SCJ | SUPERINTENDENCIA DE CASINOS DE JUEGO

CIRCULAR INTERNA N° 6

MAT.: Deja sin efecto Circular Interna N° 1 de 22 de octubre 2010 e imparte instrucciones acerca de buenas prácticas en el uso de sistemas informáticos institucionales.

ANT.: Circular Interna N° 1 de 22 de octubre 2010, Instructivo interno de buenas prácticas en el uso de sistemas informáticos institucionales a funcionarios de la SCJ.

D.S. N°83 de 03.06.2004 y D.S. N°93 de 09.05.2006, ambos del Ministerio Secretaría General de la Presidencia.

SANTIAGO, 29 ENE 2013

VISTOS; lo dispuesto en la Ley N° 19.995 que establece las Bases Generales para la Autorización, Funcionamiento y Fiscalización de Casinos de Juego; en la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en el D.F.L N° 29, de 2004, del Ministerio de Hacienda, que Fija el Texto Refundido, Coordinado y Sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; en la Ley N° 19.880 que establece las Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado; en el D.S. N° 83, de 2004 y D.S. N° 93 de 2006, ambos del Ministerio Secretaría General de la Presidencia; en el Decreto Supremo N° 573, de 2012, del Ministerio de Hacienda; así como en las demás disposiciones pertinentes; dicto la siguiente:

CONSIDERANDO

1.- Que, conforme a la Ley Nº19.995 sobre Bases Generales para la Autorización, Funcionamiento y Fiscalización de Casinos de Juego, creó la Superintendencia de Casinos de Juego, que es un organismo del Estado, de carácter autónomo, con personalidad jurídica y patrimonio propio, cuya misión es supervigilar y fiscalizar el cumplimiento de las disposiciones legales, reglamentarias y técnicas para la instalación, administración y explotación de los casinos de juego en el país.

2.- Que, en ese contexto, la Ley N°19.995, establece que al Superintendente le corresponde, entre otras atribuciones, dirigir y organizar el funcionamiento de la Superintendencia de Casinos de Juego.

3.- Que, lo estipulado en el artículo 20 del D.S. N°83, de 2004, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos, señala que "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

12000513

mensajería y comunicación remota, entre otros.

c) Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.

d) Procedimientos para reportar incidentes de seguridad."

4.- Que, lo estipulado en el artículo 9 del D.S N°93, de 2006, que aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del Estado y sus funcionarios, señala que "Los órganos del Estado deberán instruir a sus funcionarios acerca de la adecuada utilización de las casillas institucionales que se le asignen para el cumplimiento de sus funciones".

5.- Que, para esta Superintendencia la información es uno de sus más importantes activos y, por lo tanto, debe ser adecuadamente resguardada a fin de no comprometer la fe pública, la continuidad operativa, la credibilidad o la imagen de la institución.

6.- Que, teniendo presente las normas legales antes descritas, a objeto de desarrollar las funciones que la ley señala y dar cumplimiento a los objetivos establecidos, y en ejercicio de mis facultades legales, dicto la siguiente:

RESOLUCIÓN:

1.- Déjese sin efecto la Circular N° 1 de 22 de octubre 2010 que instruye acerca buenas prácticas en el uso de sistemas informáticos institucionales a funcionarios de la SCJ.

2.- IMPÁRTENSE las siguientes:

INSTRUCCIONES ACERCA DEL USO DE SISTEMAS INFORMÁTICOS INSTITUCIONALES, A FUNCIONARIOS DE LA SUPERINTENDENCIA DE CASINOS DE JUEGO

I). CONTEXTO GENERAL

La seguridad de la información electrónica o seguridad informática es el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información residente o transmitida por sus sistemas como activo valioso, a fin de minimizar las amenazas y riesgos continuos a los que está expuesta. En particular, esta circular establece un conjunto de buenas prácticas en el uso de sistemas informáticos institucionales para 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".

