Intendencia
Región de los Lagos

Ministerio del Interior y Seguridad Pública

APRUEBA MANUAL DE INDUCCIÓN SOBRE SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

RES. EXENTA N° J 1290

PUERTO MONTT, 3 de diciembre de 2012

VISTOS:

a) Lo dispuesto en la Ley N° 19.175 Orgánica Constitucional sobre Gobierno y Administración Regional;
b) El Decreto con Fuerza de Ley N° 22 de 1959, Ley Orgánica del Servicio de Gobierno Interior de la República;
c) Ley 18.575 sobre Bases Generales de la Administración de Estado;
d) La Ley N° 18.834 sobre Estatuto Administrativo;
e) La Resolución N° 1.600 de octubre de 2008 de la Contraloría General de la República.

Y CONSIDERANDO:

La importancia de formalizar el manual de inducción sobre Sistema de Seguridad de la Información, con el objeto que los funcionarios de éste Servicio, puedan conocerlo y aplicarlo en sus actividades diarias.

La necesidad de dar a conocer, fomentar e impulsar la seguridad de la información en los funcionarios de éste Servicio.

RESUELVO:

APRUEBASE el manual de inducción sobre Sistema de Seguridad de la Información, cuyo texto íntegro es el siguiente:

C-1426493~~7~~
1426493 8

SECRETARIO ABOGADO V°B°

Intendencia
Región de los Lagos

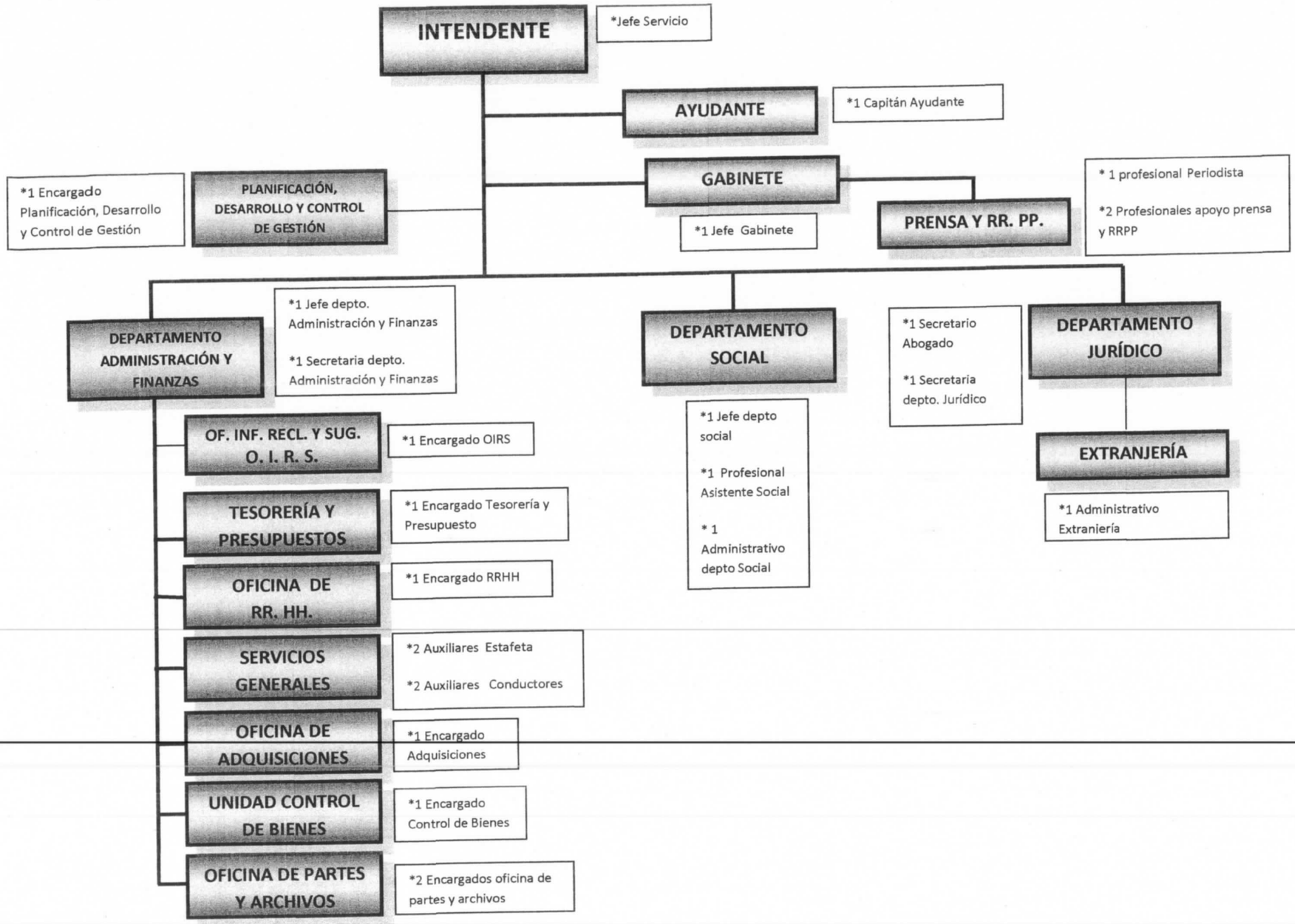
Ministerio del
Interior y
Seguridad Pública

