GOBIERNO DE LA REPÚBLICA DE GUATEMALA
SENABED

SECRETARIA NACIONAL DE ADMINISTRACION DE BIENES EN EXTINCION DE DOMINIO
Sección de Organización y Métodos
Guatemala, C.A.

Secretaría Nacional de Administración de Bienes en Extinción de Dominio
-SENABED-
Dirección de Informática y Estadística | Departamento de Informática

Manual de Políticas y Estándares de Seguridad Informática Relacionadas al uso del Sistema y Equipo

Guatemala, octubre 2016.

GOBIERNO DE LA REPÚBLICA DE
GUATEMALA

Secretaría Nacional de Administración de Bienes en Extinción de Dominio

Secretaría General

SECRETARIA NACIONAL DE ADMINISTRACION DE BIENES EN EXTINCION DE DOMINIO
Seccion de Organización y Métodos
Guatemala, C.A.

RESOLUCIÓN DE SECRETARÍA GENERAL

NO. SENABED/SG 100-2016

Guatemala, 12 de Noviembre de 2016

CONSIDERANDO:

Que por mandato legal el Secretario General, es el responsable del buen funcionamiento de la Secretaria Nacional de Administración de Bienes en Extinción de Dominio y que el Reglamento de la Ley de Extinción de Dominio lo faculta para colaborar, apoyar y ejecutar las decisiones y políticas que emanen del CONABED, en materia de administración de bienes objetos de la acción de extinción de dominio o declarados extintos de dominio.

CONSIDERANDO:

Que por mandato legal el Secretario General es el encargado de planificar, organizar, dirigir y controlar las funciones técnicas y administrativas de la SENABED, y organizar las dependencias de la SENABED, proponiendo al CONABED las modificaciones que considere pertinente.

POR TANTO:

Con fundamento en el artículos 38 de la Ley de Extinción de Dominio, Decreto Número 55-2010 del ngreso de la República de Guatemala y el artículo 21 incisos b) y e) del Acuerdo Gubernativo 514-2011.

RESUELVE:

Artículo 1°: Autorizar la implementación y socialización a la Dirección de Informática y Estadística de la Secretaría Nacional de Administración de Bienes en Extinción de Dominio de: **EL MANUAL TÉCNICO DE USUARIO SISAB: MÓDULO DE REGISTRO JURÍDICO, MANUAL TÉCNICO DE USUARIO SISAB: MÓDULO DE CONTROL Y REGISTRO, MANUAL TÉCNICO DE USUARIO SISAB: MÓDULO DE ADMINISTRACIÓN DE BIENES Y MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA RELACIONADAS AL USO DEL SISTEMA Y EQUIPO.**

Artículo 2°: Que se envíe copia de los Manuales a la Dirección de Informática y Estadística de la Secretaría Nacional de Administración de Bienes en Extinción de Dominio, indicados en el artículo uno de la presente resolución.

Comuníquese

Lic. Oscar Humberto Conde López
Secretario General

SECRETARIA NACIONAL DE ADMINISTRACION DE BIENES EN EXTINCION DE DOMINIO
SECRETARIA GENERAL
Guatemala, C.A.

Índice

1. Introducción

La utilización del equipo de cómputo se ha convertido en una necesidad latente en todas las entidades estatales, convirtiéndose en una herramienta fundamental de trabajo para todas las dependencias que integran la Secretaría Nacional de Administración de Bienes en Extinción de Dominio no es la excepción a la anterior afirmación.

La tecnología de la información (TI) contribuye a superar los niveles de productividad y eficiencia de la Institución, siendo la Dirección de Informática y Estadística, la encargada de proveer los servicios necesarios para brindar al usuario el máximo apoyo en cuanto a sistematización, mecanismos de consulta y solución de problemas computacionales. Para ello es necesario que el usuario conozca las políticas y normas establecidas por la Dirección de Informática y Estadística, las cuales deben ser definidas clara y explícitamente para poder administrar los recursos de TI de forma eficiente o en su momento poder deducir responsabilidades.

Para cumplir con esta responsabilidad se ha desarrollado una serie de lineamientos aplicables a cada área informática de la Dirección segmentándolas de la siguiente manera:

a) Políticas de utilización de Hardware y Software
b) Políticas de Utilización del Servicio de Internet
c) Políticas de Utilización de Correo Electrónico
d) Políticas de Resguardo de Información

Cada una de las anteriores políticas contiene los lineamientos y las sanciones por los cuales los colaboradores de la SENABED deberán guiarse para hacer que la utilización de los equipos, así como de los servicios electrónicos de los que dispone la secretaría sean eficientes para cumplir con los objetivos de la secretaría.

2. Objetivos

2.1. Generales

Resguardar la información institucional relevante, con el objeto de asegurar la continuidad operacional de los procesos y servicios que desarrolla SENABED.

2.2. Específicos

a) Establecer políticas, normativas y procedimientos que permitan resguardar y proteger los activos de información de SENABED.

b) Definir un Plan de Difusión que permita difundir las buenas practicas asociadas a la seguridad de la información.

c) Controlar y prevenir los riesgos de seguridad de la información, identificando las vulnerabilidades y amenazas que enfrenta.

3. Principios

a) Promover una cultura orientada a la seguridad de la información.

b) Involucrar a los directores y jefes de unidades en la correcta difusión, consolidación y cumplimiento de las políticas.

c) Mantener las políticas, normativas y procedimientos actualizados, con el fin de asegurar su vigencia y nivel de eficiencia.

4. Alcances

a) Todas las políticas de utilización de recursos tecnológicos establecidas deberán ser conocidas y cumplidas por todo el personal de la Secretaría sin excepción del renglón presupuestario al que pertenezcan.

b) Las políticas se aplicarán en todo el ámbito de la Secretaría, a sus recursos y a la totalidad de los procesos, internos y externos.

