BACHILLERATO DEL ESTADO DE HIDALGO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

LINEAMIENTOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Dirección de Planeación
Subdirección de Tecnologías de Información y Comunicación

Objetivo:

Asegurar la regulación, seguridad, eficiencia, y transparencia en las instituciones públicas, contribuyendo así a un mejor servicio a la ciudadanía y a la protección de la información pública.

Dirección de Planeación
Subdirección de Tecnologías de Información y Comunicación

ÍNDICE

Glosario	2
Mesa de servicio	*8*
Administración del servicio de internet	9
Administración de la página web	11
Mantenimiento a los sistemas internos	12
Soporte técnico al equipo de cómputo	12
Estándares de seguridad informática para usuarios	14
Estándares de seguridad física y ambiental	16
Estándares de seguridad y administración de operaciones de cómputo	18
Estándares de controles de acceso lógico	23
Estándares de cumplimiento de seguridad informática	26
Asignación de bienes informáticos de cómputo personal, y periféricos	27
De la seguridad a los sistemas informáticos y de comunicaciones	31
Transitorios	34

1. GLOSARIO

El presente ordenamiento tiene por objeto establecer los lineamientos generales para las acciones y alcances de las responsabilidades en materia de tecnología de la información y comunicación, que apliquen al Bachillerato del Estado de Hidalgo.

Para efectos de estos lineamientos se entenderá por:

Acceso. Tipo específico de interacción entre un sujeto y un objeto que resulta en el flujo de información de uno a otro. Es el privilegio de un sujeto para utilizar un objeto.
Acceso físico. Entrada o paso por donde se entra o se llega a un sitio dentro de la institución.
Acceso lógico. Es la habilidad de comunicarse y conectarse a un activo tecnológico para utilizarlo, o bien usar su información.
Acceso remoto. Conexión de dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación ya sean telefónicas o por medio de redes de área amplia que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Aplicación. Acción que se realiza a través de un programa de manera directa con el usuario. Navegadores, Chat, correo electrónico, etc. son algunos ejemplos de aplicaciones en el medio de Internet.
Antivirus. Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un equipo o dispositivo.
Ataque. Actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a ese activo y lograr afectarlo.
Archivo. Una colección identificada de registros relacionados.
Autorización. Es el proceso de asignar a los usuarios permisos para realizar actividades de acuerdo a su perfil o puesto.
Archivos ejecutables. Es un archivo binario cuyo contenido se interpreta por el ordenador como un programa.
Generalmente, contiene instrucciones en código máquina de un procesador en concreto, pero también puede contener bytecode que requiera un intérprete para ejecutarlo. Además, suele contener llamadas a funciones específicas de un sistema operativo (llamadas al sistema).
Base de datos. Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
CD Medio de almacenamiento de información.
Código malicioso. Hardware, software ·o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un caballo de Troya es ejemplo de un código malicioso.
Comprimir (rar). Reducir el tamaño de los archivos sin que éstos pierdan nada de su información. Rar es el nombre de la extensión que contiene un archivo comprimido.

Computadora. Es un conjunto de dispositivos electrónicos que forman una máquina electrónica capaz de procesar información siguiendo instrucciones almacenadas en programas.
Confidencialidad. Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.
Control de acceso. Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.
Copyright. Derecho que tiene un autor, incluido el autor de un programa informático, sobre todas y cada una de sus obras y que le permite decidir en qué condiciones han de ser éstas reproducidas y distribuidas. Aunque este derecho es legalmente irrenunciable puede ser ejercido de forma tan restrictiva o tan generosa como el autor decida. El símbolo de este derecho es ©.
Correo electrónico o e-mail. La funcionalidad es similar a usar el correo normal, pero ahora el individuo puede utilizar una computadora y un software para enviar mensajes o paquetes a otro individuo o grupo de personas a una dirección específica a través de la red o Internet.
Cuentas de usuario. Es un identificador el cual es asignado a un usuario del sistema para el acceso y uso de la computadora, sistemas, aplicaciones, red, etc.
Clonado. Imagen en medio electrónico que contiene el sistema operativo, cliente de base de datos y componentes de aplicaciones que conforman el ambiente estándar de un equipo de cómputo personal por marca y modelo.
Descargar. Acción de transferir información computarizada de una computadora a otra.
Descomprimir. Acción que se lleva a cabo después de haber comprimido un archivo para regresarlo a su estado original.
Discos ópticos. Los discos ópticos son medios de almacenamiento de información que presentan una capa interna protegida, donde se guardan los bits mediante el uso de un rayo láser éste al ser reflejado, permite detectar variaciones microscópicas de propiedades "óptico-reflectivas" ocurridas como consecuencia de la grabación realizada en la escritura. Un sistema óptico con lentes encamina el haz luminoso, y lo enfoca como un punto en la capa del disco que almacena los datos.
Disponibilidad. Se refiere a que la información esté disponible en el momento que se requiera.
Dominio. Sistema de denominación de host en Internet. Conjunto de caracteres que identifica y diferencian los diferentes sitios Web.
DVD. Medio de almacenamiento de información.
Encargado de Inventario. Persona responsable de llevar el inventario del cómputo de las oficinas centrales y planteles.
Personal soporte técnico. Persona responsable de llevar el control de los periféricos adquiridos para el buen funcionamiento de los equipos de cómputo.
Encriptación. Proceso matemático donde los datos de un mensaje, por seguridad, son codificados para protegerlos de accesos no deseados. El término encriptación como tal, no existe en el lenguaje español, el término correcto es cifrado de datos. Encriptada Referirse a Encriptación.

Estándar. Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.
Estándares de software. Sistema Operativo Windows, Suite de Office, Antivirus, Docuware, Programas de diseño.
Extensión. Número interno de comunicación, que cuenta o no con la capacidad de hacer llamadas al exterior y cuyas llamadas desde el exterior invariablemente pasan por la operadora.
Estándares de equipo de computo. Monitor, Teclado, Mouse en algunos casos módems cuando así lo requieran.
Falta administrativa. Es falta administrativa todo acto u omisión del funcionario, intencional o culposo, que viole los deberes funcionales.
Freeware (Software Libre). Programas que se pueden bajar desde Internet sin cargo.
FTP. Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
Firewall. Es un dispositivo que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a la otra. Un uso típico es situarlo entre una red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial. Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.
Gusano. Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red, antes de su llegada al nuevo sistema, el gusano debe estar activado para replicarse y propagarse nuevamente, además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.
Hardware. Se refiere a las características técnicas y físicas de las computadoras.
Help Desk1 CAU. Soporte técnico brindado a los usuarios telefónicamente, su función es proveer conocimientos especializados de los sistemas de producción para identificar y asistir en el ámbito de desarrollo de sistemas y en la resolución de problemas.
Herramientas de seguridad. Son mecanismos de seguridad automatizados que sirven para proteger o salvaguardar a la infraestructura tecnológica de una Comisión.
Impacto. Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza.
Incidente de seguridad. Cualquier evento que represente un riesgo para la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada en el desempeño de nuestra función.