MANUAL DE PROCEDIMIENTO DE INDUCCIÓN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 2012

INTENDENCIA REGIONAL DE LOS LAGOS

Introducción:

- La Intendencia Regional de Los Lagos, es una Unidad operativa del Servicio de Gobierno Interior, dependiente del Ministerio del Interior y Seguridad Pública.
- La estructura Orgánica de la Intendencia, se describe en el Organigrama que se presenta a continuación, en el que se indican los diferentes Departamentos que la constituyen.
- Posee 24 funcionarios que desarrollan diferentes labores al interior del servicio.
- Con el objeto de dar a conocer, fomentar e impulsar la Seguridad de la Información, en los funcionarios (as) que ingresan a la Intendencia, en cualquier calidad jurídica, se ha elaborado el presente Manual de Inducción en Sistema de Seguridad de la Información.


INTENDENTE
*Jefe Servicio
AYUDANTE
*1 Capitán Ayudante
GABINETE
*1 Jefe Gabinete
PRENSA Y RR. PP.
* 1 profesional Periodista
*2 Profesionales apoyo prensa y RRPP
PLANIFICACIÓN, DESARROLLO Y CONTROL DE GESTIÓN
*1 Encargado Planificación, Desarrollo y Control de Gestión
DEPARTAMENTO ADMINISTRACIÓN Y FINANZAS
*1 Jefe depto. Administración y Finanzas
*1 Secretaria depto. Administración y Finanzas
OF. INF. RECL. Y SUG. O. I. R. S.
*1 Encargado OIRS
TESORERÍA Y PRESUPUESTOS
*1 Encargado Tesorería y Presupuesto
OFICINA DE RR. HH.
*1 Encargado RRHH
SERVICIOS GENERALES
*2 Auxiliares Estafeta
*2 Auxiliares Conductores
OFICINA DE ADQUISICIONES
*1 Encargado Adquisiciones
UNIDAD CONTROL DE BIENES
*1 Encargado Control de Bienes
OFICINA DE PARTES Y ARCHIVOS
*2 Encargados oficina de partes y archivos
DEPARTAMENTO SOCIAL
*1 Jefe depto social
*1 Profesional Asistente Social
* 1 Administrativo depto Social
DEPARTAMENTO JURÍDICO
*1 Secretario Abogado
*1 Secretaria depto. Jurídico
EXTRANJERÍA
*1 Administrativo Extranjería

Consideraciones generales:

La Información, es un valioso activo del que depende el buen funcionamiento de una Organización.

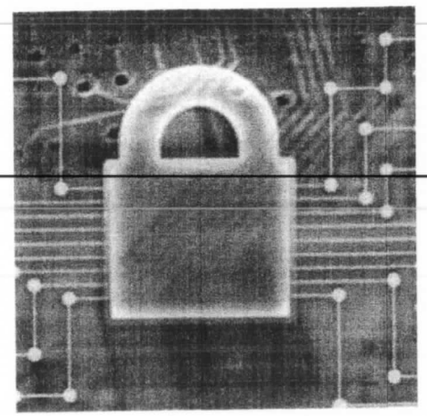
Desafortunadamente, existen riesgos físicos como incendios, inundaciones, terremotos o vandalismo y riesgos lógicos, como hackers, robos de identidad, Spam, virus, espionaje entre otros, que pueden dañar los activos y ocasionar un grave perjuicio para la continuidad de los procesos.