De lo anterior, en consideración a la necesidad de resguardar la privacidad, seguridad y el buen uso de las herramientas y sistemas informáticos institucionales, así como de la información administrada por éstos, de acuerdo a lo indicado en los decretos del antecedente, cuyas directrices deben ser cumplidas por todos los órganos de la administración del Estado, se informan e instruyen las siguientes medidas para proteger la información institucional residente en sistemas computacionales.

II). 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 debe ser almacenada en los discos de red, y conforme a las necesidades que se definan por las jefaturas respectivas.

III). USO DE SISTEMAS INFORMÁTICOS

1 Uso del Sistema Operativo

1.1 Clave de Acceso

a. La clave de acceso es alfanumérica (letras y números), y de una extensión mínima de 8 caracteres, de uso personal e intransferible.

b. Para velar por la seguridad y privacidad de la clave de usuario, la clave será modificada cada 90 días y no se permitirá su modificación por la clave anterior.

c. Ante tres intentos fallidos de acceso a la sesión de usuario, se bloqueará el acceso a la cuenta, y será necesario acudir a la Unidad de Informática para dar solución a un eventual bloqueo.

d. Al acceder a su correo electrónico a través de webmail, debe tener la cautela de no ingresar desde un equipo compartido, que manifiestamente se encuentre desprotegido ante Spywares (programas espías para recopilar información sensible), como programas de captura de password.

1.2 Almacenamiento de información

a. Se han definido las siguientes 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 ellas, se definieron tres perfiles de usuario para el manejo de información: Secretaria, Profesional y Jefaturas. Las unidades organizacionales definidas son:

- Gabinete;
- Fiscalización, Jurídica y Estudios:
- Administración y Finanzas, Comunicaciones, Informática y Auditoria Interna.

b. Los archivos de trabajo deben ser administrados en los discos de red configurados en cada equipo, y conforme a las necesidades que se definan a nivel de jefatura.

Los archivos de carácter personal como música, fotografías o similares no deben 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 accede cada usuario de acuerdo a su perfil son:

Disco F:\

- Disco para mantener información de trabajo personal, al cual ningún otro usuario o administrador tendrá acceso. Se permitirá hasta 5 Gbytes por disco.

Disco R:\

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

Disco J:\

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

Disco Z:\

- Disco compartido por toda la institución, sin excepción, permite la mantención de directorios de las UO, existiendo la posibilidad de escribir o modificar archivos exclusivamente para los miembros de cada UO, pero con la alternativa de que sean leídos por los demás usuarios.

c. Respaldos

Los archivos de todos los discos son respaldados diariamente y, en caso de pérdida de información, debe ser solicitada al Jefe de la Unidad de Informática por medio de correo electrónico por la jefatura correspondiente indicando el archivo, motivo y fecha, para gestionar su recuperación. No se respaldará información desde los discos locales de cada estación de trabajo en forma periódica.

1.3 Seguridad e Instalación de Software

a. Los usuarios deberán velar por la integridad de los sistemas a los cuales tengan acceso, tanto a nivel local como externo. Cualquier violación o intento de violación de los citados sistemas será considerado como una falta de probidad.

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. Los usuarios no podrán instalar aplicaciones en forma directa sin previa notificación a su Jefatura directa y sin la autorización del Jefe de la Unidad de Informática. La autorización de instalación deberá considerar si está o no licenciada y si reviste algún riesgo de seguridad.

2 Uso de Sistemas de Apoyo a Procesos de Negocio y a Procesos Administrativos

a. La clave de acceso es personal e intransferible, y compromete la responsabilidad administrativa 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, es información que sólo debe ser comunicada y compartida por 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 acuerdo a lo estipulado en la Ley N° 19.628 sobre Protección de la Vida Privada.

g. Evite enviar cadenas de mensajes, promociones comerciales o mensajes repetitivos.

h. Los funcionarios deben evitar hacer uso de seudónimos u otros sistemas para ocultar su identidad desde la red de la Superintendencia. En todos los mensajes debe estar claramente identificado el origen del mensaje.

i. Evite hacer uso comercial de su dirección de correo electrónico institucional, ni enviar publicidad a otros usuarios con el correo electrónico de la Institución.

j. El uso de listados de correos electrónicos institucionales es para consulta y uso exclusivo dentro de la institución, razón por la cual está prohibido difundir este listado por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional. Recuerde que se encuentra vigente la Ley 19.628, sobre sobre Protección de la Vida Privada.

