MINISTERIO DE COMUNICACIONES,
INFRAESTRUCTURA Y VIVIENDA

00670

Guatemala, 31 AGO 2009

ACUERDO MINISTERIAL No. 611-2,009

EL MINISTRO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA

CONSIDERANDO

Que a los Ministros de Estado les corresponde dirigir y coordinar la labor de las dependencias y entidades bajo su competencia, debiendo para el efecto dictar los acuerdos, resoluciones, circulares y otras disposiciones relacionadas con el despacho de los asuntos de su ramo, conforme la ley; debiendo para el efecto, tomar las medidas que correspondan en casos de faltas, incumplimiento de deberes u otras infracciones análogas cometidas por los funcionarios y empleados públicos bajo su autoridad.

CONSIDERANDO

Que la modernización y tecnificación de los servicios que presta el Estado, conlleva la puesta en funcionamiento de herramientas tecnológicas que permitan a los servidores públicos una mayor eficiencia, eficacia y efectividad en el cumplimiento de sus obligaciones, lo cual se ve reflejado en la satisfacción de los administrados; sin embargo, deben tomarse las medidas adecuadas para que aquellas no sean objeto de uso inapropiado que solo conlleve la pérdida de tiempo y recursos.

CONSIDERANDO

Que en tal sentido, corresponde a la autoridad nominadora la generación de políticas para el uso de las herramientas tecnológicas que se proporcionen a los funcionarios públicos, mismas que han sido elaboradas por el Ente de Tecnología e Informática del Ministerio de Comunicaciones, Infraestructura y Vivienda tomando en consideración los alcances y propósitos que tiene ese insumo dentro de la Institución; por lo que las mismas deben ser aprobadas en Acuerdo Ministerial a efecto de hacer obligatorio su cumplimiento y ejecución.

POR TANTO

En uso de las facultades conferidas por los Artículos 194, literales a) y f) de la Constitución Política de la República de Guatemala; 22 y 27 literal m) de la Ley del Organismo Ejecutivo,

A C U E R D A

Artículo 1: Aprobar las normas y políticas de seguridad de acceso físico al área de informática; de comunicación interna y externa (correo electrónico); de servicio de navegación por Internet; de uso y hardware y software; y, de seguridad de sistemas, elaboradas por el Ente de Tecnología e Informática del Ministerio de Comunicaciones, Infraestructura y Vivienda, cuyo texto forma parte del presente acuerdo.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

Artículo 2: Corresponde a los Directores, Coordinadores, Gerentes, Jefes y Encargados de cada una de las dependencias y oficinas del Ministerio de Comunicaciones, Infraestructura y Vivienda, velar por el estricto cumplimiento de las normas y políticas aprobadas, debiendo para el efecto aplicar los procedimientos de ley.

Artículo 3. El presente acuerdo entra en vigor inmediatamente.

COMUNÍQUESE

Guillermo Andrés Castillo Ruiz
Ministro de Comunicaciones, Infraestructura y Vivienda

El Viceministro de Comunicaciones,
Infraestructura y Vivienda

Alfredo Estuardo Mury Aguirre
VICEMINISTRO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA

Ministerio de Comunicaciones, Infraestructura y Vivienda
Políticas de Seguridad de Sistemas

Preliminares

Para efectos del presente documento, al Ente de Tecnología e Informática (Dirección de Informática, División de Informática, Departamento de Informática, o el que aplique en la Institución), en lo sucesivo se denominará "ETI".

Introducción

En este documento se enumeran las políticas de seguridad a implementar en la "ETI" de la Institución. Es importante mencionar que se podrán implementar todas aquellas políticas que no fueron mencionadas en el presente documento con el fin de mejorar la seguridad de los sistemas.

Seguridad de la información de la Institución

Para garantizar la fiabilidad de la información que guardan los sistemas informáticos de la Institución, se llevará una bitácora que controle todos los accesos a dicha información, mediante la implementación de políticas de grupo.

Las políticas de grupo no son más que un conjunto de reglas implementadas, mediante cambios efectuados en el Registro, que se activan al iniciar el equipo o cuando un usuario inicia su sesión de trabajo. Las políticas entran a formar parte del entorno de usuario e imponen restricciones sobre las acciones de dicho usuario.

