REPÚBLICA DE CHILE
I. MUNICIPALIDAD DE CONCON
ADMISTRACIÓN Y FINANZAS

DECRETO N°: 3035 /

EN CONCÓN, 30 DIC 2016

VISTOS Y TENIENDO PRESENTE:

A. Las facultades que me confieren la Ley N°18.695, Orgánica Constitucional de Municipalidades.
B. Las facultades emanadas de la Ley 19.880, en su artículo 3°.
C. Decreto 83, Ministerio Secretaria General de la Presidencia de fecha 12.01.2005.
D. Ordinario 088/2016, de fecha 15 de Noviembre de 2016, del Departamento de Control Interno, solicitando conformación "Comité de Seguridad Informática de la Municipalidad".
E. Ordinario 193/2016, de fecha 18 de Noviembre de 2016, del Departamento de Administración y Finanzas, invitando al Sr. Alcalde a Reunión de Comité.
F. Ordinario 198/2016, de fecha 23 de Noviembre de 2016, del Departamento de Administración y Finanzas, informando a la Sra. Alcaldesa (S) que no se pudo constituir el Comité.
G. Ordinario 199/2016, de fecha 23 de Noviembre de 2016, del Departamento de Administración y Finanzas, citando a los diferentes Departamentos a Reunión de Comité.
H. Ordinario 204/2016, de fecha 01 de Diciembre de 2016, del Departamento de Administración y Finanzas, informando a la Sra. Alcaldesa (S) sobre 2da. Reunión del Comité.
I. Ordinario 205/2016, de fecha 01 de Diciembre de 2016, del Departamento de Administración y Finanzas, citando a los difentes Departamentos a Reunión de Comité.
J. Ordinario 215/2016, de fecha 13 de Diciembre de 2016, del Departamento de Administración y Finanzas, citando a los diferentes Departamentos a Reunión de Comité.
K. Planilla de fecha 16.12.2016 con votación y firmas de Aprobación sobre Manual de Políticas y Estándares de Seguridad Informática.

DECRETO

1. **APRUEBESE, "**Manual de Políticas y Estándares de Seguridad Informática" para usuarios de la Municipalidad, Educación y Salud, según acuerdo del Comité de Seguridad Informática de fecha 16 de Diciembre de 2016.

2. **Notifíquese,** por Secretaria Municipal.

ANÓTESE, COMUNÍQUESE, PUBLÍQUESE Y ARCHÍVESE.

I. MUNICIPALIDAD DE CONCON SECRETARIA MUNICIPAL
MARIA LUIANA BARRIOZA GODOY
SECRETARIO MUNICIPAL

ALCALDE

OSG/MLBG/EAO/pmr
Distribución:
1.- Alcaldía.
2.- Secretaría Municipal.
3.- Control.
4.- Salud.
5.- Informático Salud (Sr. Gonzalo Román)
6.- Educación.
7.- Secular.
8.- Informático Daf.
9.- Archivo Daf.

I. MUNICIPALIDAD DE CONCON		
Dirección de Control		
Objetado	Observado	Revisado

3035

MUNICIPALIDAD DE CONCON

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

OFICINA DE INFORMATICA

CONTENIDO

3.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

4.-POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESOLÓGICO

5.-POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

Propósito

El presente documento tiene como finalidad dar a conocer las Políticas y estándares de Seguridad Informática que deberán observar Los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de la Municipalidad de Concon.

Introducción

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

La Seguridad Informática es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la Municipalidad de Concon en materia de seguridad.

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal.
- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Cumplimiento.

Estas Políticas en seguridad informática se encuentran alineadas con el Estándar NCh 2777.Of2003.

Objetivo

Establecer y difundir las Políticas y Estándares de Seguridad Informática a todo el personal de la Municipalidad de Concon, para que sea de su conocimiento y cumplimiento en los recursos informáticos asignados.

Alcance

El documento define las Políticas y Estándares de Seguridad que deberán observar de manera obligatoria todos los usuarios para el buen uso del equipo Computacional, aplicaciones y servicios informáticos de la Municipalidad de Concon.

Justificación

La Oficina de informática de la Municipalidad de Concon está facultada para definir Políticas y Estándares en materia informática.

Sanciones por Incumplimiento

El incumplimiento al presente Manual podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Beneficios

Las Políticas y Estándares de Seguridad Informática establecidos Dentro de este documento son la base para la protección de los activos tecnológicos e información de la Municipalidad de Concon.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

Política

Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la Municipalidad de Concon, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para usuarios.

1.1. Obligaciones de los Usuarios

Es responsabilidad de los usuarios de bienes y servicios Informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente manual.

1.2 Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos de la Municipalidad de Concon deberán conducirse conforme a los principios de confidencialidad y uso adecuado de los recursos informáticos y de información que posee la Municipalidad de Concon, y cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.3. Entrenamiento en Seguridad Informática.

Todo empleado de la Municipalidad de Concon, de nuevo ingreso deberá:

- Leer y firmar el Manual de Políticas y Estándares de Seguridad de la Municipalidad de Concon, donde se dan a conocerlas obligaciones para los usuarios y las sanciones que pueden aplicar en caso de incumplimiento.

1.4. Medidas disciplinarias.

Cuando La Oficina de Informática identifique el incumplimiento al presente Manual remitirá el reporte o denuncia correspondiente al Órgano Interno de Control, para los efectos de su competencia y atribuciones.

2.-POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Política

Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la Municipalidad de Concon, sólo a personas autorizadas para salvaguarda.

2.1 Resguardo y protección de la información.

2.1.1. El usuario deberá reportar de forma inmediata a la Oficina de Informática, cuando detecte que existan riesgos reales o potenciales para equipos computacionales o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2. El usuario tiene la obligación de protegerlos CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

2.1.3. Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Municipalidad de Concon que se encuentre almacenada en los equipos computacionales personales que tengan asignados.

2.2. Controles de acceso físico.

Cualquier persona que tenga acceso a las instalaciones de la Municipalidad de Concon, deberá portar a la vista una credencial que identifique la calidad en la que se encuentra al interior de las instalaciones, pudiendo ser éstas como funcionario o visita.

Se debe registrar en portería toda persona externa que quiera acceder a dependencias de la Municipalidad de Concon, deberá identificarse e indicar motivo de la visita, posteriormente se deberá constatar con el departamento respectivo y de ser positivo el ingreso se le debe proporcionar una credencial de visita que la identifique como tal.

En el caso del ingreso de equipos computacionales que no sean propiedad de la Municipalidad de Concon, y que permanezca dentro de la institución más de un día hábil, es necesario que el responsable de la unidad de la Municipalidad de Concon en la que trabaja el dueño del equipo, debe enviar a la Oficina de Informática una solicitud de autorización. El equipo quedará sujeto a revisión por parte del Encargado de Informática y éste podrá negar la autorización si establece que es potencialmente riesgoso y/o comprometa la red de datos o la seguridad.

Todo acceso físico a las personas será restringido, debiéndose gestionar y documentar.

El proceso para la obtención de las credenciales, tarjetas de acceso magnético o claves de acceso a instalaciones de la Municipalidad de Concon deberán ser solicitadas por el jefe de departamento al cual pertenece o desempeña labores el funcionario y deberá incluir la aprobación del encargado de la Oficina de informática de la Municipalidad de Concon. La emisión de las credenciales, tarjetas de acceso magnético o claves de acceso será efectuada únicamente por la Oficina de informática de la Municipalidad de Concon, entidad que llevará el registro de las emisiones.

Las tarjetas de acceso magnético o claves de acceso NO deben ser compartidas o cedidas a otros.

Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos a la Oficina de Informática de la Municipalidad de Concon. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.

La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados a la Oficina de Informática de la Municipalidad de Concon al correo informatica@concon.cl, incluyendo en el mensaje los siguientes datos: RUT, Nombre completo del funcionario, dependencia, y circunstancias en las cuales sucedió el robo o pérdida.

2.3. Seguridad en áreas de trabajo.

Los Centros de Cómputo de la Municipalidad de Concon son áreas restringidas, por lo que sólo el personal autorizado por la Oficina de Informática puede acceder a ellos.

2.4. Protección y ubicación de los equipos.

2.4.1. Los usuarios no deben mover o reubicar los equipos computacionales o de telecomunicaciones, instalar o desinstalar dispositivos ni software, tampoco se pueden retirar sellos de los mismos sin la autorización del Encargado de Informática, debiéndose solicitar al mismo, en caso de requerir este servicio.

2.4.2. El Encargado de Bodega e Inventario será el responsable de generar el resguardo y recabar la firma del usuario como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Departamento.

2.4.3. Los equipos computacionales asignado, deberán ser para uso exclusivo de las funciones asignadas al usuario de la Municipalidad de Concon.

2.4.4. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

2.4.5. Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, ya que los otros están destinados para archivos de programas y sistema operativo.