Para evitarlos, es necesario conocer las amenazas, para luego afrontarlas de una manera adecuada, mediante Políticas, procedimientos y controles, con el objeto de minimizar los riesgos.

A continuación, se darán a conocer los aspectos relevantes del Sistema de Seguridad de la Información, a fin de familiarizar a los funcionarios (as) con el tema, e instalar en el Servicio, una cultura de Seguridad.

Capítulo I: algunos conceptos básicos

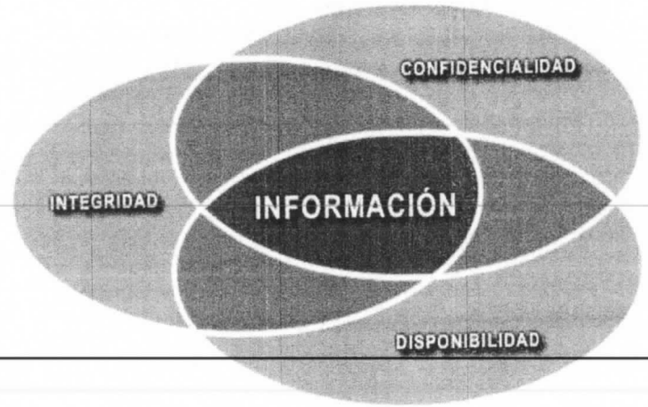
- **Seguridad de la Información**: Es la protección a los activos de Información, fundamentales para asegurar la continuidad de las operaciones de la Organización.
- **Activos de Información**: Son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución.
- **Tipos de Activos**: Lo constituye la Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, etc.), los equipos, sistemas e infraestructura y, las personas que utilizan la información.



- **Confidencialidad de los activos:** implica el acceso a la información solamente por personas o entidades autorizadas. La confidencialidad puede ser pública o reservada. Se debe evitar que exista filtración, fuga o divulgación de Información.

- **Integridad de los activos:** La información se encuentra completa, actualizada y es veraz, sin modificaciones inapropiadas. Se debe evitar que exista falsificación, modificación, manipulación o acceso no autorizado a la información

- **Disponibilidad:** Es la certeza de que la información se encuentra disponible en el momento que los usuarios lo requieran. Se debe evitar que exista pérdida, falla, hurto, extravío o daño parcial o total de la información.



- **Amenaza**: Causa potencial de un incidente no-deseado pudiendo resultar dañado un Sistema u Organización. (terremoto, inundación, incendio, cortes eléctricos, negligencias humanas, etc.)
- **Riesgo:** Es la contingencia de un daño a un activo de información. Por contingencia se entiende que el daño puede materializarse en cualquier momento o no suceder nunca.

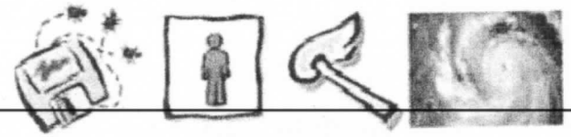
Ejemplo:

Amenaza: falla eléctrica

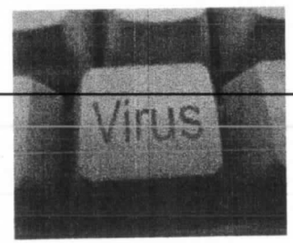
Riesgo: pérdida total o parcial de información.

- **Medios de procesamiento de Información**: Son los dispositivos internos y/o externos que tengan la capacidad de procesar información, almacenarla y que se encuentre disponible para ser manipulada por el usuario.