Integridad. Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.

Internet o world wide web (www). Es un sistema a nivel mundial de computadoras conectadas a una misma red, conocida como la red de redes en donde cualquier usuario consulta información de otra computadora conectada a esta red e incluso sin tener permisos necesarios acceder a dichos activos.

Intrusión. Es la acción de introducirse o acceder sin autorización a un activo tecnológico.

Lenguaje de programación. Sistema de escritura para la descripción precisa de algoritmos o programas informáticos.

Maltrato, descuido o negligencia. Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia daña los recursos tecnológicos propiedad del BACHILLERATO DEL ESTADO DE HIDALGO.

Mecanismos de seguridad o de control. Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. Que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.

Metodología. Es un conjunto de procedimientos ordenados y documentados que son diseñados para alcanzar un objetivo en particular y comúnmente son divididos en fases o etapas de trabajo previamente definidas.

"Necesidad de saber", principio o base. Es un principio o base de seguridad que declara que los usuarios deben tener exclusivamente acceso a la información, instalaciones o recursos tecnológicos de información entre otros que necesitan para realizar o completar su trabajo cumpliendo con sus roles y responsabilidades dentro de la Comisión.

Nodo. Punto principal en el cual se les da acceso a una red a las terminales o computadoras.

Normatividad. Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.

Obsolescencia tecnológica. Descarte o desuso de máquinas, dispositivos y tecnología en general.

Una tecnología obsoleta es cualquier tecnología que ya no se emplea o ha sido reemplazada por otra tecnología (que puede o no ser tecnología de punta).

Razones por las cuales una tecnología puede pasar a la obsolescencia:

- Mal desempeño comparado a las nuevas tecnologías.
- Imposibilidad de encontrar los repuestos adecuados.
- Nuevas tecnologías que reemplazan la antigua (tecnologías sustitutivas).
- Dos o más tecnologías salidas en una época determinada y que compiten entre sí, pero donde una termina superando a las otras.
- Estrategias comerciales.

Problemas con la tecnología obsoleta. El principal problema con la tecnología obsoleta está en la basura y contaminación que la acumulación de estas puede producir.

Una de las soluciones típicas es el reciclaje de esta tecnología antigua, pero muchas veces no está bien implementada o no se hace.

Página Web. Ver sitio Web.

Parche (patch). Un parche (algunas veces llamado Fix) son piezas de programación que representan una solución rápida al software o sistema, para incrementar la seguridad o incrementar la funcionalidad del mismo.
Password Contraseña. Secuencia de caracteres utilizados para determinar que un usuario específico requiere acceso a una computadora personal, sistema, aplicación o red en particular. Típicamente está compuesto de 6-10 caracteres alfanuméricos.
Periféricos. Se entiende como periféricos los aparatos auxiliares que se conectan a la unidad central de una computadora tales como: CD Writer, Impresoras, Digitalizadores, entre otros.
Respaldo. Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida,si los originales se destruyen o quedan fuera de servicio.
Riesgo. Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.
Servidor. Computadora que responde peticiones o comandos de una computadora cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.
Sitio Web. El sitio Web es un lugar virtual en el ambiente de Internet, el cual proporciona información diversa para el interés del público, donde los usuarios deben proporcionar la dirección de dicho lugar para llegar a él.
Sistema interno. Conjunto de medios que permiten recolectar, clasificar, integrar, procesar, almacenar y difundir información interna y externa que la organización necesita para tomar decisiones en forma eficiente y eficaz.
Software. Programas y documentación de respaldo que permite y facilita el uso de la computadora. El software controla la operación del hardware.
Software antivirus. Aplicaciones que detectan, evitan y posiblemente eliminan todos los virus conocidos, de los archivos ubicados en el disco duro y en la memoria de las computadoras.
Switch. Dispositivo de red que filtra y direcciona paquetes a las direcciones destinatarias. El switch opera en la capa de enlace de datos del modelo OSI.
Tarjeta inteligente. Es una tarjeta de plástico del tamaño de una tarjeta de crédito, que incorpora un microchip, en el cual se puede cargar datos como números telefónicos anteriormente llamados, pagos realizados a través de medios electrónicos y otro tipo de aplicaciones, las cuales pueden ser actualizadas para usos adicionales.
Telefonía. Servicio para proveer la comunicación electrónica a través de teléfonos de escritorio. No incluye servicios de Telefonía Celular.
Tecnología de información. Se ocupa del uso de las computadoras y su software para convertir, almacenar, proteger, procesar, transmitir y recuperar la información.
USB. Siglas de " Universal Serial Bus"

.

User-ID (identificación de usuario). Se denomina al nombre de usuario con el cual accedemos a una página o sistema en el que previamente nos hemos registrado. Este nombre puede estar compuesto de letras, números o signos.
Usuario. Este término es utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo (hardware).
Virus. Programas o códigos maliciosos diseñados para esparcirse y copiarse de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos de computadoras.
Vulnerabilidad. Es una debilidad de seguridad o hueco de seguridad, el cual indica que el activo es susceptible a recibir un daño a través de un ataque, ya sea intencionado o accidental.
.

2. MESA DE SERVICIO

La mesa de servicio proporciona un único punto de contacto para todos los usuarios del Bachillerato del Estado de Hidalgo que requieren de servicios relacionados con las Tecnologías de la Información.

El propósito de la Mesa de Servicio es solucionar problemas o para orientar acerca del hardware (computadoras personales, impresoras), redes o software.

2.1 Servicios que atiende

a) Seguridad (Administración de fírewall, Antivirus, Sistemas Operativos y Respaldos)
b) Cómputo Central y Distribuido (Administración de Servidores)
c) Cómputo de Usuario Final (Mantenimiento a Hardware)
d) Redes
e) Colaboración y Correo Electrónico (Mantenimiento, altas y bajas)
f) Internet e Intranet (Nuevo contenido y cambios)
g) Aplicativos
h) Software Interno (Sistemas administrativos y sustantivos que operan en el Organismo)
i) Software Externo (Aplicaciones comerciales que se utilizan en la Institución como Word, Excel, etc.)
j) Base de Datos (Exportación de datos de software interno para su uso en software externo, actualizaciones o consultas)

Los servicios de tecnologías de la información y comunicación pueden ser solicitados vía telefónica a través de la ext. 223 para levantar el reporte o a través del formulario de google forms previsto para tal efecto.