2.4.6. Mientras se opera el equipo computacional, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico.

2.4.7. No se pueden colocar objetos encima del equipo o cubrirlos orificios de ventilación del monitor o del gabinete.

2.4.8. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

2.4.9. El usuario debe asegurarse que los cables de conexión no sean pisados o aplastados al colocar otros objetos encima o contra ellos.

2.4.10. Cuando se requiera realizar cambios múltiples de equipos computacionales o reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Oficina de Informática y al Encargado de Bodega e Inventario, a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.

2.4.11. Queda prohibido que el usuario abra o desarme los equipos computacionales, porque con ello perdería la garantía que proporciona el proveedor de dicho equipo.

2.5. Mantenimiento de equipo.

2.5.1. Únicamente el personal autorizado de la Oficina de Informática podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

2.5.2. Los usuarios deberán asegurarse de respaldar la información que considere relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de la Dirección.

2.6. Pérdida o transferencia de equipo.

2.6.1. El usuario que tenga bajo su resguardo algún equipo Computacional será responsable de su uso y custodia, en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

2.6.2. El resguardo para los Laptops o Notebook, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

2.6.3. El usuario deberá dar aviso de inmediato al Encargado de Informática y al Encargado de Bodega e Inventario de la desaparición, robo o extravío del equipo computacional o accesorios bajo su resguardo.

2.7. Uso de dispositivos especiales.

2.7.1 .El uso de los grabadores de discos compactos, pendrives, discos duros externos, memorias SD, u otro dispositivo de almacenamiento masivo externo, es de uso exclusivo para respaldos de información, que por su volumen así lo justifiquen, éstos dispositivos NO pueden salir de las instalaciones de la Municipalidad de Concon y se deben guardar bajo llave con el resguardo que corresponde, tratándose de información sensible o privilegiada.

2.7.2. La asignación de este tipo de equipo será previa justificación por escrito y autorización del titular o jefe inmediato correspondiente.

2.7.3. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

2.7.4. Los módems internos deberán existir solo en las computadoras portátiles y NO se deberán utilizar dentro de las instalaciones de la institución para conectarse a ningún servicio de información externo, excepto cuando lo autorice el Encargado de Informática.

2.8. Daño del equipo.

El equipo computacional o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario, éste deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

3.- POLÍTICAS, ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Política

Los usuarios deberán utilizar los mecanismos institucionales para protegerla información que reside y utiliza la infraestructura de la Municipalidad de Concon. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de Municipalidad de Concon, o hacia redes externas como internet.

Los usuarios de la Municipalidad de Concon que hagan uso de equipo computacionales, deben conocer y aplicarlas medidas para la prevención de código malicioso como pueden ser virus, *malware* o *spyware*. El usuario puede acudir al Encargado de Informática, o a su jefe inmediato, para que éste solicite asesoría.

3.1. Uso de medios de almacenamiento

3.1.1. Toda solicitud para utilizar un medio de almacenamiento de Información compartido, deberá contar con la autorización del Encargado de Informática, jefe inmediato del usuario y del titular del área dueña de la información.

Dicha solicitud deberá explicar en forma clara y concisa los fines para los que se otorgará la autorización, ese documento se presentará con timbre y firma del titular del área.

3.1.2. Los usuarios deberán respaldar de manera periódica la información sensible y crítica que se encuentre en sus computadoras personales o estaciones de trabajo, solicitando asesoría al Encargado de Informática, para que dichos asesores determinen el medio en que se realizará dicho respaldo.

3.1.3. En caso de que por el volumen de información se requiera algún respaldo en CD, DVD, este servicio deberá solicitarse por escrito al Encargado de Informática, y deberá contar con la firma del titular del área.

3.1.4. Los trabajadores de la Municipalidad de Concon deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Encargado de Informática, en términos que indica la Ley 19628, demás criterios y procedimientos establecidos en esta materia.

3.1.5. Las actividades que realicen los usuarios de la Municipalidad de Concon en la infraestructura de Tecnología de la Información son registradas y susceptibles de auditoría.

3.2. Instalación de Software.

3.2.1. Los usuarios que requieran la instalación de software que no sea propiedad de la Municipalidad de Concon, deberán justificar su uso y solicitar su autorización al Encargado de Informática, a través de un oficio firmado por el titular del área de su adscripción, indicando el equipo computacionales donde se instalará el software y el período que permanecerá dicha instalación, siempre y cuando el dueño del software presente la factura de compra de dicho software.
Si el dueño del software no presenta la factura de compra del software, el personal asignado por el Encargado de Informática procederá de manera inmediata a desinstalar dicho Software.

3.2.2. Se considera una falta grave el que los usuarios instalen cualquier tipo de programa *(software)* en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Municipalidad de Concon, que no esté autorizado por el Encargado de Informática.

3.3. Identificación del incidente.

3.3.1. El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Encargado de Informática o a su jefatura inmediata, lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2. Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al titular de su departamento.

3.3.3. Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la Municipalidad de Concon, debe ser reportado al Encargado de Informática.

3.4. Administración de la configuración.

Los usuarios de las áreas de la Municipalidad de Concon no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos computacionales utilizando el protocolo de transferencia de archivos, empleando la infraestructura de red de la Municipalidad de Concon, sin la autorización por escrito del Encargado de Informática. Para éstos efectos el Encargado de Informática dispondrá de un servicio FTP al cual los usuarios de la Municipalidad de Concon podrán acceder mediante usuario y password, que le serán proporcionados oportunamente.

3.5. Seguridad de la red.

Será considerado como un ataque a la seguridad informática y una Falta grave, cualquier actividad no autorizada por el Encargado de Informática, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la Municipalidad de Concon, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

3.6. Uso del correo electrónico.

3.6.1. Los usuarios no deben usar cuentas de correo electrónico propias, en El desempeño de sus funciones, el Encargado de Informática proporcionará cuentas de correo institucionales a los usuarios de la Municipalidad de Concon, en las cuales su contenido es de propiedad de la Municipalidad de Concon y se encuentran protegidas por la actual normativa vigente. Se debe incluir en todos los correos enviados, el pie de firma estándar e incluir la nota "La información contenida en este correo electrónico, así como en cualquiera de sus adjuntos, es confidencial y está dirigida exclusivamente a él o los destinatarios indicados. Cualquier uso, reproducción, divulgación o distribución por otras personas distintas a él, o los destinatarios, está estrictamente prohibida. Si ha recibido este correo por error, por favor notifíquelo inmediatamente al remitente y bórrelo de su sistema sin dejar copia del mismo. (Los acentos han sido suprimidos intencionalmente para no exponer al texto a reemplazos de los caracteres acentuados)".
Los usuarios no deben usar cuentas asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien Más (mientras esta persona se encuentra fuera o ausente), el usuario Ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la Municipalidad de Concon, a menos que cuente con la autorización del titular del área.

3.6.2. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Municipalidad de Concon. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

3.6.3. Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó el Encargado de Informática.

3.6.4. La Municipalidad de Concon, se reserva el derecho de acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico

De personal que ha comprometido la seguridad violando políticas de Seguridad Informática de la Municipalidad de Concon o realizado acciones no autorizadas. Como la información del correo electrónico institucional de la Municipalidad de Concon es privada, la única forma en la que puede ser revelada es mediante una orden judicial.

3.6.5. El usuario debe de utilizar el correo electrónico de la Municipalidad de Concon, única y exclusivamente para los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso distinto.

3.6.6. Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

3.7. Controles contra código malicioso.

3.7.1. Para prevenir infecciones por virus informáticos, los usuarios de la Municipalidad de Concon, deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y Validado por el Encargado de Informática.

3.7.2.Los usuarios de la Municipalidad de Concon, deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos externos, pendrives, CD´s, DVD's estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Encargado de Informática.

3.7.3. El usuario debe verificar mediante el software de antivirus autorizado por el Encargado de Informática que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno, considerando que tengan que ser descomprimidos.

3.7.4. Ningún usuario de la Municipalidad de Concon debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software.

Tampoco debe probarlos en cualquiera de los ambientes o plataformas de la Municipalidad de Concon. El incumplimiento de este estándar será considerado una falta grave.

3.7.5. Ningún usuario ni empleado de la Municipalidad de Concon, o personal externo podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Encargado de Informática.

3.7.6. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Encargado de Informática para la detección y erradicación del virus.

3.7.7. Cada usuario que tenga bajo su resguardo algún equipo Computacional personal portátil, será responsable de solicitar de manera periódica al Encargado de Informática las actualizaciones del software de antivirus.

3.7.8. Los usuarios NO deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el Encargado de Informática en programas tales como:

- Antivirus;
- Correo electrónico;
- Paquetería Office;
- Navegadores; u
- Otros programas.

3.7.9. Debido a que algunos virus son extremadamente complejos, ningún usuario de la Municipalidad de Concon debe intentar erradicarlos de las computadoras, lo indicado es llamar al Encargado de Informática para que sean ellos quienes lo solucionen.