5. Cumplimiento de las Políticas

a) Los encargados de las Unidades de Trabajo y/o Direcciones, velaran por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

b) La DIE, realizará revisiones periódicas de todas las áreas de SENABED a efecto de garantizar el cumplimiento de las políticas, normas y procedimientos de seguridad.

6. Sanciones Previstas por Incumplimiento

a) El incumplimiento de las disposiciones establecidas por las Políticas de Utilización de Recursos Electrónicos que causen perjuicio a otros usuarios, a la seguridad o integridad de los sistemas tendrá como resultado la aplicación de diversas sanciones, por lo cual la DIE pondrá en conocimiento de las autoridades de la SENABED el hecho para adoptar las medidas disciplinarias o administrativas adecuadas conforme a la magnitud y característica del aspecto no cumplido, según el Reglamento Interno de Trabajo de la SENABED.

b) Cada una de las políticas cuenta con su respectiva área de sanciones las cuáles serán aplicadas en los casos que sean necesarios velando por la integridad de la información de la entidad.

7. Política de Utilización de Hardware y Software

7.1. Objetivos

El objetivo de estas normas es entregar las reglas adecuadas que permitan lograr un trabajo más seguro y eficiente, facilitando tanto las tareas del usuario, como las del personal de soporte de informática, aumentando así la productividad de ambos.

Estas normas deben ser conocidas y respetadas por los empleados presupuestados y personal por contrato. La violación de alguna de ellas puede acarrear consecuencias

graves para el usuario, por tanto, el usuario será responsable de conocer y respetar estas normas, así como de las consecuencias que deriven del no cumplimiento de las presentes normas.

7.2. Cambio de Ubicación Física del Equipo

Cambio de puesto o atribuciones (Esto hace variar los accesos a sistemas, así como los perfiles de acceso).

Será responsabilidad de la Dirección de Informática y Estadística, informar de los cambios, al encargado de Inventarios de la Institución, quien a su vez será responsable de la actualización de las tarjetas de responsabilidad correspondientes.

Es responsabilidad de la Dirección de Informática y Estadística, velar por el buen funcionamiento de los servicios que se presten dentro de la secretaría; así como, brindar a los usuarios el soporte técnico necesario.

7.3. Políticas Generales en la Utilización de Hardware y Software

El usuario que recibe cualquier hardware y/o software necesario para el desempeño de sus funciones, es el único responsable del mismo.

a) El hardware y el software se entregará debidamente configurado al personal.
b) Utilizar el software existente para cumplir con las funciones definidas al puesto, de ser necesario algún software adicional deberá solicitarse a la Dirección de Informática y Estadística y Estadística para determinar si es posible la instalación del mismo.
c) Todo cambio de accesorios debe ser llevado a cabo por personal que la DIE autorice o designe.
d) Todas las computadoras que la DIE instale deberán tener habilitado solamente el dispositivo USB para el mouse y el teclado. Los demás puertos USB se tendrán que deshabilitar, se recomienda el uso de carpetas compartidas para reemplazar el almacenamiento en dispositivos USB externos.

Es total responsabilidad y obligación del usuario lo siguiente:

a) Dar cumplimiento a todas las normas y políticas vigentes.
b) Preservar el estado de los equipos, manuales y cualquier otro elemento de soporte que se le entregue.
c) Utilizar adecuadamente el software que se le ha autorizado e instalado.
d) Preservar la veracidad de los datos en los sistemas a que se le dé acceso.
e) Informar a la Dirección de Informática y Estadística, cualquier cambio relacionado al hardware y/o software
f) Los usuarios deberán cuidar física y lógicamente los recursos computacionales existentes, pensando que estos están al servicio de todos.
g) El usuario deberá mantener los archivos de su equipo ordenados, siendo de su responsabilidad conservar espacio suficiente en el disco duro para poder ejecutar sus aplicaciones.

7.4. Normas Generales de Utilización de Hardware y Software

La Dirección de Informática y Estadística es la única autorizada para:

a) Efectuar mantenimientos preventivos y/o correctivos en los equipos
b) Instalar software y sistemas que los usuarios requieran
c) Solo se le dará mantenimiento a los equipos que pertenezcan a la secretaría y estén debidamente identificados con su respectivo número de inventario.
d) En ningún momento deberá manipularse alimentos o bebidas cerca o sobre los equipos computacionales, ya que cualquier derrame podrá causar daños al mismo.
e) No está permitida la utilización de los equipos con fines recreativos ni con fines particulares.
f) El usuario en lo posible debe mantener la limpieza externa de los equipos.
g) El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de los equipos.
h) Evitar prestar o intercambiar los equipos de cómputo.

i) En ningún momento se deberán instalar equipos o periféricos (módems, discos duros externos, Access point) que de alguna manera interactúen con la infraestructura o equipos de tecnología e informática de la Institución, sin la supervisión y autorización de la Dirección de Informática y Estadística.

j) El equipo que sea entregado al usuario contendrá en el disco duro el software básico, para el desempeño de sus funciones. Siendo el software básico, el definido por la Dirección de Informática y Estadística.

k) Cualquier otro software que requiera el usuario, deberá ser solicitado a la Dirección de Informática y Estadística por medio de solicitud escrita o formulario

l) Toda solicitud ingresada a la Dirección de Informática y Estadística, será evaluada y de considerarse a lugar, se procederá a la instalación del software solicitado siempre que la Institución cuente con las respectivas licencias para la instalación y uso del mismo.

m) Si la Dirección de Informática y Estadística considerara a lugar la solicitud, pero no existiere el licenciamiento correspondiente dentro del inventario de software licenciado de la Institución, entonces será responsabilidad del interesado, tramitar con las Autoridades Superiores la autorización de compra, misma que de ser autorizada deberá pasarse a la Entidad de Compras de la Institución, quienes deberán basarse en las especificaciones técnicas que la Dirección de Informática y Estadística defina y además cumplir con todos los procedimientos legales, presupuestarios o cualquier otro que la Institución establezca.