Seguridad de la Información

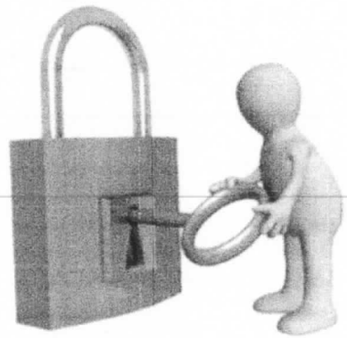


- **Usuario**: persona que utiliza un sistema informático y recibe un servicio como: correo electrónico o red de conectividad proporcionado o administrado por la Subsecretaría del Interior y Seguridad Pública, ya sea que lo utilice en virtud de un empleo, de una función o de cualquier prestación de servicio, sin importar la naturaleza jurídica de ésta.
- **Sanción**: Es una consecuencia administrativa, civil, jurídica o penal por el incumplimiento del deber que produce en relación con el obligado.
- **Spam:** correo o mensaje no solicitado, no deseado o de remitente desconocido, generalmente enviado en grandes cantidades.
- **Virus**: Programa que al ejecutarse, se propaga infectando otros software

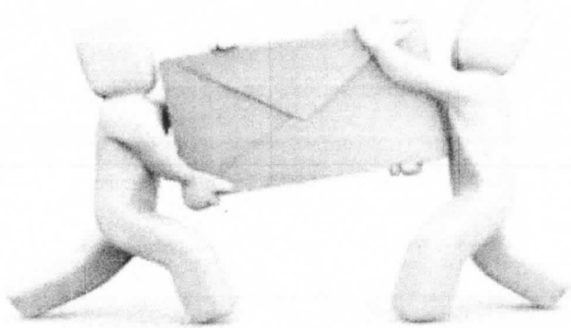


Capítulo II: Política de Seguridad de la Información

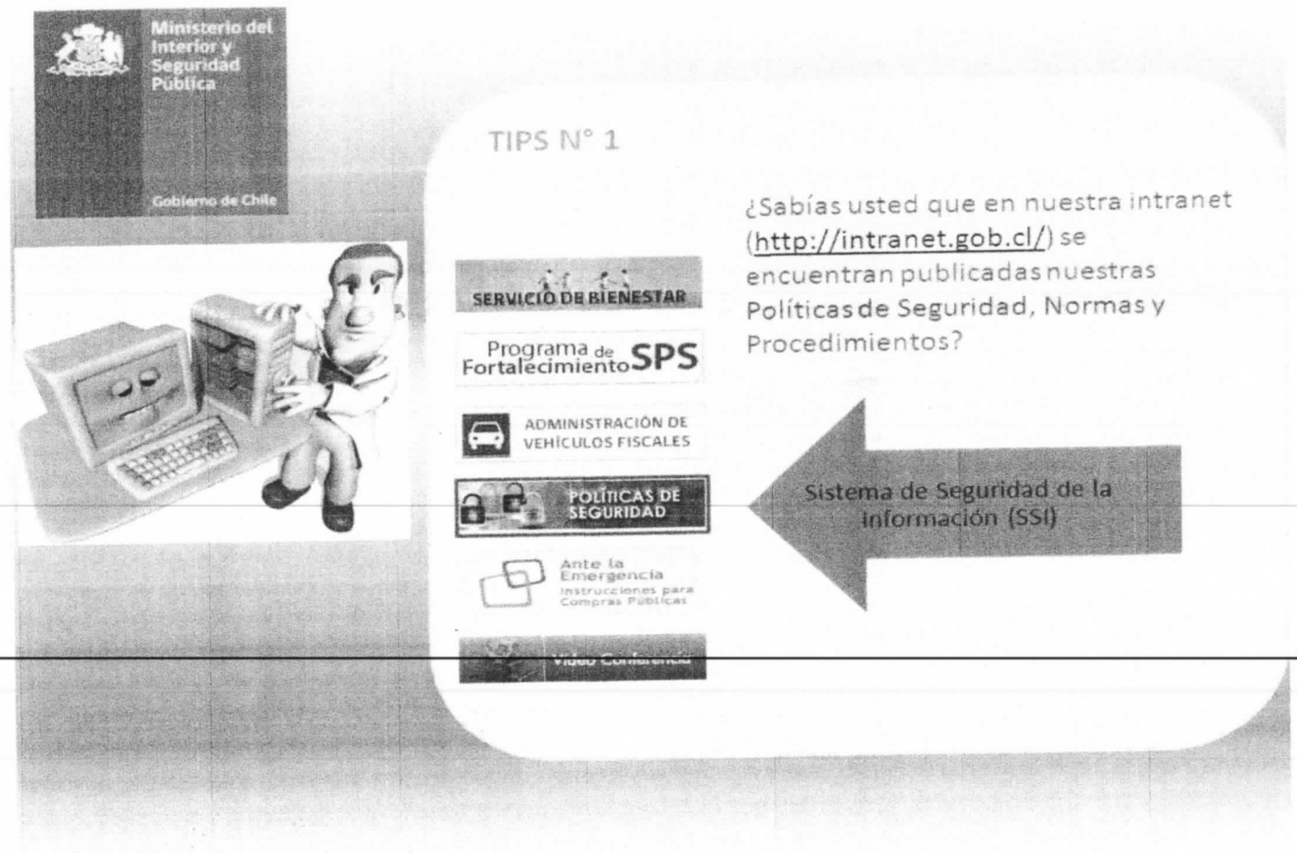
- La Resolución Exenta N° 11.128 del año 2011, modificó la Resolución Exenta N° 1.428 del año 2010, introduciendo las modificaciones necesarias para dar un mejor cumplimiento a los requerimientos Institucionales y Normativos.
- La Resolución estableció las características mínimas obligatorias de Seguridad y confidencialidad que se deben cumplir respecto de los sistemas informáticos proporcionados por el Ministerio del Interior y, al envío, recepción, almacenamiento, acceso y distribución del documento electrónico y, en general de los activos de Información.