Estas políticas también nos permiten establecer de forma centralizada múltiples aspectos de la configuración que reciben los usuarios cuando se conectan a una máquina del dominio. Estos aspectos incluyen, entre otros, configuraciones del registro, políticas de seguridad, instalación automática de software, ejecución de scripts, redirección de carpetas locales a recursos de red, etc.

Descripción de las Políticas

Dentro de las políticas de grupo a implementar en el directorio activo del dominio de la Institución, se encuentran las directivas aplicables a los equipos y las directivas aplicables a los usuarios.

La configuración del equipo agrupa todos aquellos parámetros de configuración que pueden establecerse a nivel de equipo. Cuando una política de grupo afecta a un equipo, todas aquellas políticas de equipo que el administrador haya configurado se aplicarán al equipo cada vez que se inicie.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

Las configuraciones de usuario agrupan los parámetros de configuración que pueden establecerse a nivel de usuario. Cuando una política de grupo afecta a un usuario, todas aquellas políticas de usuario que el administrador haya configurado se aplicarán cuando dicho usuario inicie una sesión local (en cualquier equipo del dominio).

La jerarquía de políticas en cada uno de ellos se subdivide en tres grupos:

Configuración de Software. Contiene la configuración, bien del equipo o bien de usuario, de la instalación automática de software.

Configuración de Windows. Contiene la configuración de ciertos parámetros de Windows, como parámetros de seguridad o scripts, para el equipo o para el usuario.

Plantillas Administrativas. Contiene las políticas y configuraciones que se guardan en el registro de Windows, para el equipo o para el usuario.

Es decir, en muchos casos, la misma política existe en ambos subárboles (equipo y usuario), aunque generalmente en cada caso con significados y parámetros distintos. Por ejemplo, bajo Configuración del Equipo--Configuración de Windows-- Scripts podemos encontrar los scripts que deben ejecutarse cada vez que el equipo se inicia o detiene, mientras que bajo Configuración de Usuario--Configuración de Windows--Scripts se encuentran los scripts que deben ejecutarse cada vez que el usuario inicia o finaliza una sesión local.

A continuación se exponen los grupos de políticas más importantes que pueden configurarse mediante políticas de grupo, independientemente de su ubicación concreta dentro de la jerarquía.

Plantillas administrativas:
Este grupo contiene todas las configuraciones de políticas basadas en el registro de Windows 2000, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows 2000 y de algunas aplicaciones que utilizan estas políticas.

Configuraciones de seguridad:
En este apartado se encuentra la configuración de muchos de los aspectos de seguridad que pueden establecerse en un Sistema Windows 2000 o superior.

En concreto, y concentrándonos en los aspectos de seguridad a nivel de equipo podemos destacar lo siguientes:

Políticas de cuentas. Se pueden configurar todos los aspectos sobre el plan de cuentas tales como la caducidad de contraseñas, bloqueo de cuentas, configuración de Kerberos, etc.

Políticas locales. Bajo este apartado se encuentran las configuraciones que corresponden a la denominada "Directiva local", es decir, la configuración de la auditoría, la asignación de derechos y privilegios de usuario y las opciones de seguridad.

Registro de eventos. Aquí se controla el registro de eventos en los registros de aplicación, seguridad y sistema, que posteriormente pueden visualizarse con la herramienta Visor de Sucesos.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A. -

Instalación de software:
Mediante este apartado se puede asignar y/o publicar aplicaciones a equipos o a usuarios en el dominio:

Asignar una aplicación significa que los usuarios que la necesitan la tienen disponible en su escritorio sin necesidad de que un administrador la instale. Cuando se asigna una aplicación a un usuario o equipo, se crea una entrada para ella en el menú de inicio y se configura el registro adecuadamente. La primera vez que el usuario ejecuta la aplicación, ésta es automáticamente instalada en el equipo cliente.

