Superintendencia del Sistema Financiero
San Salvador, El Salvador, C.A.

NORMAS PARA EL USO INTERNO DE LA INFORMACIÓN Y DE LOS RECURSOS INFORMÁTICOS EN LA SUPERINTENDENCIA DEL SISTEMA FINANCIERO

CAPÍTULO I
OBJETO Y SUJETOS

Objeto

Art. 1.- Las presentes normas tienen por objeto:

a) Dictar las reglas para el manejo, utilización de datos e información y para administrar los recursos de tecnología de información, propiedad de la Superintendencia del Sistema Financiero, en adelante denominada "la Superintendencia"; y

b) Establecer los lineamientos bajo los cuales el personal de la Institución debe utilizar los recursos informáticos para el desempeño de sus labores, así como las responsabilidades, obligaciones y derechos de los usuarios del equipo y aplicaciones.

Para los propósitos de este literal, se consideran como recursos informáticos el equipo de computación y sus accesorios, los impresores, los servidores de aplicaciones, el equipo de comunicación, los sistemas operativos, las bases de datos, el software de automatización de oficinas, el software de uso específico, los sistemas de información y los servicios de Internet y el correo electrónico.

Sujetos

Art. 2.- Los sujetos obligados al cumplimiento de las presentes normas son todos los empleados de la Superintendencia a quienes se les asignen recursos informáticos o que por la naturaleza de sus funciones utilicen datos e información de está Superintendencia.

Los recursos informáticos que utilizará el personal serán asignados por la Dirección de Informática a solicitud del Superintendente del Sistema Financiero, en adelante denominado "el Superintendente", de los Intendentes, de los Directores de Área y de los Jefes de Unidad, debiendo seguirse para ello el trámite establecido por la Dirección de Administración y Finanzas de la Superintendencia.

La Dirección de Informática de la Superintendencia velará por el cumplimiento de las presentes normas y le corresponderá orientar y brindar asistencia al personal en el buen uso de los recursos informáticos que se le asignen; también le corresponderá instalar y configurar los recursos informáticos de la Superintendencia y realizar el traslado y la conexión del equipo de computación, cuando cambie de ubicación, a solicitud de los Intendentes, Directores de Área o Jefes de Unidad.

CAPÍTULO II
OBLIGACIONES DEL PERSONAL

Obligaciones

Art. 3.- Sobre el uso y responsabilidad por los recursos informáticos:

a) Utilizar los recursos informáticos únicamente para realizar labores institucionales.

b) Los recursos informáticos de la Institución son de uso exclusivo de los empleados a quienes se le ha asignado los recursos.

c) Los usuarios se asegurarán de mantener en buen estado los recursos informáticos que utilicen.

d) Dar aviso oportuno al personal de la Dirección de Informática en caso de fallas o comportamientos anormales de los recursos informáticos;

e) Responder personalmente de las pérdidas y de daños ocasionados a las computadoras que se le hayan asignado.

f) Evitar el consumo de alimentos o bebidas cuando se esté utilizando el equipo asignado;

g) Usar correctamente los recursos informáticos asignados y evitar introducir elementos extraños en el teclado;

h) Guardar en el estuche correspondiente las computadoras portátiles asignadas a fin de protegerlas de golpes, debiendo utilizar el estuche para colocar en él únicamente los dispositivos propios de la computadora, tales como el cargador, unidades de discos removibles, conectores de red y cables. Abstenerse de sobrecargar el estuche con cualquier otro objeto que no sea de los antes mencionados;

i) Proteger las pantallas de las computadoras portátiles asignadas no poniendo carga sobre ellas, ni presionándolas con objetos punzantes;

j) No dejar la computadora portátil en lugares visibles o inseguros, cuando la transporten o la estén utilizando en la entidades en que los auditores se encuentren desempeñando sus funciones, a fin de evitar daños o hurto;

k) Utilizar los impresores láser a colores exclusivamente para imprimir presentaciones y correspondencia externa, mas no para correspondencia interna o borradores de trabajo;

l) Abstenerse de realizar múltiples impresiones de documentos en versión

preliminar, salvo los que se distribuyan en calidad de borrador a las entidades supervisadas, y en cualquier otro caso, si se necesita su distribución, debe utilizarse el correo electrónico interno o las carpetas compartidas que se han creado para tal fin en el servidor de archivos institucional.

m) Imprimir únicamente el original y fotocopiar los ejemplares necesarios en caso de requerirse la impresión de múltiples copias de documentos.

n) Los recursos informáticos serán operados, instalados y configurados, atendiendo las especificaciones del fabricante. Los usuarios seguirán las instrucciones que le sean dadas por la Dirección de informática, los manuales técnicos, así como la capacitación sobre los mismos.