3.8. Permisos de uso de Internet.

3.8.1. El acceso a internet provisto a los usuarios de la Municipalidad de Concon es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña. En caso de daño a la imagen de la institución se procederá de acuerdo a lo que determine el Órgano Interno de Control de la Municipalidad de Concon.

3.8.2. La asignación del servicio de internet, deberá solicitarse por Escrito al Encargado de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno Del titular del área correspondiente.

3.8.3. Todos los accesos a internet tienen que ser realizados a través de los canales de acceso provistos por la Municipalidad de Concon.

3.8.4. Los usuarios con acceso a Internet la Municipalidad de Concon tienen que reportar todos los incidentes de seguridad informática al Encargado de Informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

3.8.5. El acceso y uso de módem en la Municipalidad de Concon tiene que ser previamente autorizado por el Encargado de Informática.

3.8.7. Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:

- Serán sujetos al monitoreo de las actividades que realizan en internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de *software* sin la autorización del Encargado de Informática.
- La utilización de internet es para el desempeño de su función y puesto en la Municipalidad de Concon y no para propósitos Personales.

3.8.8. Los esquemas de permisos de acceso a internet y servicios de mensajería instantánea serán administrados por el Encargado de Informática de acuerdo a las necesidades particulares de los usuarios según la labor que desempeña, por lo que los accesos a paginas restringidas deberán ser solicitados mediante formulario escrito, deberá ser firmado y timbrado por el jefe de la unidad a cargo autorizando dichos accesos.

4.- POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESOS LÓGICOS

Política

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (*user ID)* y contraseña (*password*), necesarios para acceder a la información y a la infraestructura tecnológica de la Municipalidad de Concon, por lo cual deberá mantenerlo de forma confidencial.

Sólo el Alcalde de la Municipalidad de Concon, puede otorgar la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica de la Municipalidad de Concon, otorgándose los permisos mínimos necesarios para el desempeño de sus funciones, con apego al principio "Necesidad de saber".

4.1. Controles de acceso lógico.

4.1.1. El acceso a la infraestructura tecnológica de la Municipalidad de Concon para personal externo debe ser autorizado por el Encargado de Informática.

4.1.2. Está prohibido que los usuarios utilicen la infraestructura Tecnológica de la Municipalidad de Concon para obtener acceso no autorizado a la información u otros sistemas de información de la Municipalidad de Concon.

4.1.3. Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.4. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Encargado de Informática antes de poder usar la infraestructura tecnológica de la Municipalidad de Concon.

4.1.5. Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Municipalidad de Concon , a menos que se tenga autorización del Encargado de Informática.

4.1.6. Cada usuario que accede a la infraestructura tecnológica de la Municipalidad de Concon, debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

4.1.7. Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

4.1.8. Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

4.2. Administración de los usuarios.

4.2.1. Cualquier cambio en los roles y responsabilidades de privilegios que modifique sus privilegios de acceso a la infraestructura tecnológica la Municipalidad de Concon, deberán ser notificados por escrito o vía correo electrónico al Encargado de Informática, con el visto bueno del titular del área solicitante, para realizar el ajuste.

4.3. Equipo desatendido.

Los usuarios deberán mantener sus equipos Computacionales con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por el Encargado de Informática), como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

4.4. Administración y uso de contraseñas.

4.4.1. La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

4.4.2. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al Encargado de Informática, indicando si es de acceso a la red o a módulos de sistemas, para que se le bloqueen los accesos y se proporcione una nueva contraseña.

4.4.3. La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante el Encargado de Informática como empleado de la Municipalidad de Concon.

4.4.4. Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

4.4.5. Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos;

- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10).Estos caracteres deben ser alfanuméricos, o sea, números y letras;

- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.

- Deben ser diferentes a las contraseñas que se hayan usado previamente.

4.4.7. La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

4.4.8. Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

4.4.9. Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.4.10. Los cambios o desbloqueo de contraseñas solicitados por el usuario al Encargado de Informática serán solicitados mediante solicitud o e-mail, firmado por el jefe inmediato del usuario que lo requiere.

4.5. Control de accesos remotos

4.5.1. Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno del Encargado de Informática.

4.5.2. La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el Encargado de Informática.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA.

Política

De acuerdo al Decreto N° 83 del año 2005, del ministerio secretaría general De la presidencia de la república de Chile que "Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos".

5.1. Derechos de Propiedad Intelectual.

5.1.1. Está prohibido por las leyes de derechos de autor y por la Municipalidad de Concon, realizar copia no autorizadas de

Software, ya sea adquirido o desarrollado por la Municipalidad de Concon.

5.1.2. Los sistemas desarrollados por personal, interno o externo, que sea parte de la Oficina de Informática, o sea coordinado por éste, son propiedad intelectual de la Municipalidad de Concon.

5.2. Revisiones del cumplimiento

5.2.1. El Encargado de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para usuarios.

5.2.2. El Encargado de Informática, podrá implementar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la Política de Seguridad del Personal.

5.3. Violaciones de seguridad informática.

5.3.1. Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Encargado de Informática.

5.3.2. Está prohibido realizar pruebas de controles de los diferentes elementos de Tecnología de la Información.
Ninguna persona puede probar o intentar comprometer los controles internos a menos de contar con la aprobación del Encargado de Informática.

5.3.3. Ningún usuario de la Municipalidad de Concon debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Encargado de Informática.

5.3.4. No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar, introducir cualquier tipo de código (programa) conocidos como virus, malware, spyware, o similares diseñado para auto replicarse, dañar, afectar el desempeño, acceso a

las computadoras, redes e información de la Municipalidad de Concon.

Para los efectos del presente manual, se escribe el presente glosario de términos:

GLOSARIODE TÉRMINOS

TÉRMINO	SIGNIFICADO
(A)	
Acceso	Es el privilegio de una persona para utilizar un objeto o infraestructura.
Acceso Físico	Es la actividad de ingresar a un área.
Acceso Lógico	Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo.
Acceso Remoto	Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus	Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese archivo y lograr afectarlo.
(B)	
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
(C)	
Confidencialidad	Se refiere a la obligación de los servidores a no divulgar.

	Información a personal no autorizado para su conocimiento.
Contraseña Password	Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular.
Control de Acceso	Es un mecanismo de seguridad diseñado para prevenir, salva guardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.
Copyright	Derecho que tiene un autor, incluido el autor de un programa informático sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas .Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida.
(D)	
Disponibilidad	Se refiere a que la información esté disponible en el momento que se necesite.
(E)	
Estándar	Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
(F)	
Falta administrativa	Acción u omisión contemplada por la normatividad aplicable a la actividad de un funcionario de la Municipalidad de Concon, mediante la cual se finca responsabilidad y se sanciona esa acción u omisión.
FTP	Protocolo de transferencia de archivos. Es un protocolo estándar de comunicación que proporción a un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
(G)	
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
(H)	
Hardware	Se refiere a las características técnicas y físicas de las computadoras.
Herramientas de seguridad	Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
(I)	

Identificador de Usuario	Nombre de usuario (también referido como User ID) único asignado a un servidor para el acceso a equipos y sistemas desarrollados, permitiendo su identificación en los registros.
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice.
Incidente de Seguridad	Cualquier evento que represente un riesgo para la adecuada conservación de confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.
Integridad	Se refiere a la pérdida ó deficiencia en la autorización, totalidad ó exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional.
Internet	Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes (worldwideweb) en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos.
Intrusión	Es la acción de introducirse o acceder sin autorización a un activo.
(M)	
Maltrato	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad de la Municipalidad de Concon. Se contemplan dentro de éste al descuido y la negligencia.
Malware	Código malicioso desarrollado para causar daños en equipos informáticos, sin el consentimiento del propietario. Dentro de estos códigos se encuentran: virus, *spyware*, *troyanos*, *rootkits*, *backdoors*, *adware* y gusanos.
Mecanismos de seguridad o de	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. Que se utiliza para disminuir
control	La probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamiento magnéticos	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (diskettes, CD´s, DVD´s, etc.)
Módem	Es un aparato electrónico que se adapta una terminal o computadora y se conecta a una red de. Los módems convierten los pulsos digitales de una computadora en frecuencias dentro de la gama de audio del sistema telefónico. Cuando actúa en calidad de receptor, un módem decodifica las frecuencias entrantes.
(N)	

"Necesidad de saber" principio	Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidad es dentro de la Comisión.
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
(P)	
Password	Véase Contraseña.
(R)	
Respaldo	Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.
(S)	
Servidor	Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web	El sitio web es un lugar virtual en el ambiente de internet, el cual

	Proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Software	Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Spyware	Código malicioso desarrollado para infiltrar a la información de un equipo o sistema con la finalidad de extraer información sin la autorización del propietario.
(U)	
UserID	Véase Identificador de Usuario.
Usuario	Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal o dispositivo (hardware).
(V)	
Virus	Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento magnético de computadoras.
Vulnerabilidad	Es una debilidad de seguridad o brecha de seguridad, la cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencional o accidental.