2.2. Control de Refacciones

El personal del Departamento de Soporte Técnico deberá seguir el procedimiento para solicitar refacciones a la Dirección de Administración con el debido formato para dar cumplimiento con los objetivos del mismo.

3. ADMINISTRACIÓN DEL SERVICIO DE INTERNET

El servicio de internet se proporcionará a los usuarios tomando en consideración los tipos de acceso que se describen a continuación.

Tipo de Acceso		Usuarios	Quién Autoriza
3.1	Acceso Total Acceso a todos los servicios de internet	Para mandos medios, superior y personal de la Subdirección de informática	Director General
3.2	Acceso limitado De acuerdo a sus funciones, se dará el acceso únicamente a las páginas que se soliciten.	A todo el personal de Dirección General que lo requiera de acuerdo a sus funciones.	Director de Área
3.3	Acceso a servicios de gobierno, Acceso a páginas WEB de Gobierno Estatal y Federal.	A todo el personal de Dirección General que lo requiera de acuerdo a sus funciones.	Director de Área
3.4	Acceso Denegado, únicamente se proporcionael servicio de correo institucional	A todo el personal deDirección General quelo requiera de acuerdo a sus funciones.	Director de Área

No está permitido utilizar el servicio de internet para obtener archivos ejecutables, videos y música en todos sus formatos.

La cuentade correo se integra de la siguiente manera:

a) Departamento
b) @
c) Dominio: bachillerato-hgo.edu.mx

La información publicada en la página web será responsabilidad única y exclusivamente del área que solicite su incorporación, modificación y/o actualización, sin embargo, será responsabilidad de la Subdirecció Adjunta de Diseño y Desarrollo de Sistemas que la misma se encuentre en funcionamiento permanente, realizando las actualizaciones y modificaciones que se requieran, en cumplimiento a la normatividad aplicable.

El acceso se le proporcionará a todo el personal de Dirección General que así lo requiera de acuerdo a sus funciones, únicamente se deberá emitir una solicitud a través de la herramienta correspondiente con los siguientes datos:

Usuario responsable del equipo al que se le va a dar el acceso.

1) Tiempo requerido del servicio.
2) Indicar el acceso que se requiere, de acuerdo a la clasificación establecida.
3) Si el acceso es limitado deberá mencionar las páginas que requieran.
4) Dirigido al Subdirección de TIC´s.
5) Firmado por el jefe inmediato superior.
6) Vo. Bo.del Directorde Área.
7) Para el acceso denegado (correo electrónico de la entidad), se requiere un password, integrado por 8 caracteres fáciles de recordar por el usuario.

Se realiza permanentemente monitoreo al acceso a internet en Dirección General, a través del Firewall, el cual identifica el contenido de las páginas que se visitan en la red, bloqueando el servicio automáticamente en el momento en que se detecta el acceso a páginas con contenido no relacionado a las actividades de esta institución.

Bloqueo: El servicio de Internet será bloqueado y se emitirá una notificación al usuario, con copia al superior jerárquico para su conocimiento.

Para la reactivación del acceso, se observará el siguiente esquema de atención:

a) Primera ocasión

Se le informa al usuario el motivo por el cual se bloqueó el servicio y se reactiva al día siguiente hábil de la notificación.

b) Segunda ocasión:

Elaborar oficio dirigido a la Subdirección de TIC’s, con una copia a la Dirección de Planeación, indicando la siguiente leyenda "solicitud de reactivación del servicio de internet, por accesar a páginas con contenido no relacionado a las actividades de esta institución", firmado por el jefe inmediato superior.

c) Tercera ocasión

Elaborar oficio dirigido al Director General, con una copia a la Dirección de Planeación y Subdirección de TIC’s, indicando lo siguiente "solicitud de reactivación del servicio de internet, por accesar a páginas de contenido no relacionado a las actividades de esta institución, por tercera ocasión", firmado por el Director de Área correspondiente.

4. ADMINISTRACIÓN DE LA PÁGINA WEB

4.1. Para la página WEB

La Subdirección Adjunta de Soporte Técnico es el encargado de incorporar la información que las diversas áreas administrativas requieran publicar, con el objetivo de mantener informados a nuestros usuarios y público en general sobre servicios trámites y el quehacer del Bachillerato del Estado de Hidalgo.

Toda Solicitud de integración de información, será a través de la herramienta de Google Forms con las siguientes características:

La información a publicar se describirá en la misma solicitud de servicio.

La información deberá enviarse con los mismos formatos que las áreas establecieron para su publicación.

La Subdirección Adjunta de Soporte Técnico, no está facultado para hacer ningún cambio y/o cálculo matemático de los datos que se emitieron para integrarlos a la página WEB, pero si es responsable por dar cumplimiento a la normatividad en materia de operación e imagen institucional.

5. MANTENIMIENTO A LOS SISTEMAS INTERNOS

La Subdirección Adjunta de Diseño y Desarrollo de Sistemas es el responsable del buen funcionamiento de los programas que integran los sistemas del Organismo y de resguardar la información que almacenan en el sistema.

Las áreas que utilizan los sistemas internos del Bachillerato del Estado de Hidalgo, son las responsables de la información que almacenan en el sistema.

Cualquier modificación y/o cambio requerido por las áreas usuarias, deberá especificarse en la solicitud de servicio correspondiente en la herramienta de Google Forms, con la siguiente indicación:

Detalle de la modificación solicitada.

Cualquier modificación contenida en las tablas de la base de datos, será responsabilidad única y exclusivamente del área que solicite el cambio, eliminación o adición.

El área de sistemas funge únicamente como facilitador para llevar a cabo la modificación.

Se realizarán respaldos de las tablas de las bases de datos cada viernes, a partir de las 3 de la tarde.

La Subdirección Adjunta de Sistemas es la encargada de analizar y realizar las modificaciones solicitadas.

6. SOPORTE TÉCNICO AL EQUIPO DE CÓMPUTO

El equipo de cómputo propiedad del Bachillerato del Estado de Hidalgo, será destinado única y exclusivamente para la realización de las funciones propias de la institución.

El equipo de cómputo no deberá ser operado mientras se consuman alimentos o bebidas.

