SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

CIRCULAR INTERNA 01

MAT.: Instructivo interno de buenas prácticas en el uso de sistemas informáticos institucionales.

ANT.: Decreto Supremo N°83 de 3 de junio de 2004 y Decreto Supremo N°93 de 9 de mayo de 2006, ambos del Ministerio Secretaría General de la Presidencia.

SANTIAGO, 22 OCT. 2010

DE: SUPERINTENDENTE DE CASINOS DE JUEGO

A : FUNCIONARIOS DE LA SUPERINTENDENCIA DE CASINOS DE JUEGO

La información con que cuenta la Superintendencia es uno de sus activos más importantes y, por lo tanto, debe ser adecuadamente resguardada por cada uno de sus funcionarios, para no comprometer la continuidad operativa, credibilidad o la imagen pública de la institución.

La seguridad de la información electrónica o seguridad informática es entendida como el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información residente o transmitida por sus sistemas como activo valioso, con la finalidad de minimizar las amenazas y riesgos continuos a los que dicha información está expuesta.

La presente circular interna trata acerca de la protección de la información de los documentos electrónicos, entendiendo por éstos *"...toda representación de un hecho, imagen o idea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior"*.

En mérito de expuesto, de acuerdo a lo indicado en los decretos individualizados en el antecedente --cuyas directrices deben ser cumplidas por todos los órganos de la administración del Estado-- y considerando la necesidad de resguardar la

privacidad, seguridad y el buen uso tanto de las herramientas y sistemas informáticos institucionales, como de la información administrada a través de éstos, vengo en impartir las siguientes instrucciones para proteger la información institucional residente en los sistemas computacionales de esta Superintendencia:

I) DEL USO DE LOS SISTEMAS INFORMÁTICOS

1 Uso del Sistema Operativo

1.1 Clave de Acceso

a. La clave de acceso que utilicen los funcionarios deberá ser alfanumérica (letras y números), y contar con una extensión mínima de 8 caracteres. Su uso será personal e intransferible.

b. Para velar por la seguridad y privacidad de la referida clave, ésta deberá ser modificada por el usuario cada 90 días y no se permitirá su reemplazo por la clave anterior.

c. Ante tres intentos fallidos de acceso a una sesión de usuario, será bloqueado el acceso a la cuenta, y se deberá recurrir a la Unidad de Informática para dar solución al eventual bloqueo.

d. Al acceder a sus correos electrónicos a través de webmail, los funcionarios deberán adoptar las medidas necesarias para no ingresar desde un equipo compartido, que manifiestamente se encuentre desprotegido ante Spywares, tales como programas de captura de password.

1.2 Almacenamiento de información

a. Se han definido nueve Unidades Organizacionales usuarias (UO), representativas del quehacer institucional, que agrupan funcionarios con privilegios y recursos de red compartidos, tales como discos e impresoras. Para cada una de dichas Unidades Organizacionales, se han definido tres perfiles de usuario para el manejo de información: Secretaria, Profesional y Jefaturas.

Las unidades organizacionales definidas son las siguientes:

- Gabinete.
- División de Fiscalización, División Jurídica, División de Estudios.

- Unidad de Administración y Finanzas, Unidad de Comunicaciones, Unidad de Informática, Unidad de Atención a Clientes, Unidad de Auditoría.

b. Los archivos de trabajo deberán ser administrados en los discos de red configurados en cada equipo y conforme a las necesidades que definan las respectivas jefaturas. Los archivos de carácter personal, como música, fotografías o similares, no podrán ser almacenados en los discos de red, ya que afectan la capacidad de almacenamiento y respaldo de la información organizacional. Las unidades de disco de red definidas, a las que podrá acceder cada usuario, de acuerdo a su perfil, son las siguientes:

Disco F:\
- Disco para mantener información de trabajo personal de cada funcionario, al cual ningún otro usuario o administrador tendrá acceso. Se permitirá una capacidad de almacenamiento de hasta 5 Gbytes por disco.

Disco J:\
- Disco común para toda una UO, incluida Secretarias, Profesionales y Jefaturas. El Superintendente tendrá acceso a todos los discos J:\.