- Este documento, consta de 31 artículos, en el que se dan a conocer aspectos generales, definiciones, normas de uso del correo electrónico y uso malicioso, normas de seguridad física, acceso no autorizado, seguridad de la contraseña, seguridad ante programas o documentos electrónicos, seguridad ante la navegación en Internet, obtención de pruebas en investigación sumaria, soporte técnico y difusión, entre otras materias.



En el siguiente Banner, se podrá consultar la versión completa de la Política de Seguridad de la Información, en versión electrónica:



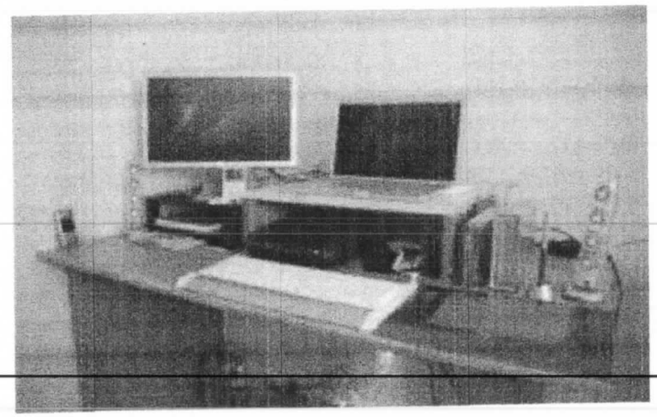
Capítulo III: Práctica de Escritorio Limpio y Seguro

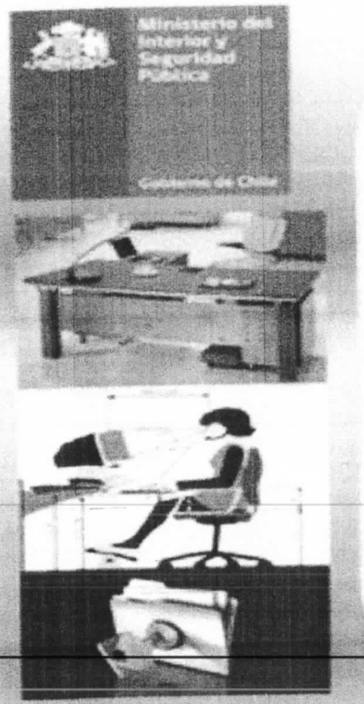
- Esta práctica fomenta el buen uso de los recursos que forman parte del escritorio y entorno más cercano, evitando riesgos del ambiente externo que puedan afectar los activos de la información: personas, información en múltiples formatos y equipos.
- Se fundamenta en el Decreto Supremo N° 83, párrafo 5 de los artículos 17, 18 y 19, los que señalan la protección física de los equipos frente a amenazas de riesgos, consumo de bebidas y tabaco, condiciones ambientales que puedan afectar los equipos y, el tratamiento de los documentos electrónicos clasificados como reservados o secretos.