El equipo de cómputo debe estar conectado preferentemente a una conexión de corriente regulada o sistema de energía interrumpible (no-break) en caso de contar con el dispositivo.

Cuando el equipo de cómputo no se utilice durante un periodo prolongado (hora de comida, finalización de labores, etc.) deberá permanecer completamente apagado en apoyo al plan de ahorro de energía.

El orden de encendido del equipo de cómputo será el siguiente; regulador (en caso de existir), monitor, CPU, equipo periférico e impresora; y deberá apagarse en el orden inverso.

Se deberá mantener alejadas del equipo de cómputo fuentes de campos magnéticos tales como celulares o imanes.

El responsable del equipo de cómputo será aquel que firme el resguardo emitido por la Subdirección Adjunta de Recursos Materiales y estará bajo su responsabilidad el equipo y los programas autorizados instalados en el mismo.

Queda estrictamente prohibida la instalación de programas de cómputo (Software sin licencia en los equipos de cómputo de la institución).

El resguardante del equipo de cómputo será el responsable de los respaldos de su información. En aquellas unidades administrativas de la Institución, donde exista mayor carga de trabajo, los respaldos deberán hacerse con mayor frecuencia. Dichos respaldos deberán almacenarse en un lugar seguro a fin de prever cualquier circunstancia que se presente.

El cambio de ubicación de equipo de cómputo ya sea entre usuarios de la misma unidad, como de una unidad administrativa a otra, deberá ser notificado, con oportunidad, a la Subdirección de TIC’s mediante oficio o correo electrónico indicando con precisión marca, modelo, número de inventario y serie, turnando copia a la Subdirección Adjunta de Recursos Materiales.

La Subdirección Adjunta de Recursos Materiales, se encargará de reubicar el equipo para que personal de la Subdirección de TIC’s proceda a su conexión y, en su caso, se solicite la instalación de conexiones de corriente regulada y prevea la conexión de red.

La Subdirección Adjunta de Soporte Técnico, deberá proporcionar la asesoría y el apoyo técnico que requieran las unidades administrativas, para la operación del equipo de cómputo.

El horario de atención para recibir y atender los reportes será de las 08:30 a las 16:30 hrs. El personal la Subdirección Adjunta de Soporte Técnico deberá explicar claramente al usuario el motivo de la falla.

Derivado de la falla detectada el personal de la Subdirección Adjunta de Soporte Técnico deberá realizar, en su caso, el cambio de la pieza en mal estado de acuerdo al inventario existente y a los tiempos establecidos en el procedimiento para la compra del material de equipo de cómputo, el equipo se trasladará a la Subdirección mencionada, dejando al usuario responsable el Formato de reporte de reparación de equipo original.

Si la falla detectada contempla una reparación mayor de 48 hrs. la subdirección adjunta de Soporte Técnico deberá proporcionar un dispositivo de respaldo, de acuerdo al stock existente.

La Subdirección Adjunta de Soporte Técnico resolverá claramente todas las dudas que el usuario tenga relacionado con el software.

7. ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

Todo usuario de bienes y servicios informáticos deben de firmar un convenio en el que acepte las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del Bachillerato del Estado de Hidalgo, así como el estricto apego al presente Lineamiento de Tecnologías de la Información y Comunicación.

Los usuarios deberán cumplir con lo establecido en los Lineamientos de los Procesos de Tecnologías de la Información y Comunicación.

7.1.1. Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir los Lineamientos de los Procesos de Tecnologías de la Información y Comunicación.

7.1.2. Acuerdos de uso y confidencialidad

Todos los usuarios de bienes y servicios informáticos del Bachillerato del Estado de Hidalgo deberán hacer el uso adecuado de los recursos informáticos y de información del Organismo, así como comprometerse a cumplir con lo establecido con el presente lineamiento.

7.1.3. Entrenamiento en seguridad informática

Todo empleado del Bachillerato del Estado de Hidalgo de nuevo ingreso deberá de contar con la inducción sobre el Lineamientos de Tecnologías de la Información y Comunicación, a través de la Subdirección Administrativa donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

7.1.4. Medidas disciplinarias

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial del Bachillerato del Estado de Hidalgo, o de que se le declare culpable de un delito informático.

Los delitos informáticos son aquellas actividades ilícitas que:

Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito).

Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos.

También se puede definir al delito informático como la conducta típica, antijurídica, culpable y punible, en que se tiene a las computadoras como instrumento o fin.

7.2. ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de acceso físico para el personal y terceros deben controlar el acceso a las instalaciones y áreas restringidas (Subdirecciones Adjuntas de Diseño Desarrollo de Sistemas, Soporte Técnico y lugares donde por su naturaleza se maneje información importante).

7.2.1. Resguardo y protección de la información

El usuario deberá reportar de forma inmediata a la Subdirección de TIC's, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

El usuario tiene la obligación de proteger los discos que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad del usuario evitar en todo momento la fuga de la información del Organismos que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

7.2.2. Controles de acceso físico

Cualquier persona que tenga acceso a las instalaciones del Bachillerato del Estado deHidalgo, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del Organismo, el cual podrán retirar el mismo día.

Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá salir de las instalaciones del Bachillerato del Estado de Hidalgo únicamente con la autorización de salida del Departamento de Recursos Materiales.

7.2.3. Seguridad en áreas de trabajo

El área de servidores del Bachillerato del Estado de Hidalgo es restringida, por lo que sólo el personal autorizado por la Subdirección de TIC's puede acceder a él.

7.2.4. Protección y ubicación de los equipos

Los usuarios no deben mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Subdirección de TIC's, en caso de requerir este servicio deberá solicitarlo a esta subdirección..

La Subdirección Adjunta de Recursos Materiales, será la encargado de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Subdirección de TIC's.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del Bachillerato del Estado de Hidalgo.

Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Es responsabilidad de los usuarios almacenar su información únicamente en la partición de disco duro identificada como "Mis documentos" o similares, ya que las otras están destinadas para archivos de programa y sistema operativo.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos

Se debe evitar colocar objetos encima del equipoo cubrir los orificios de ventilación del monitor o del CPU.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Subdirección de TIC's a través de un plan detallado de movimientos debidamente autorizados por el Director del Área que corresponda.

Queda prohibido que el usuario abra o desarme los equipos de cómputo.

7.2.5. Mantenimiento de equipo

Únicamente el personal autorizado por la Subdirección de TIC's podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

7.2.6. Pérdida de equipo

El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia durante el horario de labores; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El resguardo para las laptops, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.