CAPÍTULO III
MANTENIMIENTO

Mantenimiento del equipo

Art. 4.- Para el mantenimiento del equipo informático se deberán observar las siguientes normas:

a) La Dirección de Informática tendrá a su cargo el mantenimiento preventivo del equipo informático, para lo cual establecerá un calendario de diagnóstico y limpieza de cada equipo;

b) La referida Dirección, a través del Departamento de Soporte Técnico, notificará las fechas del servicio de mantenimiento a las Intendencias, Direcciones y Jefaturas de la Superintendencia para que avisen al personal, particularmente al destacado fuera de la Institución, que deben poner a disposición del Departamento de Soporte Técnico sus computadoras, de escritorio o portátiles en su caso, para facilitar el servicio de mantenimiento;

c) Al recibirse una computadora, la Dirección de Informática revisará su estado y el de sus componentes, lo cual quedará registrado en los controles respectivos. En caso de que el equipo presente problemas o faltantes se procederá conforme a lo descrito en el artículo 17 de estas normas.

CAPÍTULO IV
CLASIFICACIÓN DE SOFTWARE Y AUDITORÍAS

Clasificación

Art. 5.- El software institucional, instalado en las computadoras portátiles y de escritorio, estará clasificado de la siguiente forma:

a) Software estándar: es el software instalado en todas las computadoras de escritorio y portátiles, el cual incluye sistema operativo, antivirus y programas

de automatización de oficina, éstos son detallados en una carta - compromiso con nombres y versiones, que se entregará a cada usuario para su firma y de la cual la Dirección de Informática guardará copia; y

b) Software y aplicaciones de uso específico: es el software particular instalado de acuerdo a las necesidades de cada usuario, cuyo detalle también se indicará en una carta - compromiso a entregarse a cada usuario y de la cual la Dirección de Informática guardará copia firmada por el usuario.

Auditorías

Art. 6.- Para asegurar que el software instalado en los equipos de la institución esté cubiertos por las licencias adquiridas, se realizarán auditorias periódicas, para lo cual la Dirección de Informática seguirá el siguiente procedimiento:

a) Cada usuario firmará anualmente una carta-compromiso en la cual se detallará el software instalado en la computadora asignada a él, de conformidad con la clasificación citada en el artículo 5 anterior, para evitar problemas legales al usuario y a la Superintendencia.

Se prohíbe al usuario la instalación de otro software en adición al autorizado, por lo que las consecuencias que se generen por violar la Ley de Fomento y Protección a la Propiedad Intelectual será de su exclusiva responsabilidad;

b) La Dirección de Informática periódicamente realizará auditorías de software en las cuales revisará la declaración firmada por los usuarios y el software instalado en las computadoras, a fin de constatar que el software existente en ellas es el originalmente autorizado;

c) Si la Dirección de Informática encontrare software no autorizado en las computadoras asignadas a los usuarios, se desinstalará de inmediato y se procederá conforme a lo descrito en el artículo 16 de estas normas.