Publicar una aplicación a un equipo o usuario le da la oportunidad al usuario de instalar dicha aplicación bajo demanda (a voluntad), pero no se realiza ninguna acción automática en el equipo (no se modifica el menú de inicio ni el registro). La lista de aplicaciones publicadas para un usuario aparecen en el Panel de Control, bajo la herramienta de Añadir/Eliminar Programas, desde donde pueden ser instaladas.

Guiones (Scripts):
Bajo este apartado, se pueden asignar scripts a equipos o usuarios. En concreto, existen cuatro tipos de scripts principales:

Inicio (equipo). Se ejecuta cada vez que el equipo arranca.

Apagado (equipo). Se ejecuta cada vez que el equipo va a detenerse.

Inicio de sesión (usuario). Se ejecuta cada vez que el usuario inicia una sesión interactiva (local) en un equipo.

Cierre de sesión (usuario). Se ejecuta cada vez que el usuario finaliza una sesión interactiva en un equipo.

En todos esos casos, los scripts pueden implementarse en cualquiera de los lenguajes que entiende el soporte de scripts independiente del lenguaje de Windows 2000, o Windows Scripting Host. Actualmente existe soporte para Visual Basic Scripting Edition, Java Script, PERL y los tradicionales archivos por lotes MS-DOS.

El comportamiento de los scripts puede perfilarse mediante algunas políticas que se sitúan en el apartado de Plantillas Administrativas. En la Tabla a continuación se muestran algunas que resulta útil conocer.

Redirección de carpetas:
Este grupo de políticas permite redirigir la ubicación local predefinida de ciertas carpetas particulares de cada usuario (como "Mis Documentos" o el menú de inicio) a otra ubicación, bien sea en la misma máquina o en una unidad de red.

Un ejemplo útil de redirección sería que la carpeta "Mis documentos" apuntara a un directorio personal de cada usuario en la red, como por ejemplo el recurso \\servidor\home\%username%. Esta aproximación resulta más útil que conectarle a dicho usuario ese recurso a una unidad de red, puesto que muchas aplicaciones abren automáticamente la carpeta "Mis documentos" para buscar los archivos personales de ese usuario. Para que dicha redirección funcione correctamente, es necesario que el usuario que recibe la redirección sea el propietario de la carpeta compartida.

Otras políticas:
Existen muchas otras políticas que quedan fuera del contexto del presente documento. Entre ellas, podemos destacar el mantenimiento de Internet Explorer, que controla la apariencia y la configuración personal de este navegador de web para cada usuario, y los Servicios de Instalación remota, que permiten configurar automáticamente las opciones de instalación de Windows.

Directivas a implementar

Después de haber descrito muy generalmente el alcance de las políticas de grupo, pasamos a elaborar una lista detallada de las políticas a aplicar en el directorio activo de la Institución.

Directivas para el usuario

- *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. Por supuesto, hemos de huir de claves simples como internet o beatles, 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 "Keep it SECRET " que quiere decir manténgala en secreto. Esto por qué?, 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.

- *Caducidad de contraseñas:* La idea de esta directiva es proteger los passwords 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, el password permanece inalterado, la cuenta se bloquea y es necesario solicitar al Administrador del Sistema desbloquear la misma.

- *Bloqueo de usuarios por autenticación fallida:* Se considera necesario el bloqueo de cuentas de usuario después de 3 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.

- *Deshabilitar el acceso al Panel de Control.* El principal objetivo es proteger al sistema de modificaciones y mantener un entorno estándar, asegurando así la funcionalidad de las aplicaciones y sistemas operativos de los equipos en el Dominio de la Institución.

- *Deshabilitar el acceso al entorno de Red.* Esto con el objetivo primordial de evitar que usuarios malintencionados o personal ajeno a la "ETI", realicen cambios en la configuración de red de los equipos, evitando así la pérdida de comunicación.

- *Deshabilitar el uso del comando NetSend:* Con esta directiva se evita el exceso de tráfico en la red al bloquear la mensajería instantánea a través de la misma.

- *Deshabilitar la instalación de software:* Esto es importante desde el punto de vista que, se evita que los usuarios agreguen software que generen ocio y pérdida de tiempo y a la vez se evita la instalación de software pirata o no licenciado.