n) Toda solicitud de algún software aplicativo deberá hacerse por escrito a la Dirección de Informática y Estadística, por medio de la dirección interesada. Será la Dirección de Informática y Estadística, quien determine los planes de desarrollo y prioridad; así como también si el desarrollo se realizará interno o a través de la contratación de un tercero.

o) La instalación y pruebas técnicas de software y/o sistemas solo podrán ser efectuadas por la Dirección de Informática y Estadística.

p) En todo momento deberá respetarse la propiedad intelectual, por lo que no se podrá copiar o redistribuir software sin la autorización del fabricante o de la Dirección de Informática y Estadística si corresponde.

q) Toda instalación de software y/o sistema no autorizado por la Dirección de Informática y Estadística, que provoque el inadecuado funcionamiento del equipo o de aplicaciones autorizadas, será total responsabilidad del usuario.

r) Todo software que no haya sido instalado con autorización expresa de la Dirección de Informática y Estadística, podrá ser eliminado sin previo aviso y sin responsabilidad alguna para la Dirección de Informática y Estadística por los datos o información que el usuario reclame como perdidos.

7.5. Prohibiciones

a) Copiar o "piratear" software, a menos que este sea de domino público (Freeware, Open Source). La violación a esta prohibición es un acto ilícito, que puede causar sanciones legales para la secretaría.

b) Alterar software y/o sistemas que se encuentran a su disposición.

c) Instalación y uso de software recreativos (juegos).

d) Cambiar la configuración de los equipos, que ha sido determinada por la Dirección de Informática y Estadística.

e) Ninguno de los programas que se encuentran registrados deben ser instalados en otro sistema o computador diferente de aquel donde este se encuentre instalado, licenciado y autorizado por la Dirección de Informática y Estadística.

f) Instalar software no autorizado, ni siquiera un simple protector de pantalla, ya que esto podría en algún momento causar daños a los equipos informáticos y/o redes por infección de virus, spyware, hardware o algún otro; lo que podría ocasionar pérdidas importantes de información, atrasos y en el peor de los casos, consecuencias irremediables que signifiquen un alto costo para la secretaría.

g) Realizar la actualización a nuevas versiones de software sin la autorización expresa de la Dirección de Informática y Estadística.

h) Copiar y/o almacenar en el disco duro del equipo que le fue asignado cualquier tipo de archivo que no tenga relación a las funciones laborales del usuario; como por ejemplo: archivos de sonido, videos, imágenes o cualquier otro de carácter personal.

i) Colocar información contraria a aquella socialmente aceptada o que vaya en contra del decoro y el respeto debidos a la SENABED o a alguno de sus miembros.
j) Colocar información ofensiva directa o indirecta en contra de las autoridades, sus compañeros de labores o personas vinculadas.
k) Consumir alimentos y bebidas junto a los equipos de cómputo.
l) Intercambiar componentes o accesorios entre equipos de cómputo, sin la autorización de la DIE.
m) Instalar software sin autorización del personal encargado de la DIE.
n) Utilizar chat, solamente si se demuestra la finalidad laboral del mismo, este servicio será autorizado por el personal encargado de la DIE.
o) Cambiar la configuración de los equipos, servidores o cualquier dispositivo que se encuentre conectado a la red.
p) Instalar y utilizar aplicaciones que evadan las políticas de seguridad de la información de la entidad (proxy´s, anonimizadores)
q) Utilizar herramientas de análisis de tráfico de red.
r) Utilizar los servicios de red para propósitos no académicos o usarlos para propósitos fraudulentos, comerciales o publicitarios, o para la propagación de archivos de cualquier tipo y mensajes obscenos o destructivos.

7.6. Amonestaciones

a) Cualquier quebranto a las normas o políticas establecidas en el presente documento será motivo de amonestación administrativa, por lo que es obligación de la Dirección de Informática y Estadística, elaborar los informes correspondientes a la Dirección Administrativa o de Recursos Humanos de la Institución quienes en su momento determinarán la sanción correspondiente basándose en lo grave de la falta, recurrencia o cualquier otro criterio administrativamente válido.

7.7. Directivas de Seguridad para el usuario

a) Contraseñas Aceptables: La principal forma es utilizar passwords con combinaciones de minúsculas y mayúsculas, números mezclados con texto, símbolos como &, $ o %, etc., y con un mínimo de 6 caracteres. No deben ser utilizadas claves simples como nombres propios, combinaciones débiles como Pepito1 o nombres de lugares, actores, personajes de libros, deportistas. Por último, es necesario recordar que para que una contraseña sea aceptable obligatoriamente ha de cumplir el principio "manténgala en secreto". Esto porque la contraseña más larga, la más difícil de recordar, la que combina más caracteres no alfabéticos pierde su robustez si su propietario la comparte con otras personas.

b) Caducidad de Contraseñas: La idea de esta directiva es proteger los claves de los usuarios dándoles un período de vida máximo de 45 días, una contraseña solo va a ser válida durante este tiempo, pasado el cual expirará y el usuario deberá cambiarla. Además del tiempo de caducidad se suma el historial de contraseñas, obligando al usuario a utilizar una contraseña distinta a la que caducó para que dicha directiva prevenga más que problemas con las claves, problemas con la transmisión de estas. De esta forma un usuario que conozca o llegue a conocer la contraseña de otro usuario solo podrá utilizarla hasta que el sistema nos obligue a cambiarla. Cabe recalcar que si tras el período de cambio obligatorio, la clave permanece inalterado, la cuenta se bloquea y es necesario solicitar al Administrador del Sistema desbloquear la misma.

c) Bloqueo de Usuarios por Autenticación Fallida: Se considera necesario el bloqueo de cuentas de usuario después de 5 intentos fallidos de autenticación, esto con el fin de evitar que usuarios malintencionados intenten repetidamente hacer login con cuentas de otros usuarios, necesitando solicitar al Administrador del Sistema desbloquear la cuenta.

