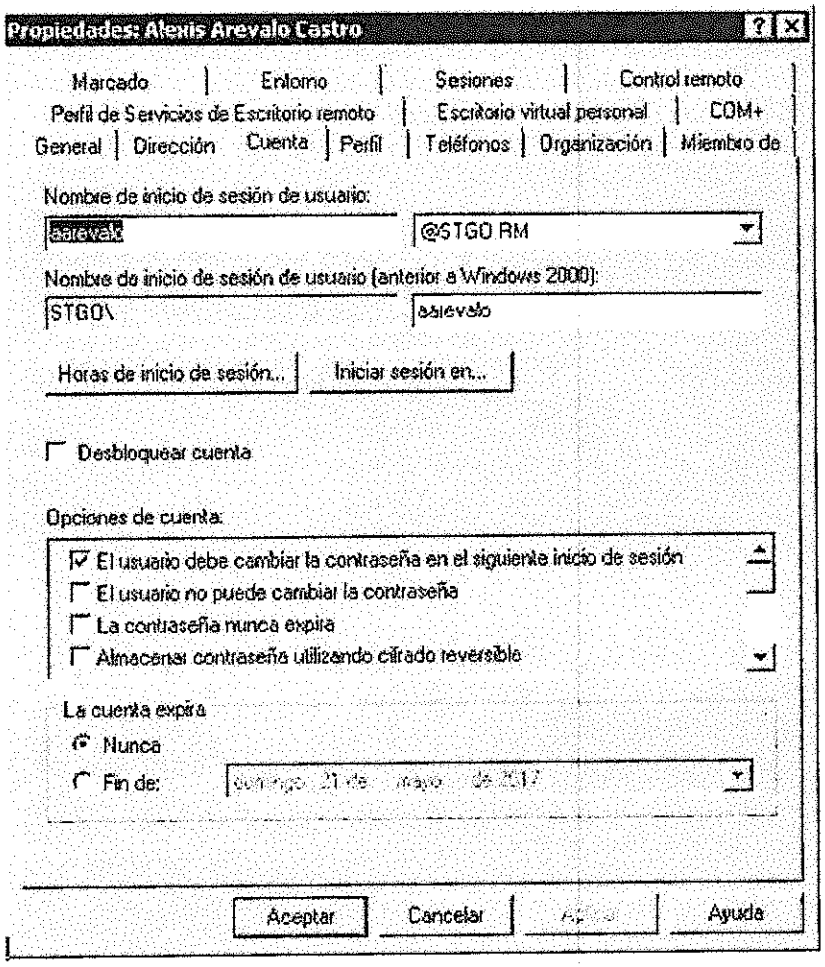
_____
FIRMA FUNCIONARIO

7.3 ANEXO 3: Registro de derechos de acceso:

stg

Tipo Acceso	Solicitado por	funcionario	Fecha	Sistema o carpeta	Usuario	Nivel de acceso	Grupo de acceso	Ip usuario	Técnico autoriza
carpeta	Juan Pérez	Matías Hernández	13/07/2016	RRHH	mhernandez	administrador	administradores	172.16.0.16	pmendoza
sistema	Roberto Olea	Pablo Espinoza	16/07/2016	\\172.16.0.20\tesoreria	pespinoza	lectura	Tesorería lectura	172.16.067	cramirez

7.4 ANEXO 4: Registro de cambio de clave en primer inicio de sesión



7.5 Anexo 5: 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 Politica Gestión de Claves de este Gobierno Regional.

_____
FIRMA SOLICITANTE

7.6 Anexo 6: Formulario de solicitud para creación/eliminación de accesos

DIVISIÓN DE DESARROLLO TERRITORIAL Y PLANIFICACIÓN
DEPARTAMENTO DE INFORMÁTICA

stg

FORMULARIO DE SOLICITUD PARA CREACIÓN ELIMINACIÓN DE ACCESOS

Tipo de Solicitud

Creación de Usuario ☐

Acceso de Sistemas ☐

Eliminación de accesos ☐

Fecha Solicitud ____/____/_____

Jefatura que Solicita

Nombre Completo:_____

Depto. O Unidad:_____

Identificación del Funcionario

Nombre Completo:_____

RUN:_____

División o Departamento:_____

Calidad Jurídica:_____

Fecha de Ingreso a la Institución:_____

Sistema(s) a los que se solicita acceso / eliminación

_____

Firma Jefatura

Bandera 46 • Santiago de Chile • Tel. 56-22 [illegible] • www.gobiernosantiago.cl

8 DIFUSIÓN

La presente Política 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.

9 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.

10 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política gestión de claves.

11 REGISTRO DE 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	10-08-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control
03	Mauricio Marín	8	18-10-17	• Agrega registro de inicio de sesión • Agrega anexo Solicitud de Contraseña • Agrega Anexo Solicitud cambio de contraseña • Agrega anexo acta entrega de identificación Agrega Formulario de solicitud para creación/eliminación de accesos
04	Mauricio Marin V.	13	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 Operaciones 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	20	17-11-2021	Se agrega capítulo 10 formalización externa
08	Carlos Hernandez	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021

12 FORMALIZACIÓN

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

stg SANTIAGO	**ACTA DE REUNION** **COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información

Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	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 autentificación**
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 PRESENTACIÓN

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

stgo 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	DAF	
11			
12			
13			