- *Deshabilitar la ejecución de software:* Se busca deshabilitar la ejecución de programas específicos tales como juegos para evitar el ocio y herramientas administrativas a las cuales solo los técnicos en soporte tendrán acceso como herramientas de trabajo.

- *Fijar configuración del explorador:* El único objetivo es evitar configurar en cada equipo la configuración del explorador para navegación por Internet. Esto no implica que todos los usuarios tendrán acceso al servicio ya que la autenticación de usuarios autorizados la realiza el servidor de Internet al momento de registrar la solicitud del usuario para navegación.

- *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.

- *Redirección de documentos del usuario:* Esta es una directiva de seguridad aplicable si se cuenta con un servidor de datos; la utilidad es sencilla, los usuarios disponen de su información no importando en que computador inicien sesión además de brindar ventajas en las tareas de back-up. Lo que se hace es direccionar la carpeta "Mis Documentos" de todos los usuarios a un servidor de datos.

- *Bloqueo de sitios 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.

- *Bloqueo de mensajería instantánea:* Bloquear el uso de programas de mensajería instantánea tales como msn messenger y yahoo messenger para evitar el trafico de red excesivo.

- *Auditoria de acceso a recursos:* Implementar una auditoria de acceso a los sistemas de la Institución. Esto para tener control de quien accesa a la información, hora y fecha del acceso así como que modifico. Estos controles se hacen a nivel de nombre usuario, es por eso la importancia de la confidencialidad de las contraseñas.

- *Activación de horarios para login:* Con esto lo que se busca es proteger a los usuarios en el sentido que, si intentan utilizar su usuario y contraseña en horarios no autorizados para acceder a los sistemas, este evento se registra con el fin de investigar la violación y mejorar la seguridad en el acceso a los recursos.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

Ministerio de Comunicaciones,
Infraestructura y Vivienda

Políticas seguridad de acceso físico al área de informática

Preliminares

Para efectos del presente documento, al Ente de Tecnología e Informática (Dirección de Informática, División de Informática, Departamento de Informática, o el que aplique en la Institución), en lo sucesivo se denominará "ETI".

Seguridad en las instalaciones de la "ETI"

Para que cualquiera de las políticas de seguridad enfocadas a los datos sea funcional, también es necesario garantizar la seguridad en cuanto a acceso a las instalaciones físicas de la "ETI", dado que, es en este lugar donde se resguardan los servidores, Bases de Datos y sistemas, así como todos los equipos de telecomunicaciones.

Basado en lo ya expuesto, se recomienda implementar las siguientes medidas de seguridad en el acceso a las instalaciones de la "ETI".

- El l acceso a la "ETI" deberá ser restringido, solo para personal autorizado, contándose con un registro de entradas y salidas de terceras personas (incluye a los de mantenimiento del aire acondicionado, los visitantes y el personal de limpieza). Éstos y cualquier otro personal ajeno a la instalación deben ser:
  - Identificados plenamente.
  - Controlados y vigilados en sus actividades durante el acceso.
  - El personal de mantenimiento y cualquier otra persona ajena a la instalación se debe identificar antes de entrar a ésta. El riesgo que proviene de este personal es tan grande como de cualquier otro visitante,
  - La permanencia dentro de las instalaciones de la "ETI", de cualquier persona ajena a la misma deberá estar siempre acompañado por algún miembro de la misma y en constante vigilancia.

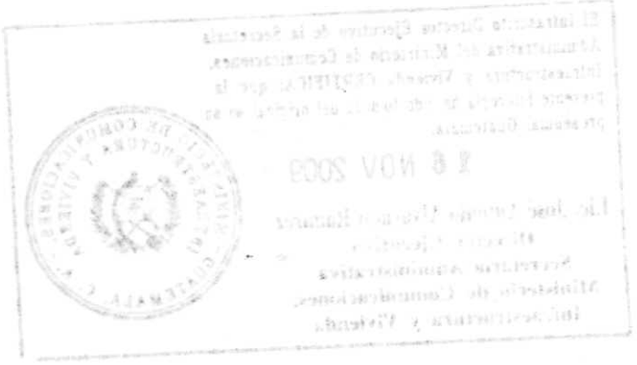
MINISTERIO DE COMUNICACIONES INFRAESTRUCTURA Y VIVIENDA GUATEMALA, C. A.