Disco Z:\
- Disco compartido por toda la institución, sin excepción, que permite la mantención de directorios de las UO. Los miembros de cada UO tendrán, de manera exclusiva, la posibilidad de escribir o modificar archivos pero con la alternativa de que sean leídos por los demás usuarios.

Disco R:\
- Disco en el que cada UO puede almacenar y procesar su información, y que será compartida por los respectivos profesionales y la jefatura correspondiente.

c. Los archivos de todos los discos serán respaldados diariamente y, en caso de pérdida de información, la recuperación de ésta deberá ser solicitada al Jefe de la Unidad de Informática por medio de un correo electrónico enviado por la jefatura correspondiente, indicando el archivo, la fecha y el motivo para gestionar su recuperación.

A partir del año 2011, durante el primer semestre de cada año, se realizará el respaldo anual de la información almacenada en cada equipo de usuario.

1.3 Seguridad e Instalación de Software

a. Se prohibe violar o intentar violar los sistemas a los cuales se tenga acceso, tanto a nivel local como externo.

b. Los usuarios tendrán acceso a sus estaciones de trabajo, pero no a directorios reservados, tales como archivos del sistema y de configuración básica de la estación (interfaces de redes, configuración de discos, y otros).

c. No se permitirá que los usuarios instalen en forma directa cualquier aplicación que no haya sido previamente autorizada por el Jefe de la Unidad de Informática. Para obtener la referida autorización, se deberá enviar una solicitud al Jefe de la Unidad de Informática, a través de correo electrónico. Previo análisis de si se justifica o no la instalación de la aplicación respectiva, considerando para estos efectos si está o no licenciada y si reviste algún riesgo de seguridad, el Jefe de la Unidad de Informática se pronunciará otorgando o denegando la autorización requerida y comunicando su decisión al solicitante.

2 Uso de Sistemas de Apoyo como Sistema de Personal y Remuneraciones, Sistema de Correspondencia, Sistema de Materiales y Sistema de Activo Fijo

a. La clave de acceso de los funcionarios es personal e intransferible, y compromete la responsabilidad del usuario en el uso y modificación de la información respectiva, de acuerdo a las funciones que le competan.

b. La información a la que cada usuario acceda en estos sistemas, sólo podrá ser comunicada a las jefaturas correspondientes, cuando ésta sea de carácter público, prohibiéndose estrictamente compartir o difundir cualquier tipo de información privada de funcionarios de la Superintendencia, o que corresponda a terceros, de conformidad a los dispuesto en la Ley N°19.628 sobre protección de la vida privada o protección de datos de carácter personal.

c. En caso de problemas con funcionalidades de un sistema particular, o para un usuario específico, éstas deberán ser reportadas al Jefe de la Unidad de Informática de la Superintendencia por medio de correo electrónico.

II. DEL USO DE INTERNET

a. Se prohíbe que, desde el equipo que la Superintendencia ha puesto a su disposición, los funcionarios accedan a sitios que comprometan la seguridad de los sistemas que resguardan la información electrónica de la institución, o a sitios con contenidos ilegales u ofensivos (sitios de violencia en línea, de software ilegal, de pornografía, de juegos en Internet, etc.), que no tengan por finalidad ser utilizados para propósitos laborales.

b. Se prohíbe la distribución maliciosa de archivos conteniendo virus, "gusanos", "troyanos", así como la realización de cualquier tipo de actividad destructiva y/o de hackeo.

c. Debido a la alta peligrosidad que representan para la institución tanto en términos de la seguridad de la información y el resguardo de su confidencialidad, como de la recarga que ello implica para el ancho de banda de la red del Estado, en desmedro de los restantes usuarios, se prohíbe el acceso desde las estaciones de trabajo de la Superintendencia a los sitios y servicios de comunicación externos que a continuación se detallan:
   - Sitios de Videos On Demand o a Radios On Line, excepto aquellos casos, debidamente calificados por el Superintendente, en que sea necesario para propósitos laborales.
   - Servicios de mensajería instantánea o chat como Gtalk, Yahoo Messenger, Skype o ICQ. Se proveerá un acceso restringido a las funciones de MSN Messenger, a través del sistema MS OCS (MS Office Communicator Service), que permite la habilitación de la función de chat en un entorno seguro, con bloqueo de la posibilidad de intercambiar archivos, o realizar conversaciones de voz y de video. Se exceptúa de esta regla la habilitación de reuniones por videoconferencia con propósitos laborales.
   - Aplicaciones de transferencia de información de computador a computador tales como Ares, Kazaa, Emule, Gnutella.
   - Sitios que permiten bajar software de juegos o de sistemas con licencias adulteradas, pues conllevan la introducción a la red de Spyware o Malware.