Comité de Seguridad Informatico 16/12/2016 Acuerdo Politicas de Seguridad				
Nombre	Apellido	Departamento	Cargo	Firma
Gonzalo	Roman Sevillano	SALUD	ENCARGADO INFORMATICA	
GUILLERMO	BIADOYOLI ESPINOZA	DAEM.	DIRECTOR.	
PABLO	ROJAS	DAF	ENCARGADO INFOR	
IVAN	ARIAS	ORTEGA	DIRECTORA DAF	
EUGENIO SAN ROMAN		CONTROL	DIRECTOR	
MARCO TATINI G		SECPLAC	DIRECTOR	

MUNICIPALIDAD DE LOS LAGOS
DIRECTORA
ADMINISTRACION
Y FINANZAS

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ORD.: 215

ANT. : -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia.

MAT. : Citación "Comité de Seguridad Informático de la Municipalidad, Salud y Educación".

CONCÓN, 13-12-2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SRES. SEGÚN DISTRIBUCIÓN

Por medio del presente, se cita a Ustedes a la tercera reunión para el día viernes 16 de diciembre de 2016 a las 09:00 hrs. en las dependencias de Secplac con la finalidad de cumplir lo establecido en el Decreto N° 83 del 12.01.2005 del Ministerio Secretaria General de la Presidencia, que las personas que componen "**Comité de Seguridad Informático**", puedan votar la propuesta del "Manual de Políticas y Estándares de Seguridad Informática para usuarios" y así proceder a confeccionar el Decreto Alcaldicio correspondiente.

Esperando contar con su asistencia, saluda atentamente a Ud.

ILUSTRE MUNICIPALIDAD DE CONCÓN
DIRECTORA ADMINISTRACION Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
-Secplac.
-Secretaría Municipal.
-Control.
-Informático Daf
- Director Salud
- Informático Salud (Sr. Gonzalo Román)
-Director Daem
- Daem (Informático Daem)
-Archivo.

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ORD.: 205

ANT. : -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia.
-Ordinario N° 193 del 18.11.2016 Directora Daf.
-Ordinario N° 199 del 23.11.2016 Directora Daf.

MAT. : Citación "Comité de Seguridad Informático de la Municipalidad, Salud y Educación".

CONCÓN, 01 DIC 2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SRES. SEGÚN DISTRIBUCIÓN

Por medio del presente, se cita a Ustedes a la segunda reunión para el día lunes 12 de diciembre de 2016 a las 16:00 hrs. en la sala de Concejo, con la finalidad de cumplir lo establecido en el Decreto N° 83 del 12.01.2005 del Ministerio Secretaria General de la Presidencia, de conformar el **"Comité de Seguridad Informático"**, el cual deberá estar compuesto por la Directora Daf, Director Secplac, Secretaría Municipal, Director de Control, Encargado de Informática Municipal, Encargado Informática Salud y Encargado de Informática de Educación. Esperamos contar con su presencia, ya que hasta el momento no hemos podido tomar acuerdos muy importantes, como lo son nombrar al Encargado de Seguridad Informática y la aprobación de las Políticas de Seguridad Informática. A la vez se solicita a Educación y Salud nos puedan traer su Plan Informático para el año 2017,

Esperando contar con su asistencia, saluda atentamente a Ud.

ILUSTRE MUNICIPALIDAD DE CONCÓN
DIRECTORA ADMINISTRACION Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
-Secplac.
-Secretaría Municipal.
-Control.
-Informático Daf
- Director Salud
- Informático Salud (Sr. Gonzalo Román)
-Director Daem
- Daem (Informático Daem)
-Archivo.

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ORD.: 204

ANT. : -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia.
-Ordinario N° 88 del 15.11.2016 Director de Control Interno.
-Ordinario N° 193 del 18.11.2016 Directora Daf.
-Ordinario N° 199 del 23.11.2016 Directora Daf

MAT. : Informa sobre segunda Reunión del "Comité de Seguridad Informática de la Municipalidad, Salud y Educación".

CONCÓN, 01 DIC 2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SRA. PAMELA SOTO AGUDO
ALCALDE (S) DE LA ILUSTRE MUNICIPALIDAD DE CONCÓN

Por medio del presente, informo a Usted que el día lunes 28 de noviembre a las 16 hrs. se realizó la segunda reunión del "**Comité de Seguridad Informático**", en la que asistieron el Sr. Guillermo Biadayoli por Educación, el Sr. Gonzalo Román por Salud, el Informático Sr. Pablo Moya y la suscrita, producto de los pocos participantes no se pudieron tomar acuerdos, como elegir el Encargado de Seguridad y Aprobar las Políticas de Seguridad Informática.

De igual manera tratamos de desarrollar algunos temas y esperamos que en la próxima reunión, ya se puedan tomar los acuerdos que se necesitan para seguir avanzando en el trabajo que requiere el "Comité de Seguridad Informático", el cual en el caso de Educación se necesita con urgencia poder contar con un Encargado de Informática, el que debería estar a cargo de todos los establecimientos Educacionales y la parte administrativa del Daem, teniendo la responsabilidad que se cumplan los requerimientos que están expresados en las Políticas de Seguridad Informática. Por lo anterior se invita a Usted a participar de una nueva reunión que sería el lunes 12.12.2016 a las 16:00 hrs. en la Sala de Concejo.

Esperando poder contar con su presencia, saluda atentamente a Usted.

ILUSTRE MUNICIPALIDAD DE CONCÓN
DIRECTORA ADMINISTRACION Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
-Daem
- Daf (Informático Daf)
-Archivo

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ILUSTRE MUNICIPALIDAD DE CONCON * SECRETARIA * CESFAM 23.11.2016

ORD.: 193

ANT. : -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia.
-Ordinario N° 193 del 18.11.2016 Directora Daf.

MAT. : Reitera citación para Conformación "Comité de Seguridad Informático de la Municipalidad, Salud y Educación".

MUNICIPALIDAD DE CONCON
DEPTO. DE CONTROL
23 NOV 2016
RECIBIDO HORA: 13:16

CONCÓN, 23 NOV 2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SRES. SEGÚN DISTRIBUCIÓN

Por medio del presente, se cita a Ustedes a reunión para el día 28 de noviembre de 2016 a las 16:00 hrs. en la sala de Concejo, con la finalidad de cumplir lo establecido en el Decreto N° 83 del 12.01.2005 del Ministerio Secretaria General de la Presidencia, de conformar el **"Comité de Seguridad Informático"**, el cual deberá estar compuesto por la Directora Daf, Director Secplac, Secretaría Municipal, Director de Control, Encargado de Informática Municipal, Encargado Informática Salud y Encargado de Informática de Educación. A su vez se adjunta "Manual de Políticas y Estándares de Seguridad Informática para los usuarios", confeccionado por el Sr. Pablo Moya Encargado de Informática Municipal, con la finalidad que cada uno de Ustedes puedan presentar observaciones, sugerencias u otros en la reunión de Constitución y podamos dejar aprobadas las "Políticas de Seguridad Informática."

El Comité de Seguridad Informática, también tendrá que trabajar en la realización de la "Confección Plan Informático Municipal, Salud, Educación año 2017", por lo que también se solicita si pueden traer ideas con respecto al plan Anual.

Esperando contar con su asistencia, saluda atentamente a Ud.

22-11-16 Pablo Morales

ILUSTRE MUNICIPALIDAD DE CONCON * DIRECTORA ADMINISTRACIÓN Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
-Secplac.
-Secretaría Municipal.
-Control.
-Informático Daf
- Director Salud
- Informático Salud (Sr. Gonzalo Román)
-Director Daem
- Daem (Informático Daem)
-Archivo.

23 NOV 2016 13:09

23/11/2016
I. MUNICIPALIDAD DE CONCON
23 NOV 2016
ALCALDIA

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ORD.: 198

ANT. : -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia.
-Ordinario N° 88 del 15.11.2016 Director de Control Interno.
-Ordinario N° 193 del 18.11.2016 Directora Daf.

MAT. : Informa que no se pudo constituir el "Comité de Seguridad Informática de la Municipalidad, Salud y Educación".