El usuario deberá dar aviso inmediato a la Subdirección de TIC's y Subdirección Adjunta de Recursos Materiales de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

7.2.7. Uso de dispositivos especiales

Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por su Director de Área.

7.2.8. Daño del equipo

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la Subdirección Adjunta de Soporte Técnico determinará la causa de dicha descompostura.

7.3. ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica de la Subdirección de TIC's. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del Bachillerato del Estado de Hidalgo o hacia redes externas como Internet.

Los usuarios del Bachillerato del Estado de Hidalgo que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

7.3.1. Uso de medios de almacenamiento

Toda solicitud para utilizar un medio de almacenamiento de información compartido (File Share), deberá contar con la autorización del área dueña de la información. El personal que requiera estos medios debe justificar su utilización. Dicha justificación deberá de presentarla a la Subdirección de TIC's firmada por su Director de área de adscripción.

Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras personales o estaciones de trabajo.

Los usuarios de informática del Bachillerato del Estado de Hidalgo deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

7.3.2. Instalación de software

Los usuarios que requieran la instalación de software que no sea propiedad del Bachillerato del Estado de Hidalgo, deberán justificar su uso y solicitar su autorización a la Subdirección de TIC's, a través de un oficio firmado por su Dirección de adscripción, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

7.3.3. Identificación del incidente

El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidentede seguridad informática deberá reportarlo a la mesa de servicio lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas y de acuerdo con la gravedad notifique a la Subdirección de Asuntos Jurídicos y Normatividad, para el ejercicio de las acciones legales procedentes.

Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del Bachillerato del Estado de Hidalgo debe ser reportado a la Subdirección de TIC's.

7.3.4. Administración de la configuración

Los usuarios de las áreas del Bachillerato del Estado de Hidalgo no deben establecer conexiones remotas a redes internas o externas, intercambio de información con otrosequipos de cómputoutilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Bachillerato del Estado de Hidalgo, sin la autorización de la Subdirección de TIC's.

7.3.5. Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Subdirección de TIC's, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del Bachillerato del Estado de Hidalgo, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

7.3.6. Uso del Correo electrónico

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Bachillerato del Estado de Hidalgo, a menos que cuente con la autorización de la Dirección de adscripción.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información propiedad del Bachillerato del Estado de Hidalgo. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

El Bachillerato del Estado de Hidalgo se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática del Bachillerato del Estado de Hidalgo o realizado acciones no autorizadas.

El usuario debe de utilizar el correo electrónico del Bachillerato del Estado de Hidalgo única y exclusivamente a los recursos que tenga asignados y las facultades que les hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.

La asignación de una cuenta de correo electrónico institucional, deberá solicitarse por escrito a la Subdirección de TIC's, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director del área que corresponda.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

7.3.7. Controles contra código malicioso

Para prevenir infecciones por virus informático, los usuarios del Bachillerato del Estado de Hidalgo no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Subdirección de TIC's.

Los usuarios del Bachillerato del Estado de Hidalgo deben verificar que la información y los medios de almacenamiento, considerando al menos discos externos y USB, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutarel software antivirus autorizado por la Subdirección de TIC's.

Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Ningún usuario del Bachillerato del Estado de Hidalgo debe intencionalmente escribir generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas del Bachillerato del Estado de Hidalgo. El incumplimiento de este estándar será considerado una falta grave.

Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Subdirección Adjunta de Análisis y Desarrollo de Sistemas.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Subdirección de TIC's para la detección y erradicación del virus.

Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar a la Subdirección de TIC's periódicamente las actualizaciones del software antivirus.

Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el la Subdirección de TIC's en: antivirus, correo electrónico, office, navegadores u otros programas.

Debido a que algunos virus son extremadamente complejos, ningún usuario del Bachillerato del Estado de Hidalgo debe intentar erradicarlos de las computadoras.

7.3.8. Internet

El acceso a Internet provisto a los usuarios del Bachillerato del Estado de Hidalgo es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

La asignación del servicio de Internet, deberá solicitarse por escrito mediante correo electrónico a la Subdirección de TIC's, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno de la Dirección de área correspondiente.

Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Bachillerato del Estado de Hidalgo.

Los usuarios de Internet del Bachillerato del Estado de Hidalgo tienen que reportar todos los incidentes de seguridad informática a la Subdirección de TIC's inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:

1. Serán sujetosde monitoreo de las actividades que realiza en Internet.
2. Saben que existe la prohibición al acceso de páginas no autorizadas.
2.1. Páginas de Juegos
2.2. Página de Apuestas
2.3. Páginas de Contenido de Adultos
2.4. Páginas de descargas de archivos
2.5. Páginas de Videos
2.6. Páginas de Música
3. Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
4. Saben que existe la prohibición de descarga de software sin la autorización de la Subdirección Adjunta de Sistemas.
5. La utilización de Internet es para el desempeño de su función y puesto en el Bachillerato del Estado de Hidalgo y no para propósitos personales.

7.4. ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, su identificador de usuario y password necesarios para acceder a la información y a la infraestructura tecnológica del Bachillerato del Estado de Hidalgo, por lo cual deberá mantenerlo de forma confidencial.

El permiso de acceso a la información que se encuentraen la infraestructura tecnológica del Bachillerato del Estado de Hidalgo, debe ser proporcionado por el dueño de la información con base en el principio de la "necesidad de saber" el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

7.4.1. Seguridad Informática

1. Establecer las disposiciones aplicables acerca de seguridad informática para el Bachillerato del Estado de Hidalgo;
2. Llevar a cabo auditorías sobre los equipos de cómputo que son responsabilidad de los servidores públicos respecto a la seguridad informática;
3. Verificar que todos los protocolos y servicios innecesarios sean deshabilitados en todos los equipos de cómputo;
4. Asegurar que ningún elemento de infraestructura, aplicación o sistema de información, así como cuenta de usuarios carezcan de contraseña;
5. Mantener el control de la administración de los equipos de cómputo para permitir que sólo personal adscrito a la Dirección General tengan acceso a los mismos;
6. Realizar labores de investigación acerca de incidentes en los sistemas de información y elementos de infraestructura para determinar las causas de los mismos, y eventualmente, para deslindar responsabilidades;
7. Instalar en los equipos de cómputo del Bachillerato del Estado de Hidalgo antivirus, sistemas de control de accesos, sistemas de monitoreo de código malicioso; así como éstas y otras definiciones sean actualizadas frecuentemente;
8. Administrar las contraseñas de administrador de todos los equipos de cómputo del Bachillerato del Estado de Hidalgo;
9. Modificar los procedimientos de acceso a los sistemas de información con la finalidad de mejorar la seguridad informática;
10. Asegurar que los nodos de cableado estructurado que no estén en uso, no estén habilitados; o si lo están, tengan habilitados en los puertos de switch el acceso por medio de listas de acceso o por dirección física de Red;
11. Adquirir la infraestructura y/o sistemas para uso específico de seguridad informática más actual disponible dentro del presupuesto autorizado;
12. Capacitar al menos una vez al año a los servidores públicos responsables de la seguridad informática en cuanto a infraestructura y antivirus, o cada que haya una adquisición de infraestructura que implique una actualización o mejora a la seguridad informática;
13. Facilitar a los servidores públicos responsables de la seguridad informática el acceso permanente a información actualizada en esta materia.