- Registro de firma de entrada y salida. Consiste en que todas las personas que entren a las instalaciones firmen un registro que indique la hora de entrada, el motivo por el que entran, la persona a la que visitan y la hora de salida. Se recomienda un formato de registro de visitantes como el siguiente:

    - Fecha
    - Nombre
    - Procedencia
    - Departamento que visita
    - Persona que busca
    - Asunto
    - Hora de entrada
    - Firma
    - Hora de salida
    - Firma
    - Observaciones

- Al acceso al área de servidores debe estar totalmente restringida. Únicamente debe estar autorizado el ingreso el Jefe O Coordinador General de la "ETI", y a quienes por la naturaleza de sus funciones necesiten ingresar a esta área, siempre y cuando lo autorice el Jefe o Coordinador General de la "ETI", y que su permanencia esté siempre en constante vigilancia. Se recomienda que el control de accesos se haga por medio de lector de huella digital o cualquier otro dispositivo de lecturas biométricas.

- La "ETI" debe de contar con una caja fuerte para salvaguardar las copias de respaldo de la información.



Ministerio de Comunicaciones, Infraestructura y Vivienda

Políticas de Comunicación Interna y Externa (Correo Electrónico)

Preliminares

Para efectos del presente documento, al Ente de Tecnología e Informática (Dirección de Informática, División de Informática, Departamento de Informática, o el que aplique en la Institución), en lo sucesivo se denominará "ETI".

Objetivos

1. Definir las políticas para el correcto uso del correo electrónico.
2. Contar con un documento de referencia que pueda ser utilizado en auditorias para verificar los aspectos relacionados a los indicados en el presente documento.

Políticas del servicio

La Institución, a través de la "ETI", 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 Institución.

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

1) Acceso a los servicios

La utilización de los recursos de red y de información está abierta a todas las oficinas y/o departamentos de la Institución bajo las políticas de acceso definidas en el contexto del presente documento y a otras personas a las que la Institución desee extender los privilegios de acceso, dadas las condiciones de disponibilidad de recursos, servicios y aprobación por escrito de la Autoridad Superior.

2) Responsabilidad

Cada empleado de la institución es el único responsable de las actividades realizadas con la(s) cuenta(s) de correo electrónico y su(s) buzón(es) asociado(s) que tenga asignado(s).

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.

3) 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 totalmente permitido el envío de archivos adjuntos siempre que el contenido de los mismos tengan 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 titulo "Normas básicas de etiqueta en el uso del correo electrónico".

4) Solicitud de creación de cuentas de correo electrónico

La creación de las cuentas de correo electrónico deberán ser solicitadas a la "ETI", por medio de solicitud escrita o si la Institución tuviere formulario diseñado para el efecto, este será el único documento válido de solicitud para la creación de las cuentas de correo electrónico.

En cualquiera de las formas utilizadas, la solicitud como mínimo deberá incluir:

- Nombre completo del usuario;
- Oficina o Departamento donde labora;
- Puesto que desempeña;
- Justificación válida y que relacione el desempeño de las actividades del usuario de la cuenta;
- Visto bueno, firma y sello de la autoridad competente de la siguiente manera:
  - **Para correo Interno**, será el Jefe de Departamento o equivalente.
  - **Para correo externo**, será la Autoridad Superior (Ministro o Viceministro Administrativo para el caso de la Dirección Superior; Director o Subdirector Administrativo o equivalentes, para el caso de las Dependencias).

Toda solicitud ingresada a la "ETI" tendrá un proceso de análisis previa autorización. Es importante recalcar que no se le dará trámite a ninguna solicitud que no cumpla con los requerimientos establecidos.