CAPÍTULO V
CORREO ELECTRÓNICO

Correo Electrónico

Art. 7.- El personal podrá utilizar el correo electrónico sujeto a las siguientes reglas:

a) Todo correo electrónico enviado institucionalmente se considera una remisión oficial y tendrá la misma validez que el envío tradicional en papel, excepto aquellos documentos especiales que requieran tener la firma y sello correspondiente; de igual forma, la confirmación de lectura de los mensajes de correo electrónico, tendrá la misma validez que el acuse de recibo de los documentos impresos; en consecuencia, todos los usuarios institucionales

tienen que mantener habilitada esta opción a fin de verificarse la recepción del mensaje;

b) El correo electrónico deberá ser utilizado para propósitos estrictamente institucionales, de intercambio de información técnica o de cualquier otra información necesaria para el eficiente desempeño de las funciones de las distintas unidades de la Superintendencia. Es deber de cada empleado utilizar el sistema de correo electrónico de forma responsable, profesional, legal y ética;

c) Los buzones de los usuarios, que se encuentran en el servidor de correos electrónicos, tendrán en línea información de tres meses de antigüedad, por lo que el usuario deberá trasladar a sus carpetas personales la información que le interese conservar después de aquel período; la información cuya antigüedad sea mayor a tres meses será eliminada de los buzones;

d) La divulgación de avisos institucionales, actividades culturales, deportivas o sociales será comunicada a través del correo electrónico únicamente por la Dirección de Comunicaciones, la Dirección de Administración y Finanzas a través de sus Departamentos y los Comités respectivos. En el caso específico de alertas de seguridad informática o suspensión de servicios informáticos, será únicamente la Dirección de Informática la autorizada a enviar estos correos;

e) El correo electrónico no deberá utilizarse para usos personales como en el caso de solicitudes, comentarios o cualquier otro tipo de información no institucional;

f) Deberá abstenerse de abrir aquellos correos electrónicos cuya procedencia sea sospechosa, los cuales deberán ser eliminados inmediatamente para evitar ser infectados de virus computacionales. De igual forma deberán ser eliminados aquellos correos no solicitados, aún cuando provengan de fuentes conocidas o aquellos cuyas características concuerden con las reportadas en las alertas enviadas por seguridad informática;

g) Deberá abstenerse de participar y divulgar “cadenas de correo electrónico”;

h) Abstenerse de activar las opciones de vista previa y notificación automática en el menú del correo electrónico, ya que éstas abren el contenido del correo y provoca la activación de virus;

i) El software que provea la Institución para correo electrónico será el autorizado para tal fin;

j) Abstenerse de utilizar la dirección electrónica institucional como referencia en suscripciones de carácter personal;

k) Una dirección del correo electrónico en Internet puede conducir al recibo de correos no solicitados con contenido molesto u ofensivo. El recibo de esta información deberá notificarse al encargado de Seguridad Informática;

l) Los empleados son responsables por sus cuentas de correo y de los mensajes enviados desde su cuenta;

m) Abstenerse de enviar correos a través de cuentas ajenas, tampoco permitir que alguien envíe correos electrónicos utilizando su cuenta;

n) Abstenerse de discutir entre dos o más usuarios a través del correo electrónico;

o) La información de carácter confidencial enviada a través de correo electrónico deberá ser protegida por algún medio que asegure la confidencialidad de la información transmitida, para lo cual personal de la Dirección de Informática brindará el soporte necesario;

p) Abstenerse de enviar a través de correo electrónico material fraudulento, político, amenazante, pornográfico, intimidante, difamatorio, de alguna manera ilegal o inapropiado; este material tampoco se debe almacenar en los buzones de correo electrónico. Los empleados que encuentren o que reciban esta clase material deben dar a conocer el incidente a Seguridad Informática; y,

q) Toda comunicación electrónica recibida de forma repetitiva e indeseada puede ser considerada acoso. La comunicación dirigida a una persona para acosarla o amenazarla esta prohibida. En el caso de recibir comunicación de este tipo, deberá reportarse a Seguridad Informática.

