Norma de uso
Identificación y autentificación de Sistemas Informáticos

1 INDICE

2 OBJETIVO

El acceso a la información de los sistemas del Gobierno Regional Metropolitano de Santiago será solo otorgado a usuarios identificados y autentificados. 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 autentificación 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 papel

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)

Los Jefes de Departamento y de Unidad se asegurarán de que su personal cumpla con todas las directrices que figuran en esta política, además notificaran 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

Código del Control	Identificación del Control	Requisito de control
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.

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 autentificación 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

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 autentificación 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.

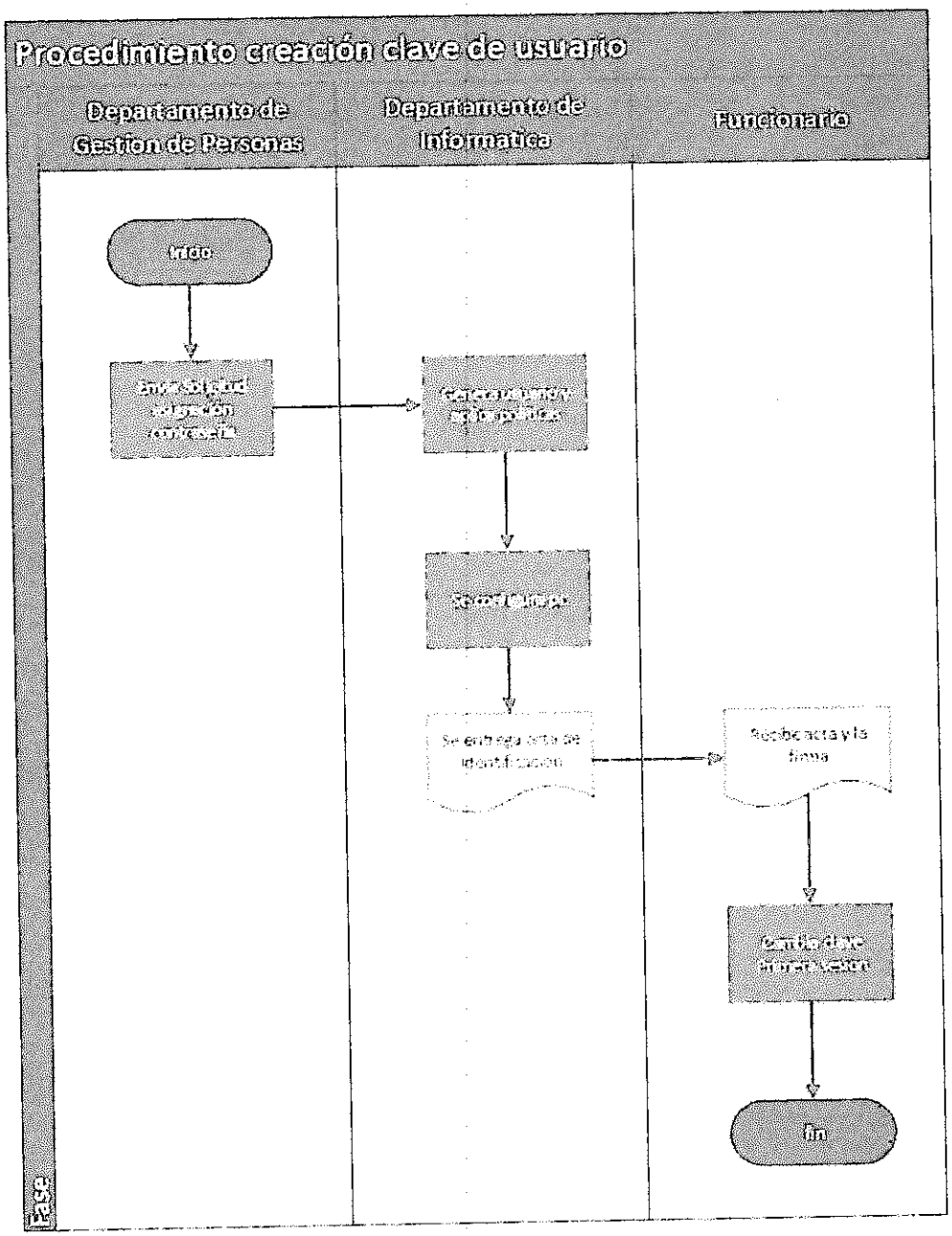
En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.