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

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

5) Prohibiciones al uso del correo electrónico

Esta 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:

- Iniciar o dar seguimiento a "cadenas de correo" que contengan mensajes que no sean relacionados al trabajo.
- Distribuir, ya sea de forma masiva o no, mensajes con contenidos inapropiados para la Institución.
- Falsificar el origen o el encabezado de los correos electrónicos.
- Utilizar las cuentas de la institución para recibir correos reenviados automáticamente (forwarded) desde una cuenta externa de correo electrónico.
- El envío de correos electrónicos masivos sin autorización previa.
- La suscripción a listas de distribución de correo electrónico que no tengan relación a las funciones laborales del empleado.
- 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).

6) Tipos de abuso en el uso del correo electrónico

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

- **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.

- **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.

- **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 este de acuerdo.

- **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.

7) 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.

- El servidor de correo electrónico cuenta con las bitácoras que permiten conocer los títulos, destinatarios, nombres de archivos, tamaños y horas de los mensajes enviados tanto en el correo interno como externo.

- 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.

8) Sanciones

Las Autoridades Superiores y Jefe de la "ETI", son los únicos autorizados para administrar y controlar la utilización de este recurso.

Cualquier quebranto de las normas establecidas en el presente documento será motivo de sanción, que implicará la suspención del acceso al servicio y reporte a RRHH.

La cancelación parcial o definitiva del acceso a este servicio será a criterio de las Autoridades Superiores, por lo que cualquier reactivación deberá solicitarse por escrito a la "ETI" con visto bueno, firma y sello de las Autoridades Superiores.

9) Normas básicas de etiqueta en el uso del correo electrónico

- Se sugiere que el asunto (subject) del correo no vaya en blanco, debe de contener una descripción razonable del contenido del mismo.

- 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.

- Se debe de utilizar un lenguaje apropiado para el profesionalismo de nuestra Institución.

- 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.**

- 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.

- Es importante leer los correos antes de ser enviados, para asegurarse de que transmitan la idea correcta.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

Ministerio de Comunicaciones, Infraestructura y Vivienda

Normas y Políticas de uso de Hardware y Software

Preliminares

Para efectos del presente documento, a la Entidad de Tecnología e Informática (Dirección de Informática, División de Informática, Departamento de Informática, o el que aplique en la Institución), en lo sucesivo se denominará "ETI".

Introducción

La tecnología informática (TI) contribuye a superar los niveles de productividad y eficiencia de la Institución, siendo la "ETI", 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 "ETI", 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.

Políticas generales de Hardware y Software

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

Es total responsabilidad y obligación del usuario lo siguiente:

- Dar cumplimiento a todas las normas y políticas vigentes.
- Preservar el estado de los equipos, manuales y cualquier otro elemento de soporte que se le entregue.
- Utilizar adecuadamente el software que se le ha autorizado e instalado.
- Preservar la veracidad de los datos en los sistemas a que se le de acceso.
- Informar a la "ETI", cualquier cambio relacionado al hardware y/o software:
  - 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 "ETI", 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.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

1

- Utilizar su contraseña y password con total discreción, ya que el usuario es el único responsable del estado o contenido de los registros de cualquier sistema, donde sea evidente (utilizando para ello cualquier método de seguimiento de auditoría) el acceso al registro por medio del código relacionado a su usuario.

Es responsabilidad de la "ETI", velar por el buen funcionamiento de los servicios de tecnología e informática que se presten dentro de la Institución; así como, brindar a los usuarios el soporte técnico necesario.

Solicitudes de adquisición de equipos

- Todas las solicitudes para la asignación de cualquier equipo de cómputo (impresoras, scanner, monitores, etc.) deben ser enviadas a la "ETI", quien determinará los planes y prioridad para el equipamiento computacional, dependiendo de las necesidades y requerimientos de la División, Departamento u Oficina solicitante.

  Si la "ETI" considerara a lugar la solicitud, pero no existiere el bien solicitado dentro del inventario 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 "ETI" defina y además cumplir con todos los procedimientos legales, presupuestarios o cualquier otro que la Institución establezca.

- La "ETI" evaluará y determinará los costos y beneficios que el solicitante incluya en el proyecto que respalda su pedido.

- La "ETI" tiene la responsabilidad de instalar los equipos de cómputo y la realización de pruebas técnicas.

Normas generales en el uso de Software y Hardware

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 tecnología de información, aumentando así la productividad de ambos.