I. MUNICIPALIDAD DE CONCON
23 NOV 2016
ALCALDIA

CONCÓN, 23 NOV 2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SRA. PAMELA SOTO AGUDO
ALCALDE (S) DE LA ILUSTRE MUNICIPALIDAD DE CONCÓN

Por medio del presente, informo a Usted que fuimos instruidos por el Ordinario N° 88 del 15.11.2016 de Director de Control interno para que por nuestro intermedio conformáramos el "**Comité de Seguridad Informático**", y nos adjuntaron el Decreto N° 83 del 12.01.2005 en donde se aprueba "Norma Técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos" , en el que en su artículo segundo, menciona que la Norma deberá ser implementada; el nivel 1; a más tardar en el **2004** y el nivel 2; a más tardar el año **2009** y en su artículo cuarto, menciona que dentro de los **30 días siguientes** se deberá nombrar un Encargado de Seguridad para que desarrolle e implemente las Políticas de Seguridad, en aquellas instituciones que no se designe dentro del plazo, actuará como Encargado de Seguridad el Auditor Interno de Cada Servicio.

Producto de lo anterior la suscrita por Ordinario N° 193 procedió a citar a las diferentes dependencias que conformaran el "Comité de Seguridad Informático", para el día Lunes 21.11.2016 a las 12:00 hrs. en la sala de Concejo, asistiendo la Directora Daf, Encargado de Informática Municipalidad Sr. Pablo Moya y Encargado de Informática Municipalidad sector Salud Sr. Gonzalo Román (Se Adjunta Acta de Asistencia), y la excusa por teléfono del Director de Secplac, no pudiendo constituirse dicho comité por la falta de asistentes a la reunión. Por lo anterior se invita a Usted a participar de una nueva reunión que sería el lunes 28.11.2016 a las 16:00 hrs. en la Sala de Concejo.

Esperando poder contar con su presencia, saluda atentamente a Usted.

ILUSTRE MUNICIPALIDAD DE CONCÓN
DIRECTORA ADMINISTRACIÓN Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
- Daf (Informático Daf)
-Archivo.

REPÚBLICA DE CHILE
I MUNICIPALIDAD DE CONCÓN
ADMINISTRACIÓN Y FINANZAS

ORD.: 193

ANT.: -Decreto N° 83 del 12.01.2005 Ministerio Secretaría General de la Presidencia

MAT.: Conformación "Comité de Seguridad Informática de la Municipalidad, Salud y Educación".

CONCÓN, 18 NOV 2016

DE : SRTA. EVELYN ARIAS ORTEGA
DIRECTORA DE ADMINISTRACIÓN Y FINANZAS

A : SR. OSCAR SUMONTE GONZALEZ
ALCALDE DE LA ILUSTRE MUNICIPALIDAD DE CONCÓN

Por medio del presente, se solicita la participación en reunión para el día 21 de noviembre de 2016 a las 12:00 hrs. en la sala de Concejo, con la finalidad de cumplir lo establecido en el Decreto N° 83 del 12.01.2005 del Ministerio Secretaria General de la Presidencia, de conformar el **"Comité de Seguridad Informática"**, el cual deberá estar compuesto por la Directora Daf, Director Secplac, Secretaría Municipal, Director de Control, Encargado de Informática Municipal, Encargado Informática Salud y Encargado de Informática de Educación, por lo que esta invitación se hace extensiva a las Direcciones y Encargados mencionados.

El Comité de Seguridad Informática, tendrá como uno de sus primeros trabajos, realizar la "Confección Plan Informático Municipal, Salud, Educación año 2017".

Esperando su asistencia, saluda atentamente a Ud.

ILUSTRE MUNICIPALIDAD DE CONCÓN
DIRECTORA ADMINISTRACION Y FINANZAS

EVELYN ARIAS ORTEGA
Directora
Administración y Finanzas

EAO/eao
Distribución:
-Alcaldía.
-Secplac.
-Secretaría Municipal.
-Control.
- Daf (Informático Daf)
- Salud (Informático Salud)
- Daem (Informático Daem)
-Archivo.

REPUBLICA DE CHILE
I. MUNICIPALIDAD DE CONCÓN
DIRECCIÓN DE CONTROL

I. MUNICIPALIDAD DE CONCON
ADMINISTRACION Y FINANZAS
15 NOV 2016
RECIBIDO
HORA: 11:50 Am

ORD. N° : 088/2016

ANT. : Decreto 83, Ministerio Secretaría General de la Presidencia.
Informe Final N° 31/2014, CGR.

MAT. : Comité de Seguridad Informática.

Concón, 15 de noviembre de 2016.

DE : SR. EUGENIO SAN ROMÁN COURBIS,
DIRECTOR DE CONTROL INTERNO.

A : SRTA. EVELYN ARIAS ORTEGA,
DIRECTORA ADMINISTRACIÓN Y FINANZAS.

En cumplimiento al principio de legalidad y la Ley N° 18.695 Orgánica Constitucional de Municipalidades, que en su artículo 29, letras a), b) y c), establece las funciones y competencias que nos rigen como Dirección de Control Interno, por las cuales le corresponde a esta unidad realizar la auditoria operativa interna de la municipalidad, con objeto de fiscalizar la legalidad de los actos administrativos, controlar la ejecución financiera y presupuestaria de la municipalidad y representar los actos que estime ilegales al alcalde, informo lo siguiente:

- El Decreto 83, de fecha 12 de enero de 2005, del Ministerio Secretaría General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Dicha Norma Técnica establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

Al respecto, y como primera medida, vengo en solicitar que por su intermedio se conforme, a la brevedad, el Comité de Seguridad Informática de la Municipalidad, el cual debe estar compuesto, al menos, por Directora Daf (quien deberá presidir dicho Comité por la naturaleza de su cargo), Secplac, Secretaria Municipal, Control, Encargado de Informática Municipal, Encargado Informática Daem, Encargado Informática Salud. Esto, para confeccionar el Plan Informático Municipal, para el año 2017 y siguientes.

También se debe incorporar el Departamento de Informática al Manual de Funciones de la Municipalidad, debiendo informar las Funciones Específicas a desarrollar por este Departamento, las que deben incluir, al menos, las siguientes

- Evaluar periódicamente el cumplimiento del Plan Informático Municipal.
- Asesorar técnicamente a las diferentes Unidades Municipales en el ámbito tecnológico municipal.
- Velar por la oportuna provisión de recursos computacionales en hardware, software y comunicaciones de datos que sean necesarios para el cumplimiento del Plan Informático Municipal, conforme a los recursos disponibles.
- Estudiar y proponer anualmente el presupuesto de los requerimientos municipales en materia informático-computacional, en conformidad a los planes y

proyectos respectivos, para que sea considerado dentro del presupuesto anual de la Municipalidad.

- Administrar los Recursos computacionales centrales, procurando que todo usuario cuente con sus requerimientos específicos en forma oportuna y de acuerdo a los recursos existentes.
- Evaluar, adecuar y mantener los sistemas computacionales existentes en conformidad al Plan Informático Municipal.
- Velar por la seguridad, confiabilidad y confidencialidad de los sistemas computacionales y de la información contenida en las bases de datos centrales y externas.
- Procurar un servicio oportuno y de calidad para la administración, el soporte y servicio técnico de los sistemas y equipos computacionales.
- Proponer y/o ejecutar acciones tendientes a la capacitación y a la información actualizada de los usuarios en materia informático-computacionales.
- Mantener el inventario técnico de los elementos computacionales del municipio y mantener permanentemente informada a la Unidad de Inventarios de todas las adquisiciones y ubicación física de elementos informático-computacionales y de la información computacional municipal.
- Proponer medidas de control del uso y cuidado de los equipos computacionales y de la información municipal a todos los usuarios.

Lo anterior, sin ser taxativas, y entre otras funciones que se le puedan encomendar.

Por último, se sugiere evaluar la posibilidad presupuestaria con el Sr. Alcalde, para que el funcionario encargado de esta Unidad cuente con responsabilidad Administrativa pasando a ser Funcionario a Contrata, o media Contrata, ya que nos es posible que por la responsabilidad que involucra este Cargo siga desempeñándolo sólo en calidad de Honorario.

Adjunto copia de Decreto 83/2005, y copia de Informe Final de Contraloría, Nº 31, que indica todo lo necesario para la correcta implementación y utilización del Plan Anual Informático Municipal.

Lo anterior, para su conocimiento y fines.

Sin más, le saluda atentamente a Ud.