d) Estandarización del Escritorio: Con esto se busca evitar que el usuario modifique las configuraciones de presentación de su perfil de trabajo y mejorar el rendimiento de los equipos.

e) Bloqueo de sitios y aplicaciones en la WEB: Bloquear el acceso a distintos sitios en la WEB a través de un módulo de filtrado WEB basado en el tema descriptivo que posee cada uno de los dominios, para evitar el ocio en los usuarios que poseen acceso a este servicio. Se aplicará también un reglamento del Correcto Uso del Servicio de Navegación por Internet esto con el fin de implementar sanciones a los usuarios que hagan mala utilización de esta herramienta.

f) Bloqueo de mensajería instantánea: Bloquear el uso de programas de mensajería instantánea tales como skype, gtalk, whats app en wifi, etc. para evitar el tráfico de red excesivo.

g) Acceder, analizar o exportar archivos que sean accesibles a todo el mundo pero que no sean del usuario salvo que se encuentre en una localización que admita su uso público.

h) No se recomienda compartir cuentas de usuario ni las contraseñas de acceso a las mismas.

8. Política de Uso de la Red de Datos y Servicio de Internet

8.1. Objetivos

Definir las políticas para el correcto uso de la red de datos y los servicios de internet. Además contar con un documento de referencia que pueda ser utilizado en auditorias para verificar los aspectos relacionados a los indicados en el presente documento

8.2. Responsabilidad

a) La Institución, a través de la Dirección de Informática y Estadística, podrá proveer a sus colaboradores de cuentas de acceso a Internet, y a la red de datos, con el objeto de darles apoyo en su trabajo diario en las labores de investigación y comunicación con los diversos sistemas con los que se relaciona la entidad. Dichas cuentas de acceso a internet y a la red de datos están asignadas a los colaboradores, pero son constantemente monitoreadas por la Dirección de Informática y Estadística.

b) Todo usuario que haga uso de estos servicios deberá leer, entender y aceptar las políticas que se presentan a continuación.

c) El usuario se compromete a aceptar las condiciones estipuladas en este reglamento en las que se señala el uso de los servicios con fines puramente laborales, lo que excluye cualquier uso comercial de la red, así como prácticas desleales (hacking) o cualquier otra actividad que voluntariamente tienda a afectar a otros usuarios de la red, tanto en las prestaciones de ésta como en la privacidad de su información.

d) Cualquiera que se conecte a la red local queda sujeto a las normas y condiciones contenidas en este documento.

k) Corresponde al personal autorizado de la Dirección de Informática y Estadística y Estadística la coordinación del diseño y la gestión de la red incluyendo la gestión del cableado del edificio.

l) Podrá delegarse la gestión del cableado cuando las condiciones así lo requieran, mediante la aprobación de la DIE en que se especifiquen las condiciones de delegación.

m) Todos los equipos que se conecten a la red de datos de la SENABED deben ser previamente autorizados o autenticados.

n) Se hace del conocimiento que se lleva una bitácora de todos los sitios que el usuario visita, no así de la información que se transmite y que en cualquier momento se puede emitir un reporte de esta información, así como de la cantidad de veces y tiempo estimado que un usuario ha estado utilizando Internet.

o) La Institución no garantiza la privacidad de la información transmitida desde y hacia Internet por medio de los navegadores ni aun siendo transmitida por HTTPS. La Dirección de Informática y Estadística no se responsabiliza ni puede dar soporte al uso de sitios navegados, debido a que cada uno de ellos es responsabilidad propia de los creadores, administradores o publicadores por lo mismo la coordinación no tiene conocimiento de la funcionalidad de estos sitios.

p) Todo el personal respetará los derechos y la propiedad de otros y no entrarán, utilizarán modificarán o eliminarán la información de otros.

8.3. Prohibiciones

Está completamente prohibido realizar cualquiera de las actividades definidas en el apartado bajo el título "Tipos de abusos en la navegación de Internet", así como las Prohibiciones listadas a continuación:

a) Visitar páginas con contenido pornográfico, sexo explícito, juegos y violencia.
b) Visitar páginas con servicios de chateo, audio conferencia o videoconferencia, a menos que por la naturaleza de sus funciones laborales, sea justificado.
c) Descargar del Internet cualquier archivo (Imágenes, videos, música, presentaciones, programas y otros), no importando su tipo, siempre que no tenga ninguna relación con el desempeño de las actividades laborales del usuario.
d) Ejecutar en línea cualquier archivo (videos, música, juegos, programas y otros), no importando su tipo, siempre que no tenga ninguna relación con el desempeño de las actividades laborales del usuario.
e) Visitar y utilizar páginas con servicio de correo electrónico (¡Hotmail, Yahoo!!, Gmail y otros), siempre que la Institución le provea al usuario de una cuenta de correo electrónico.
f) Diseñar "virus", "gusanos", "troyanos" y otros tipos de programas dañinos para sistemas de proceso de la información.
g) Congestionar intencionalmente enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
h) Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso propio en el ambiente laboral.
i) Cambiar de lugar los equipos activos ubicados en las diferentes direcciones de la SENABED.

j) Conectar equipos activos a la red de la entidad, tal es el caso de Routers inalámbricos, módems y cualquiera que altere el buen funcionamiento de la red de datos y de internet de SENABED.

k) Causar daño a sistemas o equipos conectados a la red de SENABED.

l) Utilizar los medios de la red con fines propagandísticos o comerciales.

m) Congestionar intencionalmente enlaces de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.

n) Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso propio en el ambiente laboral.

o) Intentar acceder a las cuentas de usuario de equipos remotos utilizando cualquier protocolo: telnet, ftp etc.