CAPÍTULO VI
USO DE LA NAVEGACIÓN EN LA RED PÚBLICA INTERNET

Navegación en Internet

Art. 8.- El personal de la Superintendencia debe utilizar la navegación en la red pública Internet como una herramienta que contribuya al desempeño de sus labores, con las responsabilidades, restricciones, obligaciones y derechos de los usuarios de este servicio:

a) El acceso a la navegación en Internet y al correo electrónico externo se proporcionará a aquellos usuarios para quienes los Intendentes, Directores de Área o Jefes de Unidad les autoricen;

b) Para el acceso a Internet, todo usuario deberá autenticarse, utilizando usuario y contraseña;

c) No se permite hacer modificaciones a la configuración del navegador realizada por la Dirección de Informática;

Art. 9.- En la navegación en Internet queda prohibido el acceso a los sitios relacionados con los siguientes temas:

a) Crimen, violencia y armas;

b) Uso de estupefacientes;

c) Entretenimientos y juegos;

d) Música, video y cine;

e) Juegos de apuestas;

f) Charlas interactivas (chats) exceptuando aquellas que por su carácter técnico sean necesarias para las labores de la institución;

g) Ciencias ocultas y astrología;

h) Sexualidad, pornografía;

i) Sitios de hackers; y

j) Servidores de correo no institucionales

CAPÍTULO VII
INTRANET

Art. 10.- La Dirección de Comunicaciones, definirá el contenido y mantenimiento de la Intranet Institucional, y se atenderán al menos los siguientes aspectos:

a) Las páginas que sean propuestas por miembros de la Institución deberán tener el nombre del patrocinador y será responsabilidad de éste el contenido de la misma;

b) Abstenerse de publicar asuntos de carácter privado o sensitivo, promoción de la venta de bienes o servicios a menos que sea una actividad de la Superintendencia, promoción del uso de violencia hacia grupos o individuos debido a su afiliación o pertenencia a un grupo (raza, política, étnico, género, credo, orientación sexual, edad o clase económica); y

c) Abstenerse de colocar propaganda a favor o en contra de las Instituciones fiscalizadas ni de ninguna otra institución.

d) La Dirección de Comunicaciones será la responsable de administrar la página principal del portal institucional y que los contenidos cumplan con las reglas generales del manejo de información, definidos en estas políticas;

e) La creación de usuarios y áreas de trabajo dentro del portal será creada por la Dirección de Informática;

f) Dentro de cada área creada se asignará un administrador, el cual será responsable de administrar el contenido allí publicado;

g) Los administradores de área del portal podrán solicitar a la Dirección de Informática la creación de dos roles de usuarios para implementar un esquema de publicación en dos pasos, definiéndose dos perfiles: el redactor, responsable de escribir los contenidos de la información a publicar; y el supervisor (ó publicador), responsable de revisar, aprobar y publicar el contenido;

h) El administrador del área será el responsable por la creación y mantenimiento de vínculos a sitios, acceso a otros servicios Web u otros sitios que se construyan para ser integrados al portal;

i) El administrador del área deberá asegurarse de identificar quienes serán los receptores o destinatarios de la información con el propósito de que el contenido de ésta sea conocido únicamente por las personas correctas y establecerles el correspondiente acceso;

j) Si algún usuario requiere acceso a información de la cual no es destinatario, deberá solicitar al responsable del área específica su acceso con la correspondiente justificación.

CAPÍTULO VIII
SEGURIDAD Y CONTROL DE LA INFORMACIÓN

Confidencialidad

Art. 11.- De conformidad con la Ley Orgánica de la SSF y con los contratos individuales de trabajo suscritos entre la Institución y el personal, la información que se recaba tiene carácter confidencial.

Para los efectos de estas Normas se entenderá por información confidencial, toda aquella almacenada en medios electrónicos, impresa, transmitida por medio de correo electrónico o por cualquier otro medio electrónico, presentaciones y cualquier otra generada o recabada institucionalmente.

Regulaciones Aplicables

Art. 12.- La confidencialidad informática estará sujeta a las siguientes reglas:

a) Existirá una carpeta dentro del servidor de archivos que contendrá únicamente las siguientes clases de datos: leyes, normativa y reglamentos; manuales, instructivos y otros similares, por lo que los usuarios de las mismas, que tengan derecho de escritura no deberán colocar información distinta a la mencionada;

b) Ningún usuario está autorizado para extraer información de las bases de datos, de los envíos de datos de las entidades fiscalizadas, de los resultados de reportes de los sistemas de información internos, de los estudios o cualquier otra información propiedad de la Superintendencia para usos y divulgación externa en algún medio;

