Intendencia
Región de los Lagos

Ministerio del Interior y Seguridad Pública

APRUEBA PROCEDIMIENTO DE CONTROL DE ACCESO INTENDENCIA REGIONAL DE LOS LAGOS

RES. EXENTA N° J 1285

PUERTO MONTT, 30 de noviembre 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 la aprobación del procedimiento de control de acceso de la Intendencia Regional de Los Lagos, con el objeto que los funcionarios de éste Servicio, puedan conocerlo y aplicarlo.

RESUELVO:

APRUEBESE el procedimiento de control de acceso de la Intendencia Regional de Los Lagos, cuyo texto íntegro es el siguiente:

PROCEDIMIENTO CONTROL DE ACCESO

INTENDENCIA REGIONAL DE LOS LAGOS

(Noviembre de 2012)

Alcance

Esto se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información de la Intendencia de Los Lagos y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Marco Referencial

Declaración del propósito del Ministerio, apoyando los objetivos y principios de la seguridad de la información.
Los contenidos y controles esenciales de carácter legal que debe considerarse en las políticas de la Subsecretaría de interior y por ende la Intendencia son:

- NCh-ISO 27002.Of2009 - Tecnología de la Información – Código de prácticas para la gestión de seguridad de la información - INN Chile.
- Decreto N° 83, de 2004, de la citada Secretaría de Estado: Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad del documento electrónico.
- Decreto N° 93, de 2006, de la citada Secretaría de Estado: Aprueba norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados, en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- Decreto N° 271, de 2009, del Ministerio de Economía, Fomento y Reconstrucción: Reglamento de la inscripción de esquemas documentales en el Repositorio del Administrador de Esquemas y Metadatos para los órganos de la Administración del Estado.

SECRETARIO ABO... V°B°

- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.223 de Delitos informáticos.
- Ley 19.927 de Delitos de Pornografía Infantil.

Control de documentos

Los documentos requeridos por el Sistema de Seguridad de la Información (SSI) deben protegerse y controlarse. Para lograr este objetivo, las acciones necesarias para implementar son:

- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
- Registrar todos los cambios o actualizaciones a los documentos en la tabla de control de cambios.
- Los registros de las actualizaciones o modificaciones en la tabla de control de cambio debe ser coincidente con el texto del respectivo documento.
- Los registros de las tablas de cambio deben ser legibles y fácilmente identificables en el documento respectivo.
- Se deberá controlar el uso no intencionado de documentos obsoletos.
- En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo a los procedimientos aplicables a su clasificación.

Control de accesos

Reglas para el control de acceso

Las reglas para el control de acceso, estarán documentadas a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos.

Gestión de identidades

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.

Responsabilidad de los usuarios

Todos los funcionarios o terceros que tengan un usuario en la plataforma tecnológica de la División Informática, deberán conocer y cumplir con su uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio y pantalla limpia.

Control de acceso a la red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

Las reglas de acceso a la red a través de los puertos, estarán basadas en la premisa "todo está restringido, a menos que este expresamente permitido".

Control de conexión de las redes

La capacidad de descarga de cada usuario final será de 10 Mb.

Dentro de la red de datos institucional se restringirá el acceso a:

- Mensajería instantánea.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.
- Conexiones a sitios de streaming no autorizado
- Acceso a sitios de pornografía.
- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

Acceso a internet

La División Informática, proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet a la Intendencia, el cual será administrado por el proceso de direccionamiento tecnológico y será el único servicio de internet autorizado.
El uso de internet estará regulado por la Manual de buenas prácticas de Política de Seguridad de la Información.

Control de acceso al sistema operativo

Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema, hasta tanto el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro.

SECRETARIO ABOGADO Vo Bo

Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del Área de soporte del nivel central. Las recomendaciones son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción "recordar clave en este equipo", que ofrecen los programas
- No enviarla por correo electrónico
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre- definido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema, estará restringido a usuarios administradores. Se establecerá una política a nivel del controlador de dominio, desde la unidad de informática del nivel central, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final, deberá tener privilegios de usuario administrador.

Tiempo de inactividad de la sesión

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

Computación móvil y trabajo remoto

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación se establecen directrices que permitirán regular el uso de la computación móvil y trabajo remoto:

Computación y comunicaciones *móviles*

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones policiales.
El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución y deberán contemplar las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Cifrado de la información.
- Uso de software antivirus provisto por la División Informática.
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por la División Informática.
- Realización de copias de seguridad periódicas.
- Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos.
- Permanecer siempre cerca del dispositivo
- No dejar desatendidos los equipos
- No llamar la atención, acerca de portar equipos móviles
- No identificar el dispositivo con distintivos de la División Informática
- No colocar datos de contacto técnico en el dispositivo
- Mantener cifrada la información clasificada
- No conectarse a redes WiFi publicas
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- Informar de inmediato al Area de Soporte sobre la pérdida o hurto del dispositivo, quien procederá al bloqueo del usuario.

Para dispositivos de comunicación móvil (telefonía celular) institucionales se aplicaran los controles antes mencionados y los detallados a continuación:

- Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.
- No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.

GLOSARIO DE TÉRMINOS

Definiciones para los propósitos de este Procedimiento, se entenderá por:

- Acceso a la información: El acceso a la información es el derecho que tiene toda persona de buscar, recibir y difundir información en poder del Estado.
- Derechos de accesos: Conjunto de permisos dados a un usuario, de acuerdo con sus funciones, para acceder a un determinado recursos.
- Restringir el acceso: Delimitar el acceso de los funcionarios, servidores públicos a honorarios y terceras partes a determinados recursos.
- Sanción: Puede ser definida como consecuencia administrativa, civil, jurídica o penal por el incumplimiento del deber que produce en relación con el obligado.