Estas normas deben ser conocidas y respetadas por todos. 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.

Normas generales en el uso de Hardware

- La "ETI" es la única autorizada para:
  - Efectuar mantenimientos preventivos y/o correctivos en los equipos.
  - Instalar software y sistemas que los usuarios requieran.
  - Solo se le dará mantenimiento a los equipos que pertenezcan a la Institución y estén debidamente identificados con su respectivo número de inventario.

- Los usuarios deberán cuidar física y lógicamente los recursos computacionales existentes, pensando que estos están al servicio de todos.

- En ningún momento deberá manipularse alimentos o bebidas cerca o sobre los equipos computacionales, ya que cualquier derrame podrá causar daños al mismo.

- No está permitida la utilización de los equipos con fines recreativos ni con fines particulares.

- El usuario en lo posible debe mantener la limpieza externa de los equipos.

- El usuario no deberá abrir los equipos de cómputo, como tampoco sacar o cambiar componentes de los equipos.

- Evitar prestar o intercambiar los equipos de cómputo.

- En ningún momento se deberán instalar equipos o periféricos que de alguna manera interactúen con la infraestructura o equipos de tecnología e informática de la Institución, sin la supervisión y autorización de la "ETI".

Normas generales Software

- 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 "ETI".

- Cualquier otro software que requiera el usuario, deberá ser solicitado a la "ETI" por medio de solicitud escrita o, si la Institución tuviere un formulario diseñado para el efecto, este será el único documento válido de solicitud.

  En cualquiera de las formas utilizadas, la solicitud como mínimo deberá incluir:
  - Nombre completo del usuario;
  - Oficina o Departamento donde labora;
  - Puesto que desempeña;
  - Justificación válida y que relacione el desempeño de las actividades laborales del usuario;
  - Visto bueno, firma y sello del Jefe inmediato o en su defecto por la Autoridad Superior.

  Toda solicitud ingresada a la "ETI", 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.

  Si la "ETI" 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 "ETI" defina y además cumplir con todos los procedimientos legales, presupuestarios o cualquier otro que la Institución establezca.

- Toda solicitud de algún software aplicativo deberá hacerce por escrito a la jefatura de la "ETI", por medio de la jefatura interesada. Será la "ETI", quien determine los planes y prioridad; así como también si el desarrollo se haga interno u outsourcing.

- 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.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

- La instalación y pruebas técnicas de software y/o sistemas solo podrán ser efectuadas por la "ETI".

- 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 "ETI" si corresponde.

- Toda instalación de software y/o sistema no autorizado por la "ETI", que provoque el inadecuado funcionamiento del equipo o de aplicaciones autorizadas, será total responsabilidad del usuario.

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

Prohibiciones para los Usuarios

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

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

- Instalación y uso de software de juegos.

- Cambiar la configuración de los equipos, que ha sido determinada por la "ETI".

- 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 "ETI".

- Instalar software no autorizado por la "ETI", 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, adware 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 Institución.

- Realizar la actualización a nuevas versiones de software sin la autorización expresa de la "ETI".

- 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.

Sanciones

Cualquier quebranto a las normas o políticas establecidas en el presente documento será motivo de sanción administrativa, por lo que es obligación de la "ETI", elaborar los informes correspondientes a la Jefatura 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.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

Ministerio de Comunicaciones, Infraestructura y Vivienda

Políticas del servicio de navegación por Internet

Preliminares

Para efectos del presente documento, al Ente de Tecnología e Informática (Dirección de Informática, División de Informática, Departamento de Informática, o el que aplique en la Institución), en lo sucesivo se denominará "ETI".

Objetivos

1. Definir las características del correcto uso del servicio de acceso a Internet.

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

Políticas del servicio

La Institución, a través de la "ETI", podrá proveer a sus colaboradores de cuentas de acceso a Internet, con el objeto de darles apoyo en su trabajo diario en las labores de investigación. Dichas cuentas de acceso a Internet están asignadas a los colaboradores pero son constantemente monitoreadas por la "ETI".