c) La Superintendencia es propietaria de la información resultante de auditorías, investigaciones, informes o trabajos encomendados a su personal, por lo que, los usuarios deberán actualizar el servidor de archivos con la información del trabajo realizado en la carpeta asignada para tal fin y con la periodicidad establecida por el jefe inmediato. La Dirección de Informática revisará las actualizaciones de estas carpetas e informará a las Intendencias sobre la periodicidad de las actualizaciones para su respectivo seguimiento;

d) La creación de usuarios de red, de correo interno, de correo externo, de navegación en Internet, de acceso a sistemas de información, de carpetas y de base de datos será solicitada a la Dirección de Informática mediante el formulario que deberá ser autorizado por los Intendentes, Directores de Área o Jefes de Unidad, en los que se detallará la información a la que se solicita tener acceso;

e) Las solicitudes de acceso a los sistemas de información puestos a disposición de las entidades fiscalizadas serán canalizadas a través de la Intendencia de Supervisión o del Departamento que ésta designe;

f) Es responsabilidad de cada usuario que maneja información Institucional asegurarse de mantener la confidencialidad de los datos contenidos en sus computadoras, en cumplimiento a los artículos 26 y 36 de la Ley Orgánica de la Superintendencia, de manera que éstos no sean copiados o leídos por personas ajenas a sus labores, pertenezcan o no a la Institución;

g) La información contenida en los sistemas de información y los recursos informáticos podrá ser utilizada solamente en actividades propias de la Superintendencia; y

h) Cada usuario es responsable por la conservación permanente del respaldo de la información que se encuentre en su computadora.

CAPÍTULO IX
PRÁCTICAS INDEBIDAS

Prácticas indebidas

Art. 13.- En los sistemas informáticos de la Superintendencia se consideran faltas sujetas a sanción las siguientes prácticas:

a) Instalar software diferente del autorizado por la Dirección de Informática;

b) Eliminar o desinstalar software instalado y configurado por la Dirección de Informática;

c) Descargar programas o archivos de Internet, música, protectores de pantalla, videos y otros elementos sin autorización de la Dirección de Informática;

d) Instalar o mantener en la computadora cualquier archivo que no sea producto del trabajo o necesario para el trabajo, o que sea antiestético u ofensivo para personas o instituciones;

e) Instalar o mantener en su computadora cualquier archivo relacionado con los temas mencionados en los sitios no permitidos, a que alude el artículo 9 de las presentes normas;

f) Copiar al disco duro archivos de trabajo provenientes de equipo ajeno a la Superintendencia sin antes verificarlos contra virus;

g) Realizar actividades que puedan incurrir en daño, deterioro, pérdida o degradación de los recursos informáticos que provee la Institución;

h) Inhabilitar el programa antivirus o cambiar su configuración;

i) Cancelar o desactivar la verificación automática de antivirus, que se ejecuta todos los días;

j) Instalar cualquier tipo de programa que venga adjunto en los correos electrónicos;

k) Hacer uso de los recursos informáticos para actividades que no están relacionadas con el trabajo;

l) Modificar las configuraciones de los recursos informáticos;

m) Dejar funcionando la computadora o el impresor después de finalizadas las labores del día;

n) Instalar programas o permitir que terceros instalen programas en la computadora asignada;

o) Retirar sin autorización manuales, software o libros propiedad de la Superintendencia, que están bajo la custodia de la Dirección de Informática;

p) Cambiar de ubicación el equipo de computación;

q) Fumar en lugares en donde se encuentre equipo de cómputo;

r) Extraer, tomar o intercambiar partes o componentes de los recursos informáticos propiedad de la Superintendencia;

s) Divulgar a terceros la información correspondiente a la configuración de las estaciones de trabajo;

t) Acceder con la cuenta de usuario desde otro equipo que no sea el asignado originalmente; y

u) Acceder a la red de datos, con equipo de cómputo que no pertenezca a la Institución.