- La Práctica de Escritorio Limpio y Seguro, promueve incorporar conductas como:

1. Almacenar en lugares seguros y bajo llave, documentación importante.
2. Disponer en forma ordenada los elementos de trabajo (teléfono, artículos de escritorio, etc.)
3. Disponer espacio apropiado para el mouse.
4. Disponer de mobiliario apropiado
5. No fumar no consumir alimentos (por el daño que pudiera ocasionar a los equipos)

- En el Banner del Ministerio del Interior y Seguridad Pública http//intranet.gov.cl/, se encuentra disponible el Manual de Buenas Prácticas de Escritorio Limpio y Seguro.





Boletín N°3

SERVICIO DE BIENESTAR

Comité Técnico Asesor

Programa de Fortalecimiento SPS

ADMINISTRACIÓN DE VEHÍCULOS FISCALES

Políticas y Normas de Seguridad de la Información

Ante la Emergencia Instrucciones para Empleados Públicos

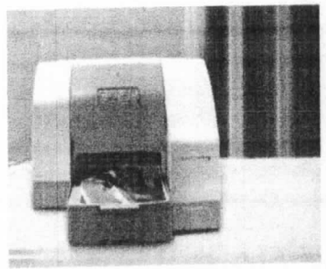
Video Conferencia

En la intranet de la Subsecretaría http://intranet.gob.cl/ se encuentran publicado el Manual de buenas practicas escritorio limpio y seguro, donde encontrará instrucciones y consejos de uso de su escritorio limpio y ordenado, manejo apropiado de contraseñas, uso de impresiones y otros datos importantes.

Sistema de Seguridad de la Información (SSI)

Para mayor información, escribanos a ssi@interior.gov.cl

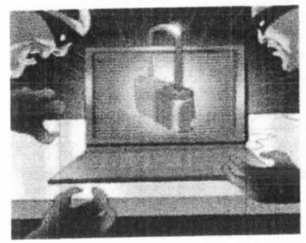
Capítulo IV: manejo de impresiones



Es muy importante tener presente las siguientes recomendaciones:

- Las impresoras solo podrán ser utilizadas para imprimir documentos requeridos por la Institución.
- Todo documento que quede en la impresora al final del día, debe ser eliminado.
- En caso del mal funcionamiento en una impresora, o que está siendo mal utilizada, deberá informar al área de Soporte.
- Cada área será la responsable de mantener los suministros correspondientes.
- El tratamiento del material impreso que contenga información sensible, no debe dejarse descuidado en áreas abiertas y debe ser removido de las impresoras sin demora.
- Los impresos como cheques, certificados, etc, deben ser almacenados en forma segura y sólo proporcionados al personal autorizado.

Capítulo V: manejo de contraseñas



El manejo apropiado de las contraseñas obliga a:

- No guardar las contraseñas, en ningún tipo de papel, agenda, etc.
- Mantenerlas confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambiar la contraseña si piensa que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccionar contraseñas que no sean fáciles de adivinar.
- No grabar la contraseña en una tecla de función o en un comando de caracteres pre-definido.
- Cambiar las contraseñas regularmente.
- No habilitar la opción "recordar clave en este equipo" que ofrecen los programas.
- No utilizar contraseña con números telefónicos, nombre de familia, fechas de nacimiento etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

Cómo crear una buena contraseña:

- Mientras más "desordenada" sea la contraseña mejor, pues más difícil será descubrirla. Así, intente mezclar letras mayúsculas, minúsculas, números y símbolos de puntuación.

Categoría de caracteres	ejemplos
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios	~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

Capítulo VI: uso apropiado de Internet

- El acceso a internet, se encuentra protegido por filtros para disminuir sitios peligrosos, que contengan códigos maliciosos o que se encuentren ajenos al servicio, permitiendo de esta manera, aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

RECOMENDACIONES:

- No navegar por sitios no confiables.
- Queda prohibido el uso de sitios de radios online.
- Queda prohibido el uso de intercambio de archivos (Ares, eMule, Torrents, Limewire, etc.).
- Queda prohibido el uso de sitios de chat (Messenger, chat, etc.).
- Queda prohibido el uso de internet para actividades ilícitas.
- Queda prohibido la descarga que no cumpla con la normativa vigente de copyright y similar.
- Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
- No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo, Sitios del Ministerio, etc.)
- No permitir que el navegador de internet recuerde la contraseña automáticamente.