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)

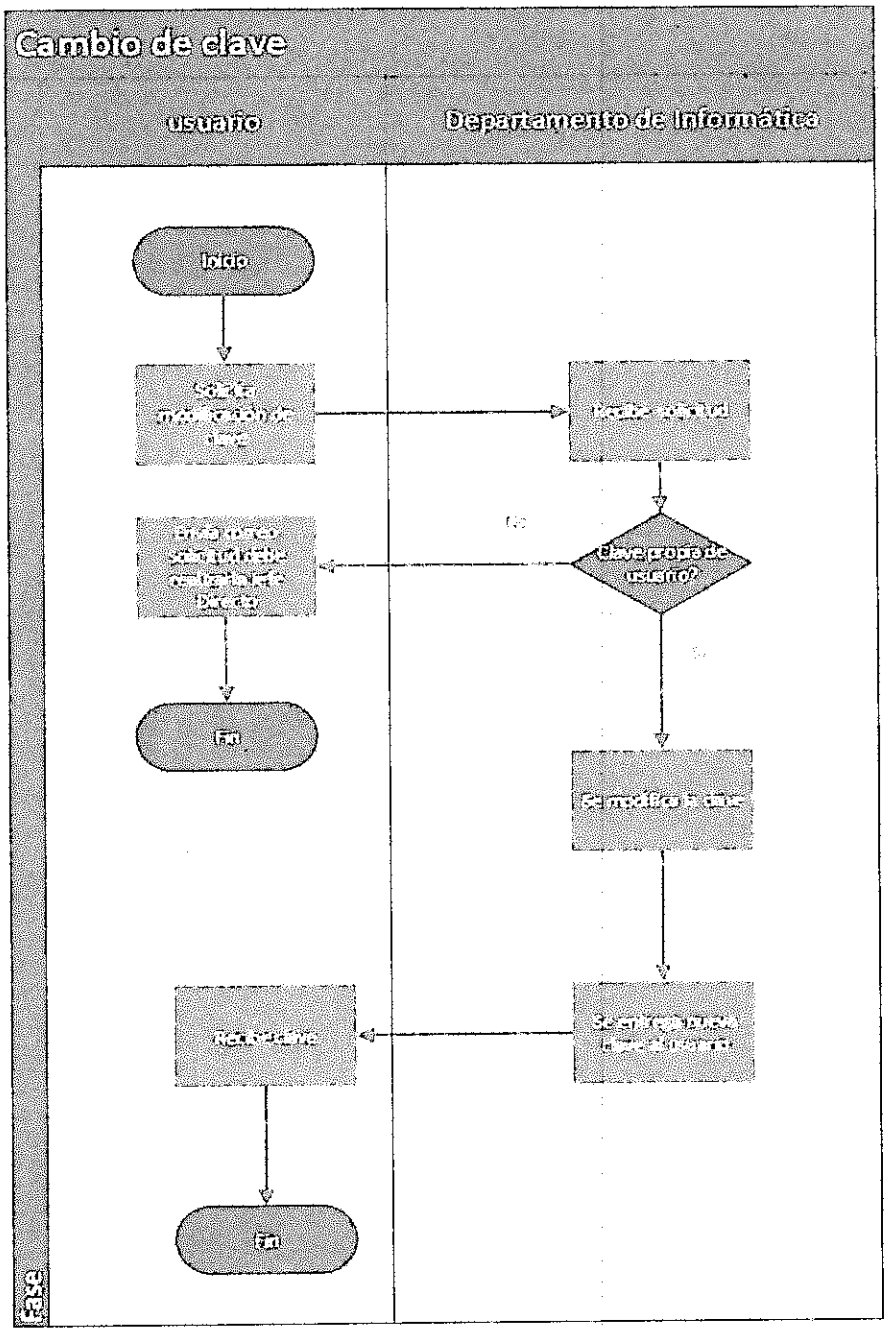
9 Monitoreo

El Departamento de Informática controlará la identificación y autentificación 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



12 ANEXOS

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMATICA

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

12.1 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 Politica Gestión de Claves de este Gobierno Regional.

_____
FIRMA SOLICITANTE

13 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.

14 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.

15 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Norma de uso identificación y autenticacion.

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	• Cambio diseño • Se incorpora periodicidad de evaluación • Se incorpora periodicidad de revisión • Se incorpora Roles y responsabilidades
03	Mauricio Marín	todas	24/10/ 2017	Actualización y Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control • Agrega anexos de creación modificación clave de usuarios • Agrega flujogramas de procedimientos de procedimientos
04	Mauricio Marin V.	6	1/08/2018	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.
05	Mauricio Marin	6	3/12/201	Se agrega el título de Procedimientos Documentados
06	Matias Benitez.	Todas	12-07-2019	**Comité SSI revisa y aprueba año 2019.**

07	Carlos Hernández	12	15-11-2021	Se agrega capítulo 15 formalización externa Se actualiza índice
08	Carlos Hernández	todas	23-11-2021	Comité SSI revisa y aprueba año 2021

17 FORMALIZACION

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 SUPERINTENDENCIA DE TRANSPORTE 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 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

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	
	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			