7.4.2. Controles de acceso lógico

La Subdirección de TIC's tiene la facultad de registrar a nuevos usuarios de la red local, asignando nombre de usuario y contraseña proporcionada por el servidor público de nuevo ingreso.

El acceso a la infraestructura tecnológica del Bachillerato del Estado de Hidalgo para personal externo debe ser autorizado al menos por un Director de área del Organismo quien deberá notificarlo a la Subdirección de Informática quien lo habilitará.

Está prohibido que los usuarios utilicen la infraestructura tecnológica del Bachillerato del Estado de Hidalgo para obtener acceso no autorizado a la información u otros sistemas de información del Organismo.

Todos los servidores públicos son responsables por el usuario y password que recibe para el uso y acceso de los recursos de red y tecnológicos.

Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Subdirección Adjunta de Sistemas antes de poder usar la infraestructura tecnológica del Bachillerato del Estado de Hidalgo.

Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Bachillerato del Estado de Hidalgo, a menos que se tenga la autorización del dueño de la información y de la Subdirección de TIC's.

Cada usuario que acceda a la infraestructura tecnológica del Bachillerato del Estado de Hidalgo debe contar con un usuario único y personalizado. Por lo cual no está permitido el uso de un mismo usuario por varios servidores públicos.

Los usuarios son responsables de todas las actividades realizadas con su cuenta de usuario. Los usuarios no deben divulgar ni permitir que otros utilicen sus cuentas de usuario, al igual que tienen prohibido utilizar la cuenta de acceso de otros usuarios.

7.4.3. Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del Bachillerato del Estado deHidalgo, deberán ser notificados a la Subdirección de TIC's con el visto bueno de su Directorde área.

7.4.4. Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como passwords y protectores de pantalla institucional previamente instalados por la Subdirección de TIC's cuando no se encuentren en su lugar de trabajo.

7.4.5. Administración y uso de Passwords

La asignación del password debe ser realizadade forma individual, por lo que el uso de passwords compartidos está prohibido.

Cuando un usuario olvide, bloquee o extravíe su password, deberá levantar un reporte a la Subdirección de TIC's para que se le proporcione un nuevo password y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.

La obtención o cambio de un password debe hacerse de forma segura, el usuario deberá acreditarse ante la Subdirección de TIC's como empleado del Bachillerato del Estado de Hidalgo.

Está prohibido que los passwords se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

Sin importar las circunstancias, los passwords nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su password de todas las acciones que se realicen con el mismo.

Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus passwords:

Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), una letra mayúscula, un carácter especial y caracteres alfanuméricos.

Deben ser difíciles de adivinar, esto implica que los passwords no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.

No deben ser idénticos o similares a passwords que hayan usado previamente.

Todo usuario que tenga la sospecha de que su password es conocido por otra persona, deberá cambiarlo inmediatamente.

Los usuarios no deben almacenar los passwords en ningún programa o sistema que proporcione esta facilidad.

Los cambios o desbloqueo de passwords solicitados por el usuario a la Subdirección de TIC's serán notificados con posterioridad por correo electrónico al solicitante con copia al Director de área correspondiente, de tal forma que se pueda detectar y reportar cualquiercambio no solicitado.

7.5. ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La subdirección de TIC's tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

7.5.1. Derechos de propiedad intelectual

Está prohibido por las leyes de derechos de autor y por el del Bachillerato del Estado de Hidalgo, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por la Institución.

Los sistemas desarrollados por personal interno o externo que controle la Subdirección de TIC's son propiedad intelectual del Bachillerato del Estado de Hidalgo.

7.5.2. Revisiones del cumplimiento

La Subdirección de TIC's podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisarla actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado al Director de área correspondiente.

Los dueños de los procesos establecidos en el Bachillerato del Estado de Hidalgo deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

7.5.3. Violaciones de seguridad Informática

Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por la Subdirección de TIC's.

Está prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona puede probar o intentar comprometer los controles internos a menosde contar con la aprobación de la Subdirección de Informática, con excepciónde los Órganos Fiscalizadores.

Ningún usuario del Bachillerato del Estado de Hidalgo debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas por la Subdirección de TIC's.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Bachillerato del Estado de Hidalgo.

8. ASIGNACIÓN DE BIENES INFORMÁTICOS DE CÓMPUTO PERSONAL, Y PERIFÉRICOS

La Subdirección Adjunta de Recursos Materiales pondrá a disposición de la Subdirección de TIC's, la información necesaria de los bienes informáticos de cómputo personal y periféricos adquiridos, disponibles para reparación o asignación de equipo de cómputo.

La Subdirección de TIC's será quien valide el cumplimiento de las características técnicas de los bienes informáticos de cómputo personal y periféricos.

La Subdirección de TIC's tendrá bajo su resguardo las licencias de software, CD de software y un juego de manuales originales, así como un CD de respaldo para su instalación.

8.1 Logística para la entrega de bienes informáticos de cómputo personal y periféricos

La Subdirección de TIC's será el encargado de coordinar con las áreas usuarias la elaboración de los planes de asignaciones (nuevas) y reasignaciones de bienes informáticos de cómputo personal y periféricos, mismos que se proporcionarán a la Subdirección Adjunta de Recursos Materiales para su ejecución, según corresponda.

Asignación de bienes informáticos de cómputo personal, periféricos y de telefonía.

La Subdirección de TIC's realizará en cada asignación o movimiento de bienes informáticos de cómputo personal y periféricos, el documento el cual contiene los datos generales del usuario y de los bienes informáticos entregados, así mismo, contendrá los datos de software instalado y configuración del equipo, contando con la firma de conformidad del usuario correspondiente.