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

1) Acceso a los servicios

La utilización de los recursos de red y de información está abierta a todas las divisiones, departamentos u oficinas de la Institución bajo las políticas de acceso definidas en el contexto del presente documento y a otras personas a las que la Institución desee extender los privilegios de acceso, dadas las condiciones de disponibilidad de recursos , servicios y aprobación por escrito de la Autoridad Superior.

2) Responsabilidad

Cada empleado de la Institución es el único responsable de las actividades realizadas en la navegación en Internet con su usuario de acceso.

Los lugares o sitios que se visiten en Internet, serán de completa responsabilidad del usuario y en todo caso deberán basarse en la racionalidad y la responsabilidad individual. Se asume que en ningún momento dichos lugares atenten contra la moral ni en contra de los intereses de personas individuales, los de nuestra Institución, así como de ninguna otra Institución.

3) Uso del servicio

La Institución no garantiza la privacidad de la información transmitida desde y hacia Internet por medio de los navegadores a excepción de la que sea transmitida por HTTPS, protocolo que debe ser utilizado por el sitio visitado.

Se hace del conocimiento que se lleva una bitácora de todos lo 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.

4) Solicitud de creación de cuentas de acceso a Internet

El servicio de navegación por Internet será limitado para el personal que por la naturaleza de su puesto necesite de este servicio. La solicitud de creación de cuentas de acceso a Internet deberá hacerse a la "ETI" por escrito o si la Institución tuviere formulario diseñado para el efecto, este será el único documento válido de solicitud para la creación de cuentas de navegación en el Internet.

En cualquiera de las formas utilizadas, la solicitud como mínimo deberá incluir:

- Nombre completo del usuario;
- División, Departamento u Oficina donde labore;
- Puesto que desempeña;
- Justificación válida y que relacione el desempeño de las actividades del usuario de la cuenta;
- Visto bueno, firma y sello del jefe de la División, Departamento u Oficina.

La "ETI", gestionará ante la Autoridad Superior de la Institución la autorización final del servicio.

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

5) Prohibiciones al uso de la navegación en el Internet

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:

- Visitar páginas con contenido pornográfico, sexo explícito, juegos y violencia.

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

- Visitar páginas con servicios de chateo, audiocomferencia o videoconferencia, a menos que por la naturaleza de sus funciones laborales, sea justificado y aprobado por escrito por la Autoridad Superior.
- Bajar 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.
- 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.
- Visitar y utilizar páginas con servicio de correo electrónico (hotmail, yahoo, otros), siempre que la Institución le provea al usuario de una cuenta de correo electrónico.

6) 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:

- 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 "ETI" y del Jefe inmediato, para el cual trabaje el colaborador o en su defecto, la Autoridad Superior.

- Queda prohibido visitar cualquier sitio en Internet que atente la moral y vayan en contra de las buenas costumbres y/o afecte terceros.

- 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 para "Hacking").

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

- Utilizar el Internet para perder deliberadamente el tiempo, visitando portales que no provean información útil para el desarrollo de sus actividades diarias.

7) 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.

- 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..).

MINISTERIO DE COMUNICACIONES, INFRAESTRUCTURA Y VIVIENDA - GUATEMALA, C. A.

- Las Autoridades Superiores de la Institución están facultadas para solicitar a la "ETI", en base a una investigación oficial, el despliegue del contenido de las bitácoras relacionadas al uso del servicio de Internet por usuario.

- La "ETI", está facultada para generar los informes relacionados al uso por usuario de este servicio, a solicitud de los Jefes de División, Departamento u Oficina, que permita monitorear la utilización de este servicio.

- La "ETI", 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.

8) Sanciones

Cualquier quebranto o violación de las normas y/o políticas establecidas en el presente documento, será motivo de sanción, que implicará la suspención inmediata del acceso a este servicio y reporte a RRHH.

La cancelación parcial o definitiva del acceso a este servicio será a criterio de las Autoridades Superiores, por lo que cualquier reactivación deberá solicitarse por escrito a la "ETI", con visto bueno, firma y sello de las Autoridades Superiores.

Alfredo Estuardo Mury Aguirre
VICEMINISTRO DE COMUNICACIONES,
INFRAESTRUCTURA Y VIVIENDA