CAPÍTULO X
POLÍTICAS DE CONTROL DE ACCESO

Control de acceso

Art. 14.- Para la creación de contraseñas de acceso a los sistemas, el personal de la Superintendencia deberá tomar en cuenta:

a) Las contraseñas creadas por los usuarios tendrán al menos 10 caracteres;

b) Las contraseñas de usuario deben ser difíciles de descubrir. No deberá usar: palabras de diccionario, derivaciones de la identidad del usuario, secuencia de caracteres comunes tales como "123456" , detalles o información personal, parte de cualquier discurso institucional, nombres propios, localizaciones geográficas, siglas comunes, dialectos del ambiente o lenguaje coloquial;

c) No deberán construirse contraseñas compuestas de un cierto número de caracteres, en las que solamente uno o varios caracteres dentro de la misma clave se sustituyen por otros que previsible y continuamente están intercambiando;

d) No deberá construir contraseñas que son idénticas a contraseñas previamente empleadas;

e) Las contraseñas seleccionadas por los usuarios, dentro de la longitud mínima permitida, contendrá al menos un carácter alfabético y al menos uno no alfabético. Los caracteres no alfabéticos o numéricos incluyen números (0-9) y puntuaciones. No deberá utilizarse caracteres de control u otros caracteres que no pueden imprimirse. Además, Todas las contraseñas seleccionadas por los usuarios, contendrán al menos un carácter en letra mayúscula o minúscula;

f) Las contraseñas seleccionadas por los usuarios deben ser pronunciables, de tal forma que se pueda recordar con facilidad y no necesite escribirla;

g) No se almacenarán contraseñas en forma legible en archivos, scripts de conexión automática, macros, teclas de función de terminales, o en computadores sin algún control de acceso;

h) Toda contraseña deberá ser cambiada de forma inmediata si se sospecha que la misma ha sido descubierta;

i) Las contraseñas no serán escritas en lugares accesibles donde personas no autorizadas puedan acceder a ellas;

j) El uso de la clave de acceso es exclusivo y de total responsabilidad del usuario, por ningún motivo, debe divulgar su contraseña de red a nadie. Al conocer que un usuario abandonará la institución, el jefe superior inmediato deberá solicitar a la Dirección de Informática la eliminación del usuario y la re asignación de roles a quien corresponda;

k) Los usuarios son responsables de todas aquellas actividades ejecutadas con su código de usuario(User-ID) personal, por lo que no deberá permitir a otros ejecutar cualquier actividad con su User-ID. También está prohibido ejecutar cualquier actividad con User-ID perteneciente a otro usuario;

l) Las contraseñas no se comunicarán a través de líneas telefónicas. Para la entrega y recepción de una nueva o cambio de contraseña, el usuario se presentará a la Dirección de Informática con el carné de identificación de la Superintendencia, dejando registro en los controles de esa Dirección, de la fecha y hora de recepción de la asignación;

m) Las estaciones de trabajo o computadoras personales, no deberán ser desatendidas, sin antes salirse de su aplicativo o sesión y bloquear su estación de trabajo manualmente; y

n) Al retirarse de la institución de forma definitiva o ausentarse de forma temporal por vacaciones, incapacidades o alguna otra circunstancia, el jefe inmediato deberá comunicar oportunamente a la Dirección Informática para reasignar los roles al nuevo usuario responsable.

CAPÍTULO XI
SOBRE EL MANEJO DE LA INFORMACIÓN

Trabajo fuera de la Superintendencia

Art. 15.- El personal que se encuentra destacado en las instituciones fiscalizadas,

deberá cumplir las siguientes practicas:

a) No utilizar los recursos informáticos de las instituciones fiscalizadas para realizar trabajos de Supervisión;

b) No dejar documentos impresos desatendidos, para evitar que sean tomados por personas no autorizadas;

c) Acceder a la Red Pública Internet a través de las computadoras portátiles de la Superintendencia, siempre y cuando la institución provea una línea telefónica fija, la navegación nunca se hará desde la red interna de la institución; y

d) La recepción y envío de correos electrónicos será a través del acceso privado que se ha creado para tal fin. Nunca a través de una cuenta de la institución fiscalizada.