- Sistema informático: uno o más computadores, software asociado, periféricos, terminales, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento de información y/o transferencia de información.
- Usuario: persona que utiliza un sistema informático y recibe un servicio, tales como: correo electrónico o red de conectividad proporcionado o administrado por la Subsecretaría del Interior y Seguridad Publica, 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 o del estatuto que lo rija.
- Documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
- Documento público: aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
- Documento reservado: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano que sean remitidos.
- Documento electrónico institucional: Documento electrónico creado, enviado, comunicado o recibido, por los usuarios del Ministerio del Interior, en ejercicio de las funciones propias de la institución.
- División de Informática: División de Informática de la Subsecretaría del Interior.

- Área de Soporte: Area de Soporte de la División de Informática de la Subsecretaría del Interior.
- Seguridad del documento electrónico. La seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento:
- Activos de información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la Institución cualquiera sea el formato que la contenga y los equipos y sistemas que la soporten. Por ejemplo: dispositivos móviles, tarjetas de accesos, software, equipamiento computacional.
- Riesgo: Es la contingencia de un daño a un activo de información. A su vez, contingencia significa que el daño puede materializarse en cualquier momento o no suceder nunca.
- Amenaza: Causa potencial de un incidente no-deseado por el cual puede resultar dañado un sistema u organización. A modo terremotos, inundaciones, sabotajes, amenazas de bombas, negligencias humanas, cortes eléctricos, fallas en sala de servidores, entre otras.
- Gestión del riesgo: Proceso definido para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización. (Guía Técnica N° 53, CAIGG). Es un proceso iterativo que debe contribuir a la mejora organizacional a través del perfeccionamiento de los procesos.
- Evaluación del riesgo: Comparar los niveles de riesgo encontrados contra los criterios de riesgo preestablecidos (si es que han sido establecidos por la dirección) considerando el balance entre los beneficios potenciales y resultados adversos. Ordenar y priorizar mediante un ranking los riesgos analizados.
- Seguridad de la Información: es el proceso encargado de asegurar que los recursos de un sistema de información sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización, preservando la Integridad, Confidencialidad y Disponibilidad.
- Proceso: Conjunto de actividades o eventos que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.
- Incidente de Seguridad: Se define incidente como cualquier evento o situación que comprometa de manera importante la disponibilidad, integridad y confidencialidad de la información, junto con la plataforma tecnológica, proceso y aplicativos que permitan acceder a ésta en forma oportuna. En general, es una violación de una política, estándar o procedimiento de seguridad, que no permite prestar un servicio computacional.

- Como ejemplos de incidentes de seguridad podemos enumerar:
- Acceso no autorizado.
- Robo de contraseñas.
- Robo de información.
- Denegación de servicio.
- Robo y extravío de un medio de procesamiento de la información.
- Confidencialidad: Es la propiedad de un documento o mensaje, que está autorizado para ser leído o entendido, únicamente, por algunas personas o entidades.
- Integridad: Se entiende por la corrección y completitud de los datos o de la información manejada.
- Disponibilidad: es la certeza de que sólo los usuarios autorizados tienen acceso a la información y a los activos asociados cuando es requerido.
- Medios de procesamiento de información: Los dispositivos internos y/o externos que tenga la capacidad de procesar información, almacenarla y que se encuentren disponibles para ser manipulados por el usuario.

Como ejemplos de medios de procesamiento de información, podemos enumerar:

- Servidores de aplicaciones: de correo, de impresión, aplicaciones web.
- Servidores de Almacenamientos.
- Computadores personales.
- Discos duros externos.
- Pendrives.
- Teléfonos móviles.
- Operaciones informáticas: Todas las actividades que estén relacionadas con un sistema informático y/o procesamiento de la información.

Como ejemplos de operaciones informáticas podemos enumerar:

- Configuración de servidores y estaciones de trabajo.
- Configuración de equipos de comunicación que conectan a los usuarios a la red.
- Creación y/o retiro de acceso a los medios de procesamiento de información.
- Mantención de base de datos de los sistemas.
- Respaldo de la información de servidores y estaciones de trabajo.
- Terceras partes: Persona u organismo reconocido como independiente de las partes implicadas en lo que se refiere a la materia en cuestión. Para este procedimiento, se entenderá como terceras partes a:
- Proveedores de servicios y de red.
- Proveedores de productos de software y servicios de información.
- Outsourcing de instalaciones y operaciones.
- Servicios de asesoría de seguridad.
- Auditores externos.

- Estación de Trabajo: En una red de computadores, una estación de trabajo es un computador que facilita a los usuarios el acceso a los servidores y periféricos de la red.
- Programa malicioso: Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora sin el consentimiento de su propietario.
- Virus: Se usa para designar un programa que, al ejecutarse, se propaga infectando otros softwares ejecutables dentro de la misma computadora.
- Madware: El término malware es muy utilizado para referirse a una variedad de software hostil, intrusivo o molesto
  El término malware incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo, crimeware y otros softwares maliciosos e indeseables.
- SPAM: Se llama spam al correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

MIGUEL URRUTIA SCHWARZENBERG
SECRETARIO ABOGADO
INTENDENCIA REGIONAL

JAIME BRAHM BARRIL
INTENDENTE REGIONAL
DE LOS LAGOS

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