8.2 En caso de reasignaciones y movimientos de bienes informáticos de cómputo personal y periféricos requeridos por las áreas

Se deberá realizar la solicitud a la Subdirección Adjunta de Recursos Materiales a través del mecanismo que se tenga implantado (documento o de forma electrónica), de tal manera que sean modificados los respectivos resguardos del servidor público.

La Subdirección de TIC's es el área que debe de realizar las asignaciones, reasignaciones, almacenamientos, bajas, etc. de bienes informáticos de cómputo personal y periféricos, utilizando el mecanismo que se tenga implantado (documento o de forma electrónica), de manera que se dé aviso a la Subdirección Adjunta de Recursos Materiales para la actualización de resguardos del servidor público, o en el caso de baja entregar los bienes a la Subdirección referida para su destrucción o desecho responsable atendiendo las recomendaciones para el cuidado ambiental.

En caso de asignaciones y reasignaciones de bienes informáticos de manera masiva (Proyecto de Asignaciones y Reasignaciones de Bienes Informáticos de Cómputo Personal), la Subdirección de TIC's proporcionará por medio electrónico al Departamento de Recursos Materiales la relación de los movimientos que se llevarán a cabo. Cualquier cambio durante el proceso de asignación y reasignación será informado por la Subdirección de TIC's, según corresponda, la Subdirección Adjunta de Recursos Materiales para su conocimiento y actualización de la relación y resguardos.

8.3. Instalación y configuración del equipo

De los equipos de cómputo personal de escritorio y portátiles

El usuario deberá definir y preparar la información que se va a respaldar incluyendo todos sus archivos y carpetas de trabajo, así como sus archivos de carpetas personales.

El respaldo de la información del usuario (archivos con extensiones .DOCX, .XLSX,.PPTX, .PDF, etc.) será totalmente responsabilidad del servidor público, además de los archivos de su correo (archivos con extensiones .PST, .PAB, .MSG, etc.) la extracción de ésta será realizado por el personal de la Subdirección de TIC´s de acuerdo a lo que indique el usuario y no se podrán respaldar archivos con extensiones: avi, mpg, mov, mpeg, dvm, fli, flc, asf, real, swf, asx, mp3, mid, wav, y jpg.

La Subdirección de TIC's deberá realizar las instalaciones de acuerdo con los estándares del Bachillerato del Estado de Hidalgo, quedando prohibido instalar software no autorizado (todo software diferente al Sistema Operativo Windows, Office, compresor de archivos, lector de archivos pdf y antivirus).

La migración de la información del usuario al nuevo equipo será realizada por la Subdirección de TIC's y se deberá hacer en presencia del usuario.

El usuario será el responsable de verificar que toda la información y archivos de correo estén contenidos en el equipo asignado, al término el usuario deberá firmar el formato de servicio proporcionado por el personal asignado firmando de conformidad.

El tiempo que se lleve a cabo la asignación y configuración de una computadora de escritorio o portátil estará en función del volumen de datos, tipo de aplicaciones y servicios de información que contenga el equipo del usuario.

Antes de retirar el bien informático sujeto a reasignar o a dar de baja, el usuario deberá verificar que se le dé formato al disco duro del equipo que entrega, así como el borrado de los archivos en el directorio temporal utilizado para restaurar la información al equipo asignado.

Es responsabilidad del usuario a quien esté asignado el equipo de escritorio o portátil, la información contenida en la misma.

Cuando un usuario cambie de área, el equipo asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle el equipo de cómputo requerido para el desarrollode sus funciones.

De acuerdo a los lineamientos de reducción de costos, optimización y eficiencia de los recursos, los bienes informáticos y periféricos de cómputo personal usados podrán ser reciclados y asignados a un usuario antes de que éstos se vuelvan obsoletos.

8.4. De los equipos de impresión

Las impresoras solo se podrán asignar a niveles de subdirectores adjuntos, o bien a algún usuario quien justifique plenamente la necesidad de contar con una de ellas dadas las actividades que realice y deberán ser compartidas con el personal a su cargo.

Las impresoras láser B&N o de Color de red asignadas tendrán uso común para todos los servidores públicos del organismo por lo que no deberá ser usada como impresora personal deberán estar instaladas en lugares abiertos y accesibles para que el usuario no tenga ningún problema en utilizarlas.

La asignación de una impresora en red, será de acuerdo a la justificación plena por cargas de trabajo del área usuaria y a la capacidad de impresión de esta última.

8.5. De los equipos de digitalización (Scanner)

Los digitalizadores personales solo serán asignados a usuarios que por su función del puesto así lo requiera y deberá ser solicitado por escrito donde se describa la justificación y deberá ser autorizado por su Director de área.

Los digitalizadores departamentales asignados tendrán uso compartido por un grupo de usuarios por lo que no deberá ser usada como digitalizador personal, el resguardo del dispositivo será firmado por el servidor público al que le sea instalado.

La asignación de un digitalizador departamental, será de acuerdo a la justificación plena por cargas de trabajo del área usuaria y a la capacidad de digitalización de esta última.

Cuando un usuario cambie de área, el equipo telefónico asignado a éste deberá permanecer dentro del área designada originalmente. Será responsabilidad de la nueva área en la que habrá de laborar el usuario, el proporcionarle el equipo telefónico requerido para el desarrollo de sus funciones.

8.6. Préstamo de equipo de cómputo, periféricos y software

No existe el préstamo de equipo de cómputo, periféricos o software, por lo que cada área usuaria deberá prever la solicitud de asignación de los recursos que necesite.

8.7. Movimientos de bienes informáticos de cómputo personal y Periféricos

El usuario no deberá mover los bienes informáticos de cómputo personal o periféricos por su propia cuenta.

El usuario deberá elaborar el pase de salida cuando algún bien informático de cómputo personal y periférico requiera ser trasladado fuera de las instalaciones del Bachillerato del Estado de Hidalgo.

Si algún bien informático de cómputo personal o periférico es trasladado por el usuario a oficinas externas o foráneas para realizar sus labores, dicho bien estará bajo resguardo del responsable que retira el bien y el pase de salida será elaborado por el servidor público firmado por el director de área de adscripción.

8.8. Baja de bienes informáticos de cómputo personal y periféricos

La Subdirección de TIC's será la encargada de proporcionar a la Subdirección Adjunta de Recursos Materiales la relación de bienes que entrarán al proceso de baja, según corresponda.