- Evitar participar en juegos de entretenimiento en línea.
- Si no está navegando por internet, cierre todas las ventanas abiertas.
- Cualquier archivo que se reciba o descargue de internet, deberá revisarse con el antivirus para asegurar que no ingresen Virus que puedan dañar los activos de Información.
- La división de informática, tiene la facultad de suspender el servicio de navegación en internet bajo circunstancias que así lo requieran (Virus, mal uso de internet, trafico sospechoso, etc.).
- Si requiere navegar en algún sitio bloqueado, se debe enviar correo a soporte@interior.gov.cl para su evaluación.

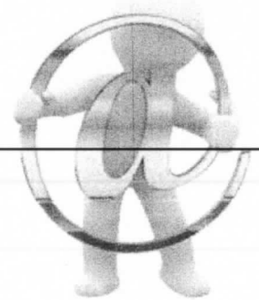
Capítulo VII: uso correo electrónico

- La División Informática cuenta con filtros para identificar y bloquear correos no deseados (Spam o Virus)

- El Correo electrónico es de uso exclusivo para trabajos para el Ministerio del Interior y Seguridad Publica y, queda restringido el uso para otros fines.

- Se prohíbe expresamente el envío de archivos, transmisión o almacenamiento de cualquier información que pudiera ser considerada pornográfica, difamatoria, racista, música, videos, etc., o que atente contra las buenas costumbres o principios.

- No se entregará soporte o algún tipo de estabilidad, a todo correo ajeno, que no pertenezca al Ministerio del Interior y Seguridad Pública
- La contraseña de correo debe ser cambiada periódicamente.
- No se deben pinchar link sospechosos llegados por correos electrónicos (bancos, tiendas, etc.).
- No se deben completar datos personales en correos electrónicos sospechosos.
- Se deben eliminar correos no deseados (spam o sospechoso).
- No se deben enviar correos que su tamaño sea superior a 5MB.



Capítulo VIII: control de virus

- El Ministerio del Interior y Seguridad Publica ha definido como producto estándar, Kaspersky Antivirus, en entorno de estaciones de trabajo, resguardando el correcto funcionamiento de los equipos computacionales.
- El sistema de actualizaciones y detección diaria, es automatizado a nivel central.
- Se debe comunicar al área de soporte, cualquier infección por virus, que no fuese eliminada por el antivirus.
- Los usuarios no podrán desinstalar el producto de antivirus existente en su equipo.
- Los dispositivos extraíbles, antes de ser usados, deben ser escaneados con el antivirus, con el fin de proteger sus activos de Información

Capítulo IX: manejo de redes sociales

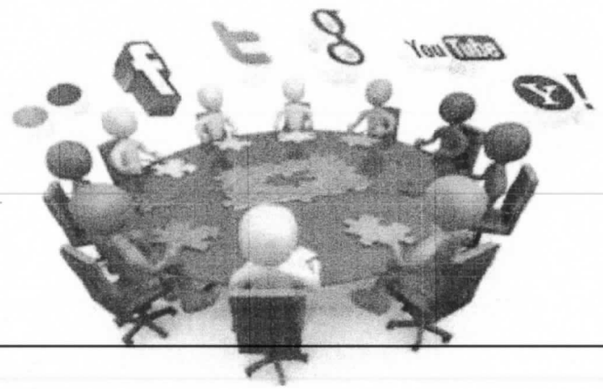
- La División Informática, bloquea todo tipo de sitio relacionado con redes sociales, permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.

- Si algún funcionario por motivos de trabajo requiera acceder a ello, su jefatura debe enviar la solicitud formal a la división informática.

Datos Solicitados

1. Nombre del Funcionario
2. IP del Equipo
3. Motivo

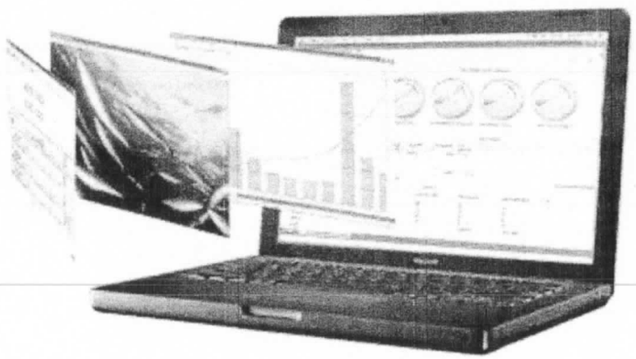
- Cabe destacar que cualquier foto subida o comentario en facebook, twitter o en alguna red social es responsabilidad exclusiva del que la emite.