MUNICIPALIDAD DE CONCON
DIRECTOR CONTROL

EUGENIO SAN ROMÁN COURBIS
ABOGADO
DIRECTOR DE CONTROL

ESRC/ppg
Distribución:
1. Directora Daf
cc.- Alcalde
cc.- Secretaría Municipal
cc.- Secplac
cc.- Asesoría Jurídica
cc.- Tránsito y Operaciones
cc.- Dom
cc.- Salud
cc.- Daem
cc.- Juzgado Policía Local
cc.- Auditor Municipal
cc.- Archivo Control

Decreto 83.- :

Tipo Norma	:Decreto 83
Fecha Publicación	:12-01-2005
Fecha Promulgación	:03-06-2004
Organismo	:MINISTERIO SECRETARÍA GENERAL DE LA PRESIDENCIA
Título	:APRUEBA NORMA TECNICA PARA LOS ORGANOS DE LA ADMINISTRACION DEL ESTADO SOBRE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DOCUMENTOS ELECTRONICOS
Tipo Versión	:Única De : 12-01-2005
Inicio Vigencia	:12-01-2005
Id Norma	:234598
URL	:https://www.leychile.cl/N?i=234598&f=2005-01-12&p=

APRUEBA NORMA TECNICA PARA LOS ORGANOS DE LA ADMINISTRACION DEL ESTADO SOBRE SEGURIDAD Y CONFIDENCIALIDAD DE LOS DOCUMENTOS ELECTRONICOS

Núm 83.- Santiago, 3 de junio de 2004.- Vistos: Lo dispuesto en el artículo 32° N° 8 de la Constitución Política de la República; el artículo 3° letra a) del DFL N° 7.912, de 1927; la ley N° 19.799, sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; el decreto supremo N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción; y lo dispuesto en la resolución N° 520, de 1996, que fija el texto refundido, coordinado y sistematizado de la resolución N° 55, de 1992, ambas de la Contraloría General de la República.

Considerando:

1.- Que, el artículo 47 del DS. N° 181 de 2002, del Ministerio de Economía, Fomento y Reconstrucción, Reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, en adelante el Reglamento, creó el Comité de Normas para el Documento Electrónico.

2.- Que, el Comité, en su agenda de trabajo fijada en sesión de fecha 8 de enero de 2003, estableció la determinación de una norma técnica para la seguridad y confidencialidad del documento electrónico y los repositorios en que se almacenan, como una de sus tareas inmediatas.

3.- Que, para el desarrollo de la referida tarea, la Secretaría Técnica del Comité creó un grupo de trabajo sobre seguridad y confidencialidad del documento electrónico, en el que participaron representantes de los miembros del Comité de Normas para el Documento Electrónico, del Ministerio del Interior, de la Contraloría General de la República, del Instituto Nacional de Normalización, del Servicio de Impuestos Internos, del Servicio Nacional de Aduanas, de la Armada de Chile, del Banco Central de Chile, del Banco Estado, de Microsoft, de Orion 2000, de Neosecure, de Sinacofi, y de American Telecommunication, y que fue asesorado técnicamente por la Universidad de Chile a través de CLCERT.

4.- Que el trabajo se realizó de conformidad con la política gubernamental orientada a la incorporación de las Tecnologías de la Información y Comunicaciones en los órganos de la Administración del Estado, para mejorar los servicios e información ofrecidos a los ciudadanos y la eficiencia y la eficacia de la gestión pública, e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.

D e c r e t o:

Artículo primero.- Apruébase la siguiente norma

técnica sobre seguridad y confidencialidad del documento electrónico para los órganos de la Administración del Estado.

''NORMA TECNICA SOBRE SEGURIDAD Y CONFIDENCIALIDAD DEL DOCUMENTO ELECTRONICO''

TITULO I

Ambito de aplicación

Artículo 1°.- La presente norma técnica establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, y las demás cuya aplicación se recomienda para los mismos fines.

Las exigencias y recomendaciones previstas en esta norma, tienen por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general; y salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

Artículo 2°.- Las disposiciones de la presente norma técnica se aplicarán a los documentos electrónicos que se generen, intercambien, transporten y almacenen en o entre los diferentes organismos de la Administración del Estado y en las relaciones de éstos con los particulares, cuando éstas tengan lugar utilizando técnicas y medios electrónicos.

Artículo 3°.- Para los efectos de esta norma, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.

Artículo 4°.- Esta norma se cumplirá en dos etapas, de conformidad con los siguientes niveles:

Nivel 1. Nivel básico de seguridad para el documento electrónico.

Nivel 2. Nivel avanzado de seguridad para el documento electrónico.

TITULO II

Definiciones

Artículo 5°.- Para los propósitos de esta norma, se entenderá por:

a) Autenticación: proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
b) Confidencialidad: aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
c) Contenido del documento electrónico: información, ideas y conceptos que un documento expresa.

d) Continuidad del negocio: continuidad de las operaciones de la institución.
e) Disponibilidad: aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
f) 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.
g) Documentos públicos: aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
h) Documentos reservados: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter.
i) Documentos secretos: los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.
j) Ejecutivo: autoridad dentro de la institución.
k) Identificador formal de autenticación: mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.
l) Incidentes de seguridad: situación adversa que amenaza o pone en riesgo un sistema informático.
m) Información: contenido de un documento electrónico.
n) Integridad: salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.
o) Negocio: función o servicio prestado por la organización.
p) Política de seguridad: conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
q) Repositorio: estructura electrónica donde se almacenan documentos electrónicos.
r) Riesgos: amenazas de impactar y vulnerar la seguridad del documento electrónico y su posibilidad de ocurrencia.
s) Sistema informático: conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, 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.
t) Usuario: entidad o individuo que utiliza un sistema informático.

TITULO III

De la seguridad del documento electrónico en general

Artículo 6°.- La seguridad del documento electrónico se logra garantizando los siguientes atributos esenciales del documento:

a) Confidencialidad;
b) Integridad;
c) Factibilidad de autenticación, y
d) Disponibilidad.

Artículo 7°.- Los atributos esenciales que aportan

seguridad al documento electrónico se obtienen y sostienen mediante la ejecución permanente de las siguientes acciones:

a) Desarrollar y documentar políticas de seguridad de uso, almacenamiento, acceso y distribución del documento electrónico y de los sistemas informáticos utilizados en su procesamiento;
b) Diseñar y documentar los procesos y procedimientos para poner en práctica las políticas de seguridad;
c) Implementar los procesos y procedimientos señalados precedentemente;
d) Monitorear el cumplimiento de los procedimientos establecidos y revisarlos de manera de evitar incidentes de seguridad;
e) Concientizar, capacitar y educar a los usuarios para operar los sistemas informáticos de acuerdo a las exigencias establecidas;
f) Definir y documentar los roles y responsabilidad de las entidades e individuos involucrados en cada una de las letras anteriores.

Artículo 8°.- Los órganos de la Administración regidos por esta norma deberán aplicar sus disposiciones para garantizar los atributos esenciales que confieren seguridad al documento electrónico, definidos en el artículo 6.

No obstante, la consecución y mantención de tales atributos por parte de cada órgano de la Administración del Estado estarán sujetas a la consideración de factores de riesgo y factores de costo/beneficio. Estos últimos podrán invocarse mediante una resolución fundada del jefe de servicio correspondiente, basada en un estudio de análisis de riesgo y/o costo/beneficio.

TITULO IV

Del nivel básico de seguridad del documento electrónico

Párrafo 1°

Normas generales

Artículo 9°.- Durante la primera etapa de aplicación de esta norma, los órganos de la Administración del Estado desarrollarán las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Básico de Seguridad de los documentos electrónicos que se establecen en este Título.

Artículo 10°.- El Nivel Básico de Seguridad para el documento electrónico tiene por objeto:

a) Garantizar condiciones mínimas de seguridad y confidencialidad en los documentos electrónicos que se generan, envían, reciben, procesan y almacenan entre los órganos de la Administración del Estado;
b) Facilitar la adopción de requerimientos de seguridad más estrictos por parte de aquellos organismos y en aquellos tópicos que se estimen necesarios, y
c) Facilitar el Nivel avanzado de seguridad para el documento electrónico, en aquellos organismos cuyo desarrollo institucional lo requiera.

Párrafo 2°

Política de seguridad

Artículo 11.- Deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional.
La política de seguridad deberá incluir, como mínimo, lo siguiente:

a) Una definición de seguridad del documento electrónico, sus objetivos globales, alcance e importancia.
b) La difusión de sus contenidos al interior de la organización.
c) Su reevaluación en forma periódica, a lo menos cada 3 años.

Las políticas de seguridad deberán documentarse y explicitar la periodicidad con que su cumplimiento será revisado.

Párrafo 3°

Seguridad organizacional

Artículo 12.- En cada organismo regido por esta norma deberá existir un encargado de seguridad, que actuará como asesor del Jefe de Servicio correspondiente en las materias relativas a seguridad de los documentos electrónicos.
Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:

a) Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de su organización y el control de su implementación, y velar por su correcta aplicación.
b) Coordinar la respuesta a incidentes computacionales.
c) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

Párrafo 4°

Clasificación, control y etiquetado de bienes

Artículo 13.- Los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección.
La clasificación de un sistema informático debe corresponder a la clasificación más estricta aplicable al documento electrónico que almacene o procese, de conformidad con el decreto supremo 26 de 2001, del Ministerio Secretaría General de la Presidencia.
A cada sistema informático, deberá asignársele un

responsable quien velará por su debida clasificación y etiquetado.

Artículo 14.- Todo documento electrónico deberá ser asignado, explícita o implícitamente, a un responsable. En este último caso, el encargado de seguridad deberá proponer quién será responsable por omisión, sea asignando tal responsabilidad al usuario que lo crea, sea atribuyéndosela al responsable por el sistema informático que lo generó, u otra modalidad.