2 Correo SPAM

2.1 Instrucciones e Información

a. El "Phishing" es una forma de delito de estafa, 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 correo electrónico del tipo "Phishing" o descubre un sitio web fraudulento, infórmelo a la Unidad de Informática, siguiendo el procedimiento indicado en el numeral V.

b. La Unidad Informática bloqueará a nivel corporativo tanto la recepción de correo electrónico que se identifique como de tipo "phishing" en su sistema de correos corporativo, así como el acceder a sitios web fraudulentos y/o dañinos en los sistemas de control de navegación corporativa.

2.2 Recomendaciones

a. No abra el correo de tipo SPAM, los que por general tienen como propósito cadenas de distinto tipo o el ofrecimiento de productos o servicios en forma masiva. Vea las propiedades y envié dicha información al administrador de su red.

b. No responda un correo SPAM, los que por general tienen como propósito cadenas de distinto tipo o el ofrecimiento de productos o servicios en forma masiva, pues esto solamente servirá para confirmar que su cuenta de correo está activa.

c. No compre productos publicitados a través de correo electrónico no solicitado. Ignore las ofertas por muy atractivas que parezcan.

d. Las entidades financieras NUNCA le solicitarán datos personales mediante correo electrónico.

e. Siempre compare el link que aparece en el correo electrónico con el que finalmente ha sido dirigido. Contacte a la empresa emisora para verificar que el correo electrónico recibido es genuino. Contacte a la Unidad Informática ante la detección de un caso sospechoso de "Phishing".

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

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

IV. USO DE INTERNET

a. Se prohíbe el acceso 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.), lo que será apoyado por políticas incluidas en el acceso a Internet desde la Superintendencia.

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

c. Debido a la alta peligrosidad que representan para la institución en términos de seguridad de la información y el resguardo de su confidencialidad, así como la recarga que ello implica para el ancho de banda de la red del Estado, en desmedro de los restantes usuarios, se ha determinado prohibir el acceso desde las estaciones de trabajo de la Superintendencia a los sitios y servicios de comunicación externos que a continuación se detallan:

- Se bloqueará todo tipo de sitios con contenido multimedia como Metacafe, Dale al Play, Google Video, Radios y Canales de Televisión en general etc. Sin embargo, dado que en algunas instancias de la Superintendencia se requiere revisar videos disponibles en sitios como www.youtube.com, se permitirá el uso de contenido multimedia en Internet, para lo que se asignará una cuota máxima de minutos al día por funcionario, la que será definida por el Comité Directivo de la Superintendencia.

- 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, a excepción de la habilitación de reuniones por videoconferencia con propósitos laborales.

- Aplicaciones de transferencia de información de computador a computador 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 programas espías o que tengan propósito de realizar daño.

- No se permite el uso de redes sociales, entre las que están: MySpace, Flickr, Windows Live Spaces, las que poseen asociadas aplicaciones que permiten el intercambio de archivos y el uso de correos externos. Sin embargo, se mantendrá la opción de utilizar Twitter, dado que la SCJ posee una cuenta que administra Comunicaciones, así como el acceso a Facebook para lo que se asignará una cuota máxima de minutos al día por funcionario, para efectos de monitorear promociones de los casinos de juego y de eventuales casinos ilegales, la que será definido por el Comité Directivo de la Superintendencia.

- Se permite el uso de correos electrónicos distintos del institucional, para uso personal de los funcionarios, generándose un registro de su uso. Este registro, que se hará de manera automática por un sistema computacional, estará a cargo de la Unidad de Informática, sin intervención humana.