CAPÍTULO XII
SANCIONES

Régimen disciplinario

Art. 16.- El personal que incumpla cualquiera de estas Normas estará sujeto a la imposición de la sanción que corresponda, según el título séptimo “Disposiciones Disciplinarias y Modo de Aplicarlas” del Reglamento Interno de Trabajo de esta Superintendencia. La Dirección de Informática informará de la falta cometida al jefe superior inmediato del usuario y al Departamento de Recursos Humanos. El jefe superior inmediato deberá proceder según el título antes citado, e informar por escrito a la Dirección de Informática y al Departamento de Recursos Humanos de la aplicación de la sanción correspondiente.

Costos

Art. 17.- En los casos de desperfectos en los recursos informáticos el usuario deberá informar de inmediato a la Dirección de Informática, quien enviará el bien a dictamen técnico, si de acuerdo al dictamen la causa del desperfecto es debido a descuido, negligencia o dolo del usuario, el costo de reparación y/o deducible del seguro del bien no cubierto por la Sociedad de Seguros, será trasladado al usuario que tiene asignado el bien al momento del evento, a quien además se le trasladará el costo de los honorarios que cobre la empresa que realice el dictamen técnico aludido.

Robo o hurto por negligencia

Art. 18.- En caso de robo o hurto de los recursos informáticos, el usuario deberá informar de inmediato a la Dirección de Administración y Finanzas del hecho y deberá presentar el parte policial. Si este hecho se dio por negligencia del usuario, el personal que tenga asignado los bienes al momento del evento deberá cancelar el valor de reposición de los mismos.

.

CAPITULO XIII
SISTEMAS DE INFORMACION

Sistemas de Información

Art.19. Los sistemas de información a la medida o software de uso específico, requerido por alguna área dentro de la institución para apoyo a sus funciones, deberá ser solicitada a la Dirección de Informática cuando se esté elaborando el presupuesto institucional. La solicitud debe ser realizada por los Intendentes o Directores de Área y debe contener al menos:

a) Identificación del Objetivo Estratégico al que estará contribuyendo su implantación;

b) Usuario responsable de definir requerimientos, en caso de ser sistema de información de desarrollo a la medida;

c) Usuario responsable de definir características técnicas, la configuración y parámetros o fórmulas para el funcionamiento, en caso de ser software de uso específico;

d) Usuarios responsables de la implantación y aceptación del sistema o software de uso específico;

e) Beneficios que brindará la implantación del sistema o software;

f) Usuario(s) final(es) del sistema o software;

g) Fechas inicial y final para la implantación de la solución;

h) Presupuesto estimado de la inversión, en caso de ser software de uso específico;

i) Identificación de posibles proveedores.

CAPÍTULO XIX
DISPOSICIONES FINALES

Glosario

Art. 20.- En anexo se presenta el glosario de los términos técnicos utilizados en estas normas, para mayor comprensión.

Casos no previstos

Art. 21.- Lo no previsto en las presentes Normas será resuelto por el Consejo Directivo de la Superintendencia.

Derogatoria

Art. 22.- Deróganse las NORMAS PARA EL USO DE LA INFORMACIÓN Y DE LOS RECURSOS INFORMÁTICOS EN LA SUPERINTENDENCIA DEL SISTEMA FINANCIERO que fueron aprobadas por el Consejo Directivo en sesión No. CD-39/01 de fecha 02 de agosto de 2001.

Vigencia

Art. 23.- Las presentes Normas entrarán en vigencia a partir del uno de julio de dos mil cuatro."

El acta que contiene el punto transcrito fue aprobada en sesión No. CD-22/04 de fecha 9 de junio de 2004.

Modificaciones

Estas normas fueron modificadas en sesión No. CD-03/07 de fechas 18 de enero de 2007.