d. Además, ante eventos de seguridad o de baja de rendimiento en la red, se podrá restringir el uso de aplicaciones internet como las redes sociales, entre las que están: Facebook, MySpace, Twitter, Flickr, Windows Live Spaces, las

que poseen asociadas aplicaciones, que permiten el intercambio de archivos y el uso de correos externos.

e. Por último, debido a la imposibilidad de aplicar las políticas contenidas en este documento a los sistemas de correo externos a la Superintendencia y, por lo tanto, al no poder garantizar respecto de dichos servicios estándares de seguridad y confidencialidad de la información, sólo se permitirá el uso de correo institucional y se bloqueará el acceso a correos externos personales, exceptuando los casos expresamente autorizados por el Superintendente.

III. DEL USO DEL CORREO ELECTRÓNICO

1. Uso del correo electrónico

a. El usuario deberá mantener bajo reserva su clave de acceso a su cuenta en el servidor de e-mail, la que será personal e intransferible.

b. El usuario tiene prohibido intentar acceder en forma no autorizada a la cuenta de correo de otro usuario y tratar de usurpar su identidad.

c. La cuenta de correo electrónico tendrá como máximo 4 GB de información almacenada en el servidor de correo. Esta capacidad de almacenamiento puede ser aumentada si los usuarios trasladan los correos más antiguos a los discos de red, lo que debe ser solicitado a la Unidad de Informática.

d. Se prohíbe la emisión de opiniones personales en foros de discusión u otras instancias de naturaleza polémica a través de la cuenta de correo institucional.

e. Los usuarios deberán usar un lenguaje respetuoso en los mensajes que dirijan tanto a usuarios internos como externos. Los referidos mensajes no podrán contener alusiones que puedan ser consideradas insultantes, injuriosas, amenazadoras, ofensivas, obscenas, racistas o sexistas.

f. Los usuarios deberán tener presente que la dirección e-mail institucional está destinada principalmente para su uso laboral, en consecuencia, cualquier otro tipo de utilización, deberá ser, en la medida de lo posible, derivada a una instancia fuera de la organización, como, por ejemplo, el hogar.

g. Los funcionarios deberán evitar informar su correo electrónico a menos que sepan quién lo utilizará.

h. El sistema de correo electrónico que la institución ha puesto a disposición de los usuarios es una herramienta de trabajo que debe ser usada para propósitos laborales. La información intercambiada por este medio deberá usarse privilegiando los propósitos institucionales y la Superintendencia estará facultada para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su uso correcto sujeto a la ley vigente.

i. El usuario deberá abstenerse de transmitir información reservada por este medio dado que no está garantizada la confidencialidad de los textos enviados a través de internet, a menos que éstos sean previamente encriptados.

j. Está prohibido a los usuarios enviar mensajes a otros usuarios o grupos que no los quieran recibir.

k. Se prohíbe a los funcionarios molestar a otros usuarios tanto internos como externos enviando cadenas de mensajes, promociones comerciales o mensajes repetitivos.

l. Está prohibido a los usuarios el uso de seudónimos u otros mecanismos o sistemas para ocultar su identidad. En todos los mensajes debe estar claramente identificado su origen.

m. Se prohíbe hacer un uso comercial de la dirección de e-mail proporcionada por la Superintendencia a sus funcionarios, y enviar publicidad a otros usuarios con el e-mail de la Institución.

n. Los listados de correos electrónicos institucionales sólo pueden ser utilizados para consulta y son de uso exclusivo para los funcionarios de la institución, estando prohibido difundir este listado por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