Capítulo X: manejo de software

- Queda prohibida la instalación de software, que no cumpla con las instrucciones del Área de Soporte y Operaciones.

- Los usuarios, no deben instalar aplicaciones ni descargar aplicaciones, que podrían provocar alguna vulnerabilidad o inestabilidad en los servicios.



- Toda solicitud debe ser canalizada al correo soporte@interior.gov.cl

Capítulo XI: manejo de cuentas de sistemas

- Cuenta de Sistema: corresponde a los permisos de acceso a los Sistemas por parte de los Usuarios del Servicio.

- Las Cuentas deben ser solicitadas formalmente, según el Sistema, a las siguientes direcciones:

1. Cuenta de red: corresponde a la que utilizará cada usuario para conectarse a su equipo PC. Solicitarla vía correo a soporte@interior.gov.cl

2. Cuenta de Correo: Solicitarla formalmente a Departamento de personal, a Marisol Torrejón, email mtorrejon@interior.gov.cl

3. Cuenta de Sistema de B3000: debe ser solicitada a María Angélica Córdova, email acordova@interior.gov.cl

4. Cuenta Sistema GDM: debe ser solicitada a Mariana Jirkal, email mjirkal@interior.gov.cl

5. Cuenta Sistema ORASMI: debe ser solicitada a Informática, Gino Peirano, email gpeirano@interior.gov.cl

6. Cuenta Sistema SIGFE: debe ser solicitada a Elízabeth Cáceres, email ecaceres@interior.gov.cl

- La eliminación de cuentas se debe efectuar formalmente a Informática del Ministerio. En situaciones especiales como despido, se podrá solicitar por correo electrónico, el bloqueo temporal de las cuentas del funcionario, y posteriormente solicitar vía oficio la eliminación de la cuenta.

Capítulo XII: manejo de teléfonos móviles (celulares)

- Para garantizar la seguridad y estabilidad de la red y los teléfonos móviles (celulares), se describen algunos consejos para su manejo adecuado:

1. Los teléfonos móviles de propiedad del Servicio, se han adquirido para facilitar el desarrollo de actividades laborales.

2. En caso de licencia o vacaciones del funcionario, el teléfono móvil debe quedar a disposición del área a la cual fue asignado. Si la jefatura autoriza puede ser utilizado en el periodo de licencia o vacaciones.

3. Se debe mantener desactivada la red Wifi, Bluetooth, Infrarrojos, etc., en caso de que no esté siendo utilizada.

4. Es responsabilidad de cada funcionario hacer copias de seguridad de la información almacenada en el teléfono móvil. Si no está seguro del proceso, debe comunicarse con el Área de Soporte del Ministerio.

5. Es responsabilidad del funcionario, reportar inmediatamente al Área de Soporte, cualquier daño o pérdida del dispositivo móvil que le ha sido asignado.

6. En general, ante cualquier instalación, configuración, modificación o eliminación de software aplicativo, sobre los dispositivos móviles, se debe solicitar su autorización a la División de Informática, área soporte.

Consideraciones finales:

- Lo presentado en este manual, forma parte de la Política de Seguridad de la Información, del Ministerio del Interior y Seguridad Pública.
- Los usuarios de la red del Ministerio del Interior, deberán conocer y dar cumplimiento a esta normativa de Seguridad y uso informático y, utilizar adecuadamente los activos de información a su cargo.
- La infracción a la normativa, podrá constituir una violación al principio de probidad administrativa, pudiendo ser sancionada.
- Se sugiere revisar periódicamente el Banner sobre Políticas y Normas de Seguridad de la Información, publicado en la intranet Institucional, en donde encontrará información detallada y actualizada.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

MIGUEL URRUTIA SCHWARZENBERG
SECRETARIO ABOGADO
INTENDENCIA REGIONAL

JAIME BRAHM BARRIL
INTENDENTE REGIONAL
DE LOS LAGOS

JBB/MPUS/YBD/MJNV
Distribución:
-Planificación, Desarrollo y Control de Gestión Intendencia
-Archivo DAF Intendencia
-Archivo Dpto. Jurídico Intendencia
-Archivo Oficina de Partes Intendencia