CAZ/gv

Superintendencia del Sistema Financiero

CIRCULAR

PARA: ***Para todo el personal.***

ASUNTO: ***Políticas complementarias a las "Normas para el uso interno de la información y de los recursos informáticos en la Superintendencia del Sistema Financiero".***

Se les recuerda el cumplimiento a las "Normas para el uso interno de la información y de los recursos informáticos en la Superintendencia del Sistema Financiero", por lo cual, considerando los términos tecnológicos y buenas prácticas en el área de informática y uso de la información, se comunica lo siguiente:

1. *Entre los sujetos obligados al cumplimiento de las citadas Normas se encuentra el personal externo que, previa autorización de Superintendentes, Intendentes o Directores de Área, se encuentren realizando trabajos o consultorías para la Superintendencia y que utilicen algún recurso informático provisto por esta Institución.*

2. *Respecto a las obligaciones en el uso y responsabilidad de los recursos informáticos enumeradas en el Art. 3 de las Normas aludidas, se incluye lo siguiente:* ***i)*** *Utilizar las características de control de cambios para la revisión de documentos, así como el uso de correo electrónico, carpetas compartidas, el portal institucional o la aplicación de digitalización de documentos para la distribución de documentos, a fin de economizar el uso de papel y tinta; y* ***ii)*** *Utilizar el cable de seguridad para los equipos portátiles, dentro y fuera de la institución, siempre que sea posible.*

3. *Con el fin de optimizar el espacio en el servidor de archivos, la Dirección de Informática revisará periódicamente el contenido del mismo y procederá a eliminar cualquier archivo relacionado con los temas mencionados en los sitios no permitidos según los Arts. 9 y 13 de las Normas.*

4. *En cuanto a las reglas de confidencialidad establecidas en el Art. 12 de las citadas Normas, éstas abarcan lo siguiente:* ***i)*** *En caso de pérdida o revelación de información confidencial a personas no autorizadas o que existan sospechas de estas acciones, se deberá notificar inmediatamente al Jefe Inmediato y a la Dirección de Informática; y* ***ii)*** *Toda información sensible o confidencial que se desee eliminar, deberá ser sometida a un proceso de destrucción que impida su recuperación.*

5. *Con respecto a los sitios que según el Art. 9 que no deben ser visitados utilizando el servicio de Internet provisto por la Superintendencia, se incluyen los relativos a:* ***i)*** *Religión;* ***ii)*** *Blogs no relacionados al trabajo desempeñado en la Institución; y* ***iii)*** *Redes sociales, exceptuando los accesos autorizados por la Dirección de Informática.*

6. *Dentro de las faltas sujetas a sanción contenidas en el Art. 13, se abarca:* ***i)*** *La navegación en Internet por medio de módems u otros dispositivos de comunicación mientras se está conectado a la red institucional;* ***ii)*** *Configurar el acceso al correo institucional por medio de dispositivos móviles sin previa autorización;* ***iii)*** *Conectarse a redes inalámbricas inseguras desde los equipos propiedad de la Superintendencia; y* ***iv)*** *Hacer uso de técnicas de hackeo.*

7. *Cuando un empleado deje de laborar para la Superintendencia, el Departamento de Gestión Humana y Organizacional deberá notificar inmediatamente tal situación a la Dirección de Informática para que esta última deshabilite las credenciales del usuario en los sistemas de información.*

8. *Por último, se aclara que cuando las Normas mencionan la Ley Orgánica de la Superintendencia del Sistema Financiero, la Dirección de Administración y Finanzas y la Dirección de Comunicaciones, se refiere a la Ley de Supervisión y Regulación del Sistema Financiero, Dirección de Administración y a la Unidad de Comunicaciones y Relaciones Institucionales, respectivamente.*

Las anteriores políticas son complementarias en la aplicación de las "Normas para el uso interno de la información y de los recursos informáticos en la Superintendencia del Sistema Financiero" aprobadas por el Consejo Directivo de la anterior Superintendencia del Sistema Financiero en sesión No. CD-22/04 de fecha 09 de junio de 2004 y modificadas en sesión No. CD-03/07 de fecha 18 de enero de 2007, por lo que se considerarán incorporadas a las mismas.

Por lo tanto, les solicitamos dar estricto cumplimiento a las mismas bajo pena de informar al Departamento de Gestión Humana y Organizacional por incurrir en lo establecido en el Art. 73 literal h) del Reglamento Interno de Trabajo.

San Salvador, mayo de 2013.

SUPERINTENDENCIA DEL SISTEMA FINANCIERO El Salvador, C.A.

Víctor Antonio Ramírez Najarro
Superintendente

Antecedentes: Memorándum No. SG-134/2012; LF-001440.