8.4. Tipos de abusos en la navegación de Internet

Las actividades catalogadas como abuso del uso del acceso a Internet se pueden clasificar en los siguientes grupos:

a) El usuario no deberá utilizar su cuenta para deliberadamente afectar el rendimiento de la red. Queda terminantemente prohibido descargar programas desde Internet hacia cualquier medio físico de almacenaje. Si es un software que apoye al trabajo del colaborador, deberá contarse con el visto bueno de la Dirección de Informática y Estadística y del Jefe inmediato.

b) No deberá visitarse sitios en Internet que provean herramientas, con o sin costo, para alterar o violentar la seguridad en los sistemas operativos o informáticos de la Institución (Sitios de "Hacking").

c) Utilizar el Internet para subscribirse a listas de distribución que envían material, no útil para desempeñar el trabajo del personal de la Institución.

d) Utilizar el Internet para perder deliberadamente el tiempo, visitando portales que no provean información útil para el desarrollo de sus actividades diarias (Instagram, Facebook, Twitter, etc.).

e) Utilizar los recursos de internet de la entidad con fines propagandísticos o comerciales.
f) Utilización de proxys anónimos para realizar navegación restringida con los equipos de seguridad de la entidad.
g) Descargar música y/o videos por medio de internet ya que esto degrada considerablemente la velocidad y los servicios dentro de la red de información, los Directores y Jefes de Departamento serán responsables del cumplimiento con esta restricción.

Todas las normas y recomendaciones anteriores son válidas independientemente de cual sea el tipo o medio de acceso a los servicios de la Red de la SENABED, tanto desde dentro, como en accesos remotos a través de Proxys o mediante Módem.

Por lo tanto, cualquier anomalía detectada debe comunicarse inmediatamente a la DIE.

8.5. Privacidad

a) Todos los usuarios conocen y aceptan las cláusulas de privacidad que se presentan a continuación, por lo que no constituirá violación de su privacidad cualquier tema contemplado.
b) El servidor de acceso a Internet cuenta con las bitácoras que permiten conocer los lugares visitados, tiempos consumidos, las horas de entrada - salida de dichos lugares, así como los nombres y tamaños de la información trasmitida (descargas).
c) Las Autoridades Superiores de la Institución están facultadas para solicitar a la Dirección de Informática y Estadística, en base a una investigación oficial, el despliegue del contenido de las bitácoras relacionadas al uso del servicio de Internet por usuario.
d) La Dirección de Informática y Estadística, está facultada para generar los informes relacionados al uso por usuario de este servicio, a solicitud de los Gerentes, Jefes y coordinadores, que permita monitorear la utilización de este servicio.

e) La Dirección de Informática y Estadística, está facultada para generar los informes relacionados al uso por usuario de este servicio y dirigirlos a donde corresponda, en el momento que considere necesario, o cuando se detecte mal uso de este servicio.

f) Todos los equipos que se conecten a la red de datos deben ser previamente autorizados y revisados por personal de la Dirección de Informática y Estadística con el fin de evitar cualquier tipo de intrusión por malware contenido en los equipos visitantes.

8.6. Amonestaciones

a) Cualquier quebranto o violación de las normas y/o políticas establecidas en el presente documento, implicará la suspensión inmediata del acceso a este servicio y reporte a RRHH para la aplicación de la medidas disciplinarias correspondientes.

b) La cancelación parcial o definitiva del acceso a este servicio quedará a disposición de criterio de las Autoridad Superior, por lo que cualquier reactivación deberá solicitarse por escrito a la Dirección de Informática y Estadística, con visto bueno, firma y sello del jefe inmediato.

c) Procedimientos de Altas y Bajas a usuarios dentro de la Red de Datos

d) Cuando se tiene personal de reciente ingreso y se le asignará un equipo de cómputo, es necesario que el Jefe inmediato lo reporte a la Dirección de Informática y Estadística para que le den de alta y se genere el usuario y contraseña.

e) Cuando un usuario se retira definitivamente de la institución, el Jefe inmediato debe reportarlo a la Dirección de Informática y Estadística y Estadística para que se eliminen sus niveles de acceso y seguridad y realizar backup de archivos.

f) Cuando un usuario se cambia de puesto, el Jefe inmediato debe reportarlo al Departamento de Informática y Estadística para que se cambien sus niveles de acceso y seguridad o para realizar backup de archivos.

g) Si una contraseña de usuario se olvida o se necesita ingresar a alguna computadora y se desconoce la contraseña de acceso, solamente se podrá efectuar este cambio con la autorización del interesado o del Jefe del departamento.

8.7. Prohibiciones

a) Instalar internet a los usuarios sin la autorización del Jefe Superior o Inmediato.
b) Instalar correo electrónico a los usuarios sin la autorización del Jefe Superior o Inmediato.
c) Dar de Alta a los usuarios en la red de datos de SENABED sin la debida autorización del Jefe Superior o Inmediato.

9. Política de Uso de Correo Electrónico.

9.1. Objetivos

Definir las políticas para el correcto uso del correo electrónico.

Contar con un documento de referencia que pueda ser utilizado en auditorias para verificar los aspectos relacionados a los indicados en el presente documento

9.2. Políticas de Servicios

La SENABED, a través de la Dirección de Informática y Estadística, proveerá a sus colaboradores de cuentas de correo electrónico, con el objeto de darles apoyo en su trabajo diario. Dichas cuentas de correo electrónico están asignadas a los colaboradores, pero son propiedad de la Secretaría Nacional de Administración de Bienes en Extinción de Dominio.

Todo usuario que haga uso de estos servicios deberá leer, entender y aceptar las políticas que se presentan a continuación:

9.3. Acceso a los Servicios

La utilización de los recursos de red y de información está abierta a todas las gerencias, unidades y/o departamentos de la secretaría bajo las políticas de acceso definidas en el

contexto del presente documento y a otras personas a las que la SENABED desee extender los privilegios de acceso, dadas las condiciones de disponibilidad de recursos, servicios y aprobación por escrito de la Secretaria Nacional de Administración de Bines en Extinción de Dominio.