Artículo 15.- Para cada clasificación, el encargado de seguridad deberá proponer los procedimientos de manipulación requeridos para cubrir las siguientes actividades de procesamiento de un documento electrónico:

a) Copiado;
b) Almacenamiento;
c) Transmisión por correo electrónico y sistemas protocolarizados de transmisión de datos digitales;
d) Destrucción.

Artículo 16.- La salida desde un sistema de un documento electrónico que está clasificado como reservado o secreto, deberá tener una etiqueta apropiada de clasificación en la salida.

Para estos efectos, deberá considerarse, entre otros, los informes impresos, pantallas de computador, medios magnéticos (cintas, discos, CDs, cassettes), mensajes electrónicos y transferencia de archivos.

Párrafo 5°

Seguridad física y del ambiente

Artículo 17.- Los equipos deberán protegerse físicamente de las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables.

En particular, la ubicación del equipamiento de la institución deberá minimizar el acceso innecesario a las áreas de trabajo y disminuir las posibilidades de amenazas de humo y fuego, humedad y agua, inestabilidad en el suministro eléctrico, hurto y robo.

Artículo 18.- Para los efectos del artículo anterior, cada órgano deberá impartir y publicitar instrucciones relativas a los siguientes aspectos del ambiente externo:

a) Consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos.
b) Condiciones climatológicas y ambientales que pueden afectar sistemas informáticos o entornos cercanos.
c) Promoción de una práctica de escritorio limpio.

Artículo 19.- Respecto de los documentos electrónicos de la organización clasificados como reservados o secretos, se aplicarán las siguientes normas de seguridad ambiental:

a) Deberán almacenarse en áreas seguras, protegidos por un perímetro de seguridad definido, con barreras apropiadas de resguardo y controles de entrada. Estos deberán estar físicamente protegidos del acceso no autorizado, daño e interferencia. La protección provista deberá guardar

relación con los riesgos identificados.
b) Deberán disponerse de manera que se minimicen las posibilidades de percances y descuidos durante su empleo.

Párrafo 6°

Seguridad del personal

Artículo 20.- El Jefe de Servicio deberá impartir instrucciones para la seguridad de los documentos electrónicos y los sistemas informáticos, respecto de las siguientes materias:

a) Uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.
b) Uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota, y otros.
c) Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.
d) Procedimientos para reportar incidentes de seguridad.

Artículo 21.- Las responsabilidades de seguridad aplicables al personal deberán ser explicitadas en la etapa de selección e incluirse expresamente en los decretos o resoluciones de nombramiento o en las contrataciones respectivas.

Párrafo 7°

Gestión de las operaciones y las comunicaciones

Artículo 22.- En todos los organismos sujetos a la presente norma, deberán explicitarse y difundirse los siguientes antecedentes e información:

a) Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
b) Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
c) Las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar.

Artículo 23.- Para los efectos de reducir el riesgo de negligencia o mal uso deliberado de los sistemas, deberán aplicarse políticas de segregación de funciones. Asimismo, deberán documentarse los procedimientos de operación de sistemas informáticos e incorporarse mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos.

Artículo 24.- En los órganos regidos por la presente norma, deberán realizarse copias de respaldo de la información y las aplicaciones críticas para la misión de la institución en forma periódica, en conformidad con las siguientes reglas:

a) La periodicidad con que se realizarán los respaldos de los computadores personales de la institución que estén asignados a usuarios, deberá explicitarse y no podrá ser menor a 1 respaldo anual;
b) La periodicidad con que se realizarán los respaldos de los sistemas informáticos y los equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos electrónicos, deberá explicitarse y no podrá ser menor a 1 respaldo mensual;
c) Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales;
d) Deberá almacenarse en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento. Esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo;
e) Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.
f) Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados, y
g) Deberán utilizarse medios y condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos definidos en el punto precedente.

Artículo 25.- Las instituciones regidas por la presente norma deberán impartir instrucciones respecto al uso seguro del correo electrónico. Esas instrucciones deberán incluir al menos:

a) Una advertencia sobre la vulnerabilidad del correo electrónico a modificaciones o accesos no autorizados;
b) Una advertencia sobre los peligros asociados a la apertura de archivos adjuntos y/o a la ejecución de programas que se reciban vía correo electrónico;
c) La responsabilidad de no divulgar contraseñas de acceso al correo electrónico;
d) Una advertencia sobre la inconveniencia de almacenar contraseñas de acceso al correo electrónico en el mismo computador desde el cual se accede el correo electrónico;
e) Indicaciones sobre la elección de contraseñas seguras de acceso al correo electrónico;
f) Una recomendación sobre la conveniencia de que los usuarios tengan cuentas de correo electrónico distintas para efectos de su uso personal;
g) Un instructivo de cuándo no usar el correo electrónico;
h) Una prevención sobre la necesidad de comprobar el origen, despacho, entrega y aceptación mediante firma electrónica, e
i) Una precisión de las responsabilidades que corresponden a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, etc.

Artículo 26.- Los organismos sujetos a la presente

norma, en la medida de sus posibilidades, deberán:

a) Instalar un antivirus que proteja frente a la posibilidad de obtener vía correo electrónico software malicioso;
b) Proveer mecanismos que mediante el uso de técnicas de cifrado, permitan proteger la confidencialidad e integridad de los documentos electrónicos;
c) Evitar el uso de cuentas de correo grupales;
d) Disponer controles adicionales para la verificación de mensajes que no se pueden autenticar;
e) Verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de ser posible, sean reformateados previo a ser dados de baja.

Párrafo 8°

Control de acceso

Artículo 27.- El empleo de identificador formal de autenticación constituye un mecanismo básico para el uso de firma electrónica.
Los identificadores son un esquema de validación de la identidad del usuario para acceder a un sistema informático.
Un identificador temporal es aquel que se asigna a un usuario la primera vez que accede a un sistema, y que debe ser cambiado por éste en su primer acceso.

Artículo 28.- La asignación de los identificadores se deberá controlar mediante un proceso formal de gestión, en que el jefe directo del usuario peticionario será el responsable de la respectiva solicitud.
Para los efectos del referido control, en cada institución se impartirán instrucciones sobre la forma de asignación de identificadores que se aplicará. Dichas instrucciones deberán incluir a lo menos, lo siguiente:

a) La obligación de mantener en forma confidencial de los identificadores que se asignen;
b) La obligación de no registrar los identificadores en papel;
c) La prohibición de almacenar identificadores en un computador de manera desprotegida;
d) El deber de no compartir los identificadores de usuarios individuales;
e) El mandato de no incluir el identificador en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado en una macro;
f) La indicación de cambiar los identificadores cuando hayan indicios de un posible compromiso del identificador o del sistema;
g) La recomendación de elegir identificadores que tengan una longitud mínima de ocho caracteres; sean fáciles de recordar; contengan letras, mayúsculas, dígitos, y caracteres de puntuación; no estén basados en cosas obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; y no sean palabras de diccionario o nombres comunes;
h) La indicación de cambiar los identificadores a intervalos regulares. Las contraseñas de accesos privilegiados se deberán cambiar más frecuentemente que los identificadores normales;
i) Normas para evitar el reciclaje de identificadores

viejos, y
j) La indicación de cambiar el identificador temporal al iniciar la primera sesión.

Los sistemas informáticos deberán configurarse de manera que los usuarios se vean compelidos a cumplir con las obligaciones detalladas en los puntos anteriores.

Artículo 29.- Se deberá entregar a los usuarios identificadores temporales de una manera segura. Específicamente, se deberá evitar el uso de terceras partes o mensajes de correo electrónico no protegido (texto en claro) para comunicar el identificador.
Los usuarios deberán dar un acuso recibo de recepción del identificador.

Artículo 30.- En caso que los usuarios necesiten acceder a múltiples servicios o plataformas y sea necesario que mantengan múltiples identificadores, deberán ser notificados de que éstos deben ser distintos. Asimismo, se incentivará y facilitará el uso de certificados de firma electrónica.

Artículo 31.- Para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, se deberá promover buenas prácticas, como las de pantalla limpia.
En particular, se incentivará a los usuarios o configurar los sistemas de manera que se dé cumplimiento a los siguientes estándares:

a) Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;
b) Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos, y
c) Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

Artículo 32.- Se deberá controlar el acceso a los servicios de red internos y externos mediante el uso de identificadores o certificados digitales.
Para tal efecto, los órganos de la Administración del Estado sujetos a la presente normativa deberán ajustarse a las siguientes exigencias:

a) Restringir la instalación de equipamiento personal que dificulte el control de acceso a documentos electrónicos y sistemas informáticos, de manera acorde a las políticas de seguridad de la institución, y
b) Mantener un catastro del equipamiento que permita la reproducción, distribución o transmisión masiva de información, y de las personas con privilegios de acceso a ellos.