2. De los Correos SPAM

El presente título contiene un conjunto de instrucciones, recomendaciones e información relativa a los correos Spam que los funcionarios de la Superintendencia deberán cumplir y tener presentes durante el desempeño de sus labores:

a. Los funcionarios no deberán abrir los correos SPAM. En tales casos, se deberán ver las propiedades de dichos correos y enviar dicha información al administrador de la red.

b. No se deberán responder los correos SPAM, pues esto solamente servirá para confirmar que su cuenta de correo está activa.

c. A través del correo institucional, no se podrán comprar productos publicitados a través de correo electrónico no solicitado.

d. Los funcionarios deberán abstenerse de recibir, abrir y/o ejecutar programas o documentos con contenido ejecutable cuya procedencia no sea conocida o sea sospechosa dado que puede tratarse de programas maliciosos (virus/troyanos/botnet/spamvirus). Además, los funcionarios tienen prohibido difundir este tipo de contenidos a otros usuarios internos o externos. Por ningún motivo el usuario deberá abrir y/o ejecutar archivos que tengan doble extensión (ej.: nombre_archivo.doc.exe), o que tengan la extensión .PIF, .LNK, .BAT, .EXE, .COM, .VBS, .SHS, .SCR., .VBE o .OCX (entre otras extensiones peligrosas).

e. Las entidades financieras nunca le solicitarán datos personales mediante e-mail.

f. El "Phishing" es un tipo de delito que corresponde a una forma de las estafas, y que se comete intentando adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). Si encuentra y/o recibe un mail del tipo "Phishing" o descubre un sitio web fraudulento, infórmelo a la Unidad de Informática, siguiendo el procedimiento indicado en el Título V de la presente Circular Interna.

g. Siempre compare el link que aparece en el e-mail con el que finalmente le ha sido dirigido. Contacte a la empresa emisora para verificar que el e-mail recibido es genuino.

h. Considere sospechoso cualquier correo no solicitado que le requiera datos personales.

i. Evite llenar formularios en mensajes e-mail que requieren información personal.

IV. GENERACIÓN, TRANSMISIÓN, RECEPCIÓN Y PROCESAMIENTO DE DOCUMENTOS ELECTRÓNICOS

a. Los usuarios de la institución deberán respetar la naturaleza confidencial de los datos que administren como parte de su trabajo, haciendo un uso responsable de la información confiada a cada cual según las funciones que le competen.

b. La documentación concerniente al trabajo propio de la institución deberá ser almacenada en los discos de red, y conforme a las necesidades que se definan por las jefaturas respectivas.

V. PROCEDIMIENTO PARA REPORTAR INCIDENTES DE SEGURIDAD

Un incidente de seguridad es cualquier hecho o evento que se cree podría afectar su seguridad personal o a la seguridad de la organización, en tanto que una amenaza corresponderá a cualquier situación o suceso intencionado, que pueda afectar adversamente a los mismos. Atendido lo expuesto anteriormente, se puede decir que, las amenazas tienen un objetivo y los incidentes simplemente ocurren.

Un incidente o amenaza en la seguridad informática puede generar múltiples problemas al interior de la organización, como la pérdida o robo de información trascendente, destrucción o corrupción de información clasificada, pérdida de credibilidad o imagen pública. Es por estas razones que existe la necesidad de generar y difundir procedimientos prácticos y claros para responder frente a la presencia de estas situaciones.

Un funcionario de la Superintendencia, en caso de encontrarse frente a cualquiera de las dos situaciones antes descritas, deberá hacer un reporte inmediato al Jefe de la Unidad Informática de la institución y a su jefe directo, con el fin de adoptar acciones rápidas de respuesta, por medio de correo electrónico en el que se incluyan todos los antecedentes, o telefónicamente, debiendo posteriormente formalizarlo por el correo institucional.

Les saluda atentamente,

SUPERINTENDENCIA DE CASINOS DE JUEGO
SUPERINTENDENTE

FRANCISCO LEIVA VEGA
SUPERINTENDENTE DE CASINOS DE JUEGO

MLC/FRV
Distribución:
- Funcionarios de la SCJ
- Unidad de Administración y Finanzas SCJ
- Oficina de Partes SCJ