9.4. Responsabilidad

a) Cada empleado de la institución es el único responsable de las actividades realizadas con las cuentas de correo electrónico y sus buzones asociados que tenga asignados.
b) Los mensajes que se envíen por correo, serán de completa responsabilidad del usuario emisor y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos mensajes podrán emplearse en contra de los intereses de personas individuales, los de la Institución, así como de ninguna otra Institución.

9.5. Uso del correo electrónico

El correo electrónico es un medio de comunicación que no substituye los canales y medios oficiales de comunicación de la Institución.

El uso del correo electrónico y documentos adjuntos se limita a las funciones y atribuciones propias de cada puesto. Exceptuando el uso ocasional para temas personales siempre y cuando el formato del contenido del correo sea texto plano y que, además:

- No interfieran con el rendimiento del servicio de correo electrónico de la Institución.
- No interfieran en las labores propias del empleado.
- No suponen un alto costo para la Institución.

Está permitido el envío de archivos adjuntos siempre que el contenido de los mismos tenga una relación directa con el desempeño del puesto del usuario de la cuenta de correo.

Se recomienda que todo correo electrónico enviado cumpla con las normas básicas de etiqueta definidas en el apartado bajo el título "Normas básicas de etiqueta en el uso del correo electrónico".

9.6. Solicitud de creación de cuentas de correo electrónico

La creación de las cuentas de correo electrónico deberán ser solicitadas a la Dirección de Informática y Estadística, por medio de oficio firmado por el Gerente del colaborador solicitante, este será el único documento válido de solicitud para la creación de las cuentas de correo electrónico.

Todas las solicitudes serán atendidas en un tiempo no mayor a 24 horas a partir de la recepción de la misma.

9.7. Prohibiciones

Está completamente prohibido realizar cualquiera de las actividades definidas en el apartado bajo el título "Tipos de Abuso en el uso del Correo Electrónico". Así como las Prohibiciones listadas a continuación:

a) Iniciar o dar seguimiento a "cadenas de correo" que contengan mensajes que no sean relacionados al trabajo.
b) Distribuir, ya sea de forma masiva o no, mensajes con contenidos inapropiados para la institución.
c) Falsificar el origen o el encabezado de los correos electrónicos.
d) Utilizar las cuentas de la institución para recibir correos reenviados automáticamente (forward) desde una cuenta externa de correo electrónico.
e) El envío de correos electrónicos masivos sin autorización previa
f) La suscripción a listas de distribución de correo electrónico que no tengan relación a las funciones laborales del empleado.
g) Utilizar la cuenta de correo para perder deliberadamente el tiempo en horarios de trabajo, por medio del envío y/o lectura de mensajes ajenos a la actividad diaria que se desarrolla; es decir, mensajes de entretenimiento y con archivos adjuntos, tales

como, presentaciones o imágenes, en especial aquellas que atenten contra la moral (entiéndase entre otros: contenido pornográfico, violencia y sexo).

9.8. Tipos de Abuso en el Uso del Correo Electrónico

Las actividades catalogadas como Abuso de Correo Electrónico se pueden clasificar en cuatro grandes grupos:

a) Difusión de contenido inadecuado

Contenido ilegal por naturaleza (todo el que constituya complicidad con hechos delictivos).

Ejemplos: apología del terrorismo, programas piratas, pornografía, amenazas, estafas, esquemas de enriquecimiento piramidal, virus o código hostil en general.

b) Difusión a través de canales no autorizados

Uso no autorizado de los servidores de correo electrónico de la Institución para reenviar correo de beneficio propio, por ejemplo, con el envío de publicidad u ofrecimiento de venta. Aunque el mensaje en sí sea legítimo, se están utilizando recursos de la institución sin autorización para usos particulares.

c) Difusión masiva no autorizada

Es el uso de servidores de correo electrónico propios o ajenos para enviar de forma masiva publicidad o cualquier otro tipo de correo no solicitado. Su principal agravante es que el anunciante descarga en transmisores y destinatarios el costo de sus operaciones publicitarias, aunque el usuario no esté de acuerdo.

d) Ataques con objeto de imposibilitar o dificultar el servicio

Puede ser dirigido a un usuario o al propio sistema de correo. En ambos casos el ataque consiste en el envío de un número alto de mensajes por segundo, o cualquier variante, que tenga el objetivo neto de paralizar el servicio por saturación de la capacidad de CPU del servidor, o del espacio en disco de servidor o usuario.

9.9. Privacidad

a) Todos los usuarios conocen y aceptan las cláusulas de privacidad que se presentan a continuación, por lo que no constituirá violación de su privacidad cualquier tema contemplado.
b) Se guarda un historial de todos los correos enviados y recibidos en el servidor de correo electrónico lo cual permite realizar auditorías de la información alojada en el mismo en el momento que sea requerido.
c) Las autoridades superiores están facultadas para solicitar en base a una investigación oficial, que la persona permita que sea revisado su buzón de correo electrónico y carpetas personales de correo.

9.10. Amonestaciones

La Dirección de Informática y Estadística es la única autorizada para administrar y controlar la utilización de este recurso.

Cualquier quebranto de las normas establecidas en el presente documento, implicará la suspensión del acceso al servicio y reporte a RRHH para la aplicación de las medidas disciplinarias correspondientes.

La cancelación parcial o definitiva del acceso a este servicio quedará a criterio de la Autoridad Superior, por lo que cualquier reactivación deberá solicitarse por escrito a la Dirección de Informática y Estadística con visto bueno, firma y sello del jefe inmediato.