Artículo 33.- Las instituciones regidas por la presente norma impartirán instrucciones relativas al uso de redes y servicios en red que, al menos, especifiquen lo siguiente:

a) Las redes y servicios de red a las que el acceso está permitido;
b) Los procedimientos de autorización para determinar quién tiene permitido acceder a las distintas redes y servicios de red, y
c) Los controles de gestión y procedimientos para

proteger el acceso a las conexiones de la red y servicios de red.

Párrafo 9°

Desarrollo y mantenimiento de sistemas

Artículo 34.- Aquellos organismos que requieran precaver que la seguridad esté incorporada en los sistemas en la etapa de diseño, se entenderán como organismos complejos y para tal efecto, deberán adoptar las indicaciones contenidas en la sección correspondiente del Título V de esta norma, sobre ''Nivel Avanzado de Seguridad para el Documento Electrónico''.

Párrafo 10

Gestión de la continuidad del negocio

Artículo 35.- El encargado de seguridad deberá formular un plan de contingencia para asegurar la continuidad de operaciones críticas para la institución. Este plan deberá, como mínimo, disponer la efectiva gestión de las relaciones públicas, la eficiente coordinación con las autoridades apropiadas, como policía, bomberos, autoridades directivas, etc., y mecanismos eficaces para convocar a quienes sean los responsables de los documentos electrónicos y sistemas informáticos afectados.

TITULO V

Del nivel avanzado de seguridad del documento electrónico

Artículo 36.- Durante la segunda etapa de aplicación de esta norma, los órganos de la Administración del Estado deberán desarrollar las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Avanzado de Seguridad de los documentos electrónicos que se establecen en este Título.

Artículo 37.- El Nivel Avanzado de seguridad para el documento electrónico exige el cumplimiento de las exigencias y condiciones reguladas en el Título IV para el Nivel Básico de seguridad, y las previstas en la Norma NCh2777, que se entiende parte integrante del presente decreto, con los ajustes que se establecen en este artículo.

NOTA

a) Política de Seguridad:

Se aplicarán las disposiciones contenidas en el capítulo 3 de la norma NCh2777, con la siguiente adecuación:

- Las instituciones deberán tener las políticas de seguridad descritas en la sección 3.1 para los repositorios de documentos electrónicos. En particular, estas políticas deberán contener lo

siguiente:

i. Indicaciones respecto de los sistemas informáticos, con énfasis en el procedimiento de autorización de instalación o modificación de software y archivos de configuración de los sistemas;
ii. Indicaciones de uso de la red;
iii. Procedimientos de respuesta a incidentes de seguridad;
iv. Procedimientos de delegación de autoridad para ejecutar acciones de emergencia en los sistemas y los procedimientos correspondientes.

b) Seguridad organizacional:

Se aplicará la sección 4.1 del capítulo 4 de la norma NCh2777, con excepción de sus puntos 4.1.5 y 4.1.7 que se adoptarán como recomendaciones, y las secciones 4.2 y 4.3 de dicho capítulo.

c) Clasificación y control de bienes:

Se aplicará la sección 5.1 del capítulo 5 de la norma NCh2777, en lo referido a bienes relacionados con el Documento Electrónico. Asimismo, se aplicará el punto 5.2.1 de la sección 5.2.
El punto 5.1.2 de dicha sección se aplicará con las siguientes adecuaciones:

- Los procedimientos de etiquetado y manipulación de la información se entienden referidos al Documento Electrónico.
- Se excluyen las normas contenidas en las letras (c) y (d).

d) Seguridad del personal:

Se aplicarán las secciones 6.1 y 6.3 del capítulo 6 de la norma NCh2777. La sección 6.2 se adoptará como recomendación.

e) Seguridad física y del ambiente:

Se aplicarán las secciones 7.1 y 7.2 del capítulo 7 de la norma NCh2777, para repositorios de documentos electrónicos, con las siguientes adecuaciones:

Nch 2777

- Para la sección 7.1:

i. Los controles físicos de entrada en el perímetro de seguridad deberán utilizar el carné de identidad como identificación válida en el caso de los chilenos, y el pasaporte en el caso de los extranjeros.
ii. Todo ingreso de visitas al perímetro de seguridad deberá ser autorizado por escrito, quedando constancia del propósito y duración de ella. Los visitantes serán acompañados en todo momento por alguna persona autorizada de la organización hasta que abandonen el recinto.

- Para la sección 7.2:

Se deberá velar para que los equipos computacionales en los que se almacenen documentos electrónicos y sistemas informáticos que los procesen, tengan un adecuado suministro de energía eléctrica, incluyendo no sólo el flujo de energía suministrado,

sino también la ''tierra eléctrica'' de las instalaciones.
La sección 7.3 se adoptará como recomendación.

f) Gestión de las operaciones y comunicaciones:

Se aplicarán las normas del capítulo 8 de la norma NCh2777, en su integridad.

g) Control de acceso:

Se aplicarán las normas del capítulo 9 de la norma NCh2777, con excepción de sus secciones 9.5, 9.6, 9.7 y 9.8 que se adoptarán como recomendaciones, y con los siguientes ajustes:

- Los registros de privilegios asignados, a los que hace referencia la sección 9.2.2, deberán tener un carácter histórico, es decir, no sólo se deben registrar los privilegios en aplicación. El período de conservación de estos registros será al menos el que las leyes vigentes indiquen para los documentos electrónicos a los que se pudo tener acceso con dichos privilegios.
- Las estipulaciones de la sección 9.4 deberán formalizarse en una política de uso correspondiente, de acuerdo a lo expresado en la sección ''Política de Seguridad''.

h) Desarrollo y mantenimiento de sistemas:

Se aplicarán únicamente las normas de la sección 10.3 del capítulo 10 de la norma NCh2777, con la siguiente adecuación:

- En las secciones referidas a firma electrónica, se adoptará lo establecido por la ley 19.799, sobre documentos electrónicos, firma electrónica y los servicios de certificación para dicha firma.

i) Gestión de la continuidad del negocio: Se aplicarán las estipulaciones del capítulo 11 de la norma NCh2777, en su integridad.

NOTA
El Artículo 2° de la Resolución 1535 Exenta, Economía, publicada el 02.09.2009, anula y reemplaza la Norma NCh2777 por la Norma NCh-ISO 27002, que el Artículo 1° de la mencionada Resolución, declara como Norma Oficial de la República de Chile, con su respectivo código y título de identificación como Tecnología de la información, Códigos de prácticas para la gestión de la seguridad de la información.

Artículo Segundo.- La presente norma deberá ser implementada por los diferentes órganos de la Administración del Estado dentro de los siguientes plazos:
- El Nivel 1, a más tardar en el año 2004.
- El Nivel 2, a más tardar en el año 2009.

Con la finalidad de lograr la debida implementación de esta norma en los plazos señalados, los servicios públicos deberán contemplar acciones adecuadas en sus respectivos

planes de desarrollo informático. Los niveles de cumplimiento de la presente norma por parte de los servicios públicos se determinarán mediante la aplicación de un instrumento de evaluación que elaborará el Comité de Normas.

Artículo Tercero.- Créase el Subcomité de Gestión de Seguridad y Confidencialidad del Documento Electrónico como organismo asesor del Comité de Normas para el Documento Electrónico.

El Subcomité será coordinado por el Ministerio del Interior y tendrá entre sus funciones, proponer el Nivel de cumplimiento de la presente norma técnica por parte de los órganos de la Administración del Estado y el cronograma de implementación de la Norma en su nivel 2 por parte de los diferentes órganos de la Administración del Estado.

Artículo Cuarto.- Los Subsecretarios y Jefes de Servicio deberán designar, dentro del plazo de 30 días contados desde la fecha de total tramitación del presente decreto, un Encargado de Seguridad, para que desarrolle e implemente las políticas de seguridad en forma conjunta con el Comité de Gestión de Seguridad y Confidencialidad. En aquellos órganos en que no se designe dentro de plazo, actuará como Encargado de Seguridad el Auditor Interno de cada servicio.

Artículo Quinto.- El Comité de Normas para el Documento Electrónico podrá iniciar, de oficio o a petición de parte, un procedimiento de normalización con el objeto de sugerir al Presidente de la República la actualización de la norma técnica fijada por este decreto. En dicho procedimiento se tendrán en consideración los planteamientos del sector público y privado y de las Universidades.''.

Anótese, tómese razón y publíquese.- RICARDO LAGOS ESCOBAR, Presidente de la República.- Francisco Huenchumilla Jaramillo, Ministro Secretario General de la Presidencia.- José Miguel Insulza Salinas, Ministro del Interior.

Lo que transcribo a Ud. para su conocimiento.- Saluda Atte. a Ud., Rodrigo Egaña Baraona, Subsecretario General de la Presidencia.