V. USO DEL CORREO ELECTRÓNICO

1 Uso del correo electrónico

1.1 Instrucciones e Información

a. El usuario debe mantener bajo reserva su clave de acceso a su cuenta en el servidor de e-mail, la que es 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 tomar su identidad.

c. La cuenta de correo electrónico requiere mantención del contenido de la misma por parte de los usuarios, atendida su capacidad limitada, por lo cual se podrá solicitar por parte de la Unidad de Informática, que cada usuario elimine correos que ya no sean utilizados. Se debe considerar, que en todo caso, estos correos eliminados estarán disponibles en el sistema de respaldo institucional.

d. Está prohibido al usuario enviar mensajes a otro usuario o grupo que no los quieran recibir, actuando como un emisor de correo de tipo Spam.

1.2 Recomendaciones

a. Evite emitir opiniones personales en foros de discusión u otras instancias de esa naturaleza con la cuenta de correo institucional.

b. El usuario deberá usar en sus mensajes con usuarios internos o externos, un lenguaje respetuoso y acorde a la calidad de funcionario público. No cumplen esta condición, los mensajes de contenido insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.

c. Tenga presente que la cuenta de correo electrónico institucional está destinada principalmente para su uso laboral; cualquier otro tipo de utilización, debe ser prioritariamente derivado a una instancia fuera de la organización (física y lógicamente), como por ejemplo el hogar. La información intercambiada por el correo electrónico institucional deberá usarse privilegiando los propósitos institucionales y la organización estará facultada para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su uso correcto sujeto a la ley vigente.

d. Evite dar su dirección de correo electrónico a menos que sepa quién lo usará.

e. Cada usuario deberá preocuparse de identificar la validez y propiedades de los correos electrónicos recibidos, consultando al personal de la Unidad de Informática en caso de dudas.

f. Evitar transmitir información confidencial o reservada por este medio a usuarios externos de la Superintendencia, dado que no está garantizada la confidencialidad de los textos enviados a INTERNET a menos que éstos sean encriptados.

g. Evite llenar formularios en mensajes correo electrónico que requieren información personal.

h. Evite 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, tales como virus, troyanos, botnet, spamvirus, etc. Además tiene prohibido difundir este tipo de contenidos a otros usuarios internos o externos. De igual manera, no deberá por ningún motivo abrir y/o ejecutar archivos que tengan doble extensión, somo por ejemplo, nombre_archivo.doc.exe, o que tengan la extensión .PIF, .LNK, .BAT, .EXE, .COM, .VBS, .SHS, .SCR., .VBE o .OCX, entre otros, toda vez que son extensiones peligrosas que pueden encubrir programas maliciosos.

VI. 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.

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.

El funcionario que se encuentre frente a cualquiera de estas dos situaciones, debe reportarlo de inmediato al Jefe de la Unidad Informática con copia a su jefe directo, por medio de correo electrónico en el que se incluyan todos los antecedentes, o telefónicamente, debiendo posteriormente formalizarlo por el correo institucional.

La Unidad de Informática, deberá tomar acciones rápidas de respuesta ante la situación, informando por escrito de las medidas adoptadas y sus efectos al Superintendente, con copia al funcionario y su Jefe directo. En caso que el incidente o amenaza constituyese un riesgo más allá de los sistemas y redes institucionales, la Unidad Informática deberá informarlo al Superintendente quien lo informará al CSIRT del Ministerio del Interior (CSIRT: Computer Security Incident Response Team), para proveer una respuesta común del Estado al riesgo detectado y reportado.

VII. VIGENCIA: La presente Circular entrará en vigencia a contar de su dictación.-

Anótese, comuníquese y archívese.

SUPERINTENDENCIA DE CASINOS DE

RENATO HAMEL MATURANA
SUPERINTENDENTE DE CASINOS DE JUEGO

MLC