9.11. Normas básicas de etiqueta en el uso del correo electrónico

a) Se sugiere que el asunto (subject) del correo no vaya en blanco, debe de contener una descripción razonable del contenido del mismo.
b) El contenido del correo debe ser políticamente correcto. Entiéndase no debe ofender o incitar actitudes en contra de los intereses de la institución o de sus empleados o cualquier ente externo.
c) Se debe de utilizar un lenguaje apropiado para el profesionalismo de nuestra Institución.

d) Todos los correos deben de incluir una firma que incluya los siguientes datos: nombre completo, puesto, departamento. Se sugiere incluir el número telefónico y algún otro medio alterno de comunicación. No deberá incluir imágenes.
e) NO DEBEN DE ESCRIBIRSE LOS CORREOS EN MAYÚSCULAS. El hecho de escribir en mayúsculas puede ser considerado ofensivo, ya que sugiere un tono elevado de voz.
f) Es importante leer los correos antes de ser enviados, para asegurarse de que transmitan la idea correcta.

10. Políticas de Realización de Backups

10.1. Objetivos

Definir las características del procedimiento de copias de respaldo de los equipos instalados en la red de datos de la SENABED.

Contar con un documento de referencia que pueda ser utilizado en auditorias para verificar los aspectos relacionados a los indicados en el presente documento.

10.2. Políticas del Servicio

a) La Secretaría Nacional de Administración de Bienes en Extinción de Dominio, a través de la Dirección de Informática y Estadística, Realizará una copia de respaldo semanal, quincenal, mensual o a petición de los directores de cada unidad de los equipos que tienen bajo su cargo los colaboradores de la entidad.
b) Todo colaborador que cuente con un equipo de cómputo de la SENABED debe entender y aceptar las políticas que se presentan a continuación.

10.3. Mecanismo de Respaldo

La Dirección de Informática y Estadística instalará un cliente (software instalado) en cada una las estaciones de trabajo de los usuarios de la SENABED, así como en los dispositivos móviles que son propiedad de la SENABED, con el objeto de realizar una sincronización periódica con el servidor de almacenamiento.

El software cliente se conectará con el servidor de backups, y automáticamente trasladará semanalmente toda la información de los usuarios de las distintas gerencias, este procedimiento puede ser realizado automáticamente o por solicitud de los gerentes en cualquier momento que consideren pertinente requerir la información de un colaborador para su revisión.

10.4. Tipos de Documentos a respaldar

La Dirección de Informática de Informática y Estadística de la SENABED, realizará un respaldo con periodicidad diaria, quincenal y mensual a todas las Direcciones y unidades de la institución de los siguientes tipos de archivos.

- Documentos de Ofimática; Word, Excel, Power Point, Adobe Pdf.
- Correo Electrónico; Archivo PST de correo electrónico.
- Documentos de diseño; Photoshop, AutoCad y otros afines.
- Archivos comprimidos; Zip, Rar, .7zip, previo análisis de los mismos.
- Archivos de mapas y geo posicionamiento
  Archivos multimedia serán respaldados únicamente en el caso de unidades que estén relacionadas íntimamente con este tipo de archivos.

La Dirección de Informática y Estadística no se hace responsable de la información personal que el usuario pueda almacenar en el equipo y está en la libertad de borrar cualquier contenido que pueda afectar el funcionamiento del equipo o material con contenido inapropiado haciendo del conocimiento respectivo a la Dirección de Recursos Humanos. Dentro del material antes mencionado se encuentran:

- Música y video; archivos .mp3, .wmv, .mpeg, .avi, y todo archivo multimedia que no esté relacionado con las actividades de la SENABED.
- Material pornográfico de cualquier índole
- Archivos ejecutables de programas que no son instalados por el personal de la Dirección de Informática y Estadística de la SENABED.

La Dirección de Informática y Estadística borrará automáticamente todo aquel contenido inapropiado y trasladará una copia de dicho material a Recursos Humanos para que se tomen las medidas pertinentes sobre la posesión de dicho material.

10.5. Requerimiento de Copia de respaldo

Las copias de respaldo de los equipos de una unidad, dirección o de un equipo en específico deben ser solicitadas por escrito por el director a cargo, Recursos Humanos, o autoridad superior de la secretaría; al realizar la copia de respaldo de un usuario o usuarios las copias serán entregadas a la entidad solicitante.

La Dirección de Informática guardará una copia en el servidor correspondiente durante un periodo de tiempo prudencial mientras la información es archivada dentro del histórico de backups de la SENABED.

El usuario o usuarios a los que se les realice la copia de respaldo están en la libertad de pedir una copia a su jefe inmediato quedando a discreción del mismo la entrega de la misma.

10.6. Ingreso Local y Remoto a los equipos a sincronizar

La Dirección de Informática y Estadística tendrá acceso remoto a los equipos de las unidades para realizar la sincronización de los equipos, este acceso remoto estará permitido exclusivamente para la Dirección de Informática y Estadística. En caso de ser necesario la DIE puede restablecer la contraseña de acceso al equipo de un usuario para sincronizar su información en cualquier momento y de forma presencial (frente al equipo del usuario).

En caso de que el usuario posea instalado algún software que impida el acceso a su información de manera remota o física, la Dirección de Informática puede desinstalar

dicho programa o extraer el disco duro del equipo para extraer la información y formatear el disco duro del usuario.

10.7. Prohibiciones al uso de almacenaje en servicios ajenos a la SENABED

Está completamente prohibido realizar cualquiera de las actividades definidas en el apartado bajo el título "Tipos de abusos en el almacenaje de información", así como las Prohibiciones listadas a continuación:

- Visitar y utilizar páginas con servicio de almacenaje como Dropbox, Google Drive, Sky Drive y almacenar información de la SENABED en dichos Servicios.

10.8. Tipos de abusos en el almacenaje de información

Las actividades catalogadas como abuso se pueden clasificar en los siguientes grupos:

- El usuario no deberá utilizar su cuenta para deliberadamente afectar el rendimiento de la red. Queda terminantemente prohibido descargar programas desde Internet hacia cualquier medio físico de almacenaje. Si es un software que apoye al trabajo del colaborador, deberá contarse con el visto bueno de la Dirección de Informática y Estadística y del Jefe inmediato.
- Queda prohibido almacenar cualquier tipo de material que atente la moral y vayan en contra de las buenas costumbres y/o afecte terceros.
- No deberá instalar programas que impidan el acceso al equipo de cómputo, firewalls, antivirus, u otros que deliberadamente sean instalados para evitar la sincronización periódica.
- Todo el personal respetará los derechos y la propiedad de otros y no deberán ingresar, utilizar, modificar o eliminar la información de otros usuarios.

Este enunciado está amparado por los siguientes artículos del Código Penal de Guatemala.

Registros Prohibidos
Artículo 274 "d"

Programas Destructivos
Artículo 274 "g"

10.9. Privacidad

Todos los usuarios conocen y aceptan las cláusulas de privacidad que se presentan a continuación, por lo que no constituirá violación de su privacidad cualquier tema contemplado.

- La autoridad superior y directores de área la SENABED están facultados para solicitar a la Dirección de Informática copia de la información de los usuarios en cualquier momento lo consideren pertinente.
- La Dirección de Informática y Estadística, está facultada para generar los informes relacionados al servicio de copias de respaldo de los usuarios, a solicitud de los Directores, Jefes y coordinadores, permitiendo monitorear el tipo de información que es almacenada en los equipos de las direcciones.
- La Dirección de Informática y Estadística, está facultada para generar los informes relacionados al uso por usuario de este servicio y dirigirlos a donde corresponda, en el momento que considere necesario, o cuando se detecte irregularidades en la información almacenada.
- Ningún usuario puede borrar, alterar o extraer una copia de respaldo en su beneficio, ni tampoco destruir los registros y archivos que se encuentran en el equipo de cómputo deliberadamente y a su favor.

  El anterior enunciado está respaldado por el siguiente artículo del Código Penal de Guatemala:

  Destrucción de Registros Informáticos
  Artículo 274 "a"
  Alteración de Programas
  Artículo 274 "b"

10.10. Amonestaciones

Cualquier quebranto o violación de las normas y/o políticas establecidas en el presente documento, implicará la suspensión inmediata del acceso a este servicio y reporte a RRHH para la aplicación de las medidas disciplinarias correspondientes.

La cancelación parcial o definitiva del acceso al equipo asignado dependerá de las Autoridad Superior, por lo que cualquier reactivación deberá solicitarse por escrito a la Dirección de Informática y Estadística, con visto bueno, firma y sello de la Autoridad Superior.

11. Glosario de Términos

Chat

Chat (español: charla), que también se le conoce como cibercharla, es un anglicismo que usualmente se refiere a una comunicación escrita a través de Internet entre dos o más personas que se realiza instantáneamente.

DIE

Dirección de Informática y Estadística.

EMAIL

Servicio de mensajería provisto a la comunidad universitaria para facilitar la comunicación y gestión de la institución.

FTP

FTP es uno de los diversos protocolos de la red Internet, concretamente significa File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red.

Gusano

En informática un gusano es un virus o programa autoreplicante que no altera los archivos, sino que reside en la memoria y se duplica a sí mismo.

Hacker

El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas Hacking Es la acción de un Hacker. Usualmente se refiere a la intrusión en un sistema informático.

Internet

Internet es una red de redes a escala mundial de millones de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Módem

Acrónimo de las palabras modulador/demodulador. El módem actúa como equipo terminal del circuito de datos (ETCD) permitiendo la transmisión de un flujo de datos digitales a través de una señal analógica.

Proxy

En el contexto de las ciencias de la computación, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

Red

Una red de computadoras (también llamada red de ordenadores, red informática o red a secas) es un conjunto de computadoras y/o dispositivos conectados entre sí y que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (e-mail, chat, juegos), etc.

SENABED

Secretaría Nacional de Administración de Bienes en Extinción de Dominio.

Spam

Hace referencia a los mensajes no solicitados, no deseados o con remitente no conocido (correo anónimo, correo basura y mensaje basura), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades.

Telnet

Telnet es el nombre de un protocolo (y del programa informático que implementa el cliente) que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.

Usuario

Toda persona que utilice de manera directa o indirecta un servicio provisto por un Recurso Computacional.

Virus

Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada.

12. Validación y Autorización

Manual de Políticas y Estándares de Seguridad Informática Relacionadas al uso del Sistema y Equipo			
Validación de Elaboración: Dirección de Administración de Bienes			
Nombre: Pablo Vela	Nombre: Romeo Cabrera	Nombre: Sergio Barillas	Nombre:
Puesto: Jefe seccion Sistemas	Puesto: Jefe de Informatica	Puesto: Director de Informatica y Estadistica	Puesto:
Firma y Sello:	Firma y Sello:	Firma y Sello:	Firma y Sello:
Fecha: 26/09/2016	Fecha: 26-09-2016	Fecha: 26/09/2016	Fecha:
Validación Técnica del Manual: Dirección de Informática y Estadística			
Nombre: Nara Lucero	Nombre: OSCAR MAURICIO LOPEZ IXCOLIN.	Nombre: Sergio Barillas	Nombre:
Puesto: Jefe Oficina	Puesto: JEFE DEL DEPTO. DE PLANIFICACION Y ESTADISTICA.	Puesto: Director de Informatica y Estadistica	Puesto:
Firma y Sello:	Firma y Sello:	Firma y Sello:	Firma y Sello:
Fecha: 12/10/16	Fecha: 12/10/2016	Fecha: 12/10/2016	Fecha:
Autorización: Secretaría General			
Nombre: Lic. Oscar Humberto Conde		Firma y Sello:	
Puesto: Secretario General			
Fecha: 12/11/2016			