Los equipos de cómputo personal y periféricos que por sus características técnicas (obsolescencia tecnológica) ya no sean útiles para el Bachillerato del Estado de Hidalgo, serán entregados por la Subdirección de TIC's a la Subdirección Adjunta de Recursos Materiales, mediante un documento denominado "Dictamen Técnico de baja", para que se lleve a cabo el proceso de destrucción mediante el procedimiento que establezca el Comité de Adquisiciones, Arrendamientos y Servicios del Bachillerato del Estado de Hidalgo.

9. DE LA SEGURIDAD A LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIONES

9.1. Autenticación

9.1.1 Se deberá establecer la validación o autenticación como mecanismo para permitir o denegar el acceso a los sistemas, así como para negar una transacción proveniente de alguien no autorizado.

9.1.2 El proceso de validación deberá minimizar las falsas aceptaciones o entradas no autorizadas a los sistemas, así como los falsos rechazos, esto mediante la utilización de mecanismos de autenticación (contraseña, credenciales, etc.) para lograr el acceso a los sistemas.

9.1.3 Para verificar la identidad del sujeto y por lo tanto ganar el acceso a los recursos como sujeto autorizado, deberá existir una cuenta única de usuario vinculada al sujeto, es decir, existirá una relación única entre la persona y su cuenta.

9.2. Contraseña de acceso a sistemas informáticos

9.2.1 Parala asignación de una contraseñase deberán tomar en cuenta los siguientes criterios:

9.2.1.1 La contraseña deberá tener las siguientes características:

12 (doce) caracteres, dentro de los cuales se establece una letra mayúscula, un número y un carácter especial (#, ?, $, %, &, ¿... etc.).

9.2.1.2 Únicamente la persona que ostenta el cargo de Responsable de Plantel deberá ser quien solicite la contraseña.

9.2.1.3 Acudir al Departamento de Registro y Control Escolar para dar de enterado su asignación al plantel correspondiente.

9.2.1.4 La Subdirección Adjunta de Control Escolar junto con el Responsable del Plantel, se presentarán la Subdirección de TIC's para registrar la contraseña como medio de acceso a la cuenta institucional de correo electrónico del plantel, una vez evaluada y aprobado el nivel de seguridad de la contraseña aprobado el nivel de seguridad de la contraseña por parte de la aplicación de administración de correo electrónico, se asigna a la cuenta de usuario para los sistemas de información internos del Bachillerato del Estado de Hidalgo, como medio de acceso a los módulos informáticos.

9.2.1.5 El nombre completo del Responsable del Plantel quedara asentado en la tabla y base de datos correspondiente para su impresión en documentos oficiales.

9.2.2 Para modificación de contraseña solicitada por el Responsable del Plantel, sin existir un cambio de personal en el cargo se establecelo siguiente:

9.2.2.1 Únicamente la persona que ostenta el cargo de Responsable de Plantel deberá ser quien solicite el cambio de la contraseña.

9.2.2.2 Acudir a Dirección General, marcar a la extensión del Departamento de Registro y Control Escolar o mediante un correo electrónico, solicitar el cambio de contraseña.

9.2.2.3 La Subdirección Adjunta de Control Escolar validará que el solicitante sea quien ostente el Cargo de Responsable de Plantel, mediante la presentación de su Credencial Oficial Vigente. Si el trámite es llevado por correo electrónico, se solicitará al Responsable del Plantel enviar una copia del Credencial Oficial Vigente por el medio antes mencionado. Lo anterior también aplicará si el. trámite es por vía telefónica.

9.2.2.4 La Subdirección Adjunta de Control Escolar o en su caso junto con el Responsable del Plantel, se presentarán a la Subdirección de TIC's para registrar la contraseña como medio de acceso a la cuenta institucional de correo electrónico del plantel, una vez evaluada y aprobado el nivel de seguridad de la contraseña por parte de la aplicación de administración de correo electrónico y asignada a la cuenta del correo electrónico institucional se asigna a la cuenta de usuario para los sistemas de información internos del Bachillerato del Estado de Hidalgo, como medio de acceso a los módulos informáticos.

9.2.2.5 El nombre completo del Responsable del Plantel quedará asentado en la tabla correspondiente para su impresión en documentos oficiales.

9.2.3 Para cambio de contraseña por motivos como cambio de plantel o nivel dentro del mismo plantel se hará lo siguiente:

9.2.3.2 Únicamente las personas que ostenten el cargo de Responsable de Plantel deberán ser quien soliciten el cambio de la contraseña.

9.2.3.3 Acudir a la Subdirección Adjunta de Control Escolar para dar de enterado su asignación al plantel correspondiente.

9.2.3.4 La Subdirección Adjunta de Control Escolar junto con el Responsable del Plantel, se presentarán la Subdirección de TIC's para registrar la contraseña como medio de acceso a la cuenta institucional de correo electrónico del plantel, una vez evaluada y aprobado el nivel de seguridad de la contraseña por parte de la aplicación de administración de correo electrónico y asignada a la cuenta del correo electrónico institucional se asigna a la cuenta usuario para los sistemas de información internos del Bachillerato del Estado de Hidalgo, como medio de acceso a los módulos informáticos.

9.2.3.5 El nombre completo del Responsable del Plantel quedara asentado en la tabla correspondiente para su impresión en documentos oficiales.

9.3. Respaldo de Información

9.3.1 La Subdirección de TIC's será la responsable de llevar a cabo el respaldo de todos los registros contenidos de las bases de datos de los diferentes sistemas de información del Bachillerato del Estado de Hidalgo.

9.3.2 La Subdirección Adjunta de Diseño y Desarrollo de Sistemas será el responsable de llevar a cabo el respaldo de todos los archivos fuente de los sistemas.

9.3.3 Los respaldos se darán en un plazo máximo de 8 días para minimizar en medida de lo posible la pérdida de información en caso de contingencia.

9.3.4 Los respaldos deberán resguardarse en duplicado manteniendo un juego en el centro de datos y otro fuera del mismo para minimizar la pérdida de información en caso de un sismo.

TRANSITORIOS

Primero.- Los presentes lineamientos entrarán en vigor al día siguiente de su publicación.

Segundo.- Los presentes lineamientos dejan sin efecto toda disposición interna que se oponga a estas.

Tercero.- Las operaciones que se hayan efectuado con anterioridad a la entrada en vigor del presente ordenamiento, se regirán por la normatividad interna vigente al momento de la operación hasta su totalidad.



Elías Cornejo Sánchez
Director General
Bachillerato del Estado de Hidalgo

Agosto de 2026

BACHILLERATO DEL ESTADO DE HIDALGO

EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

CONTACTO

771-718-3237 ext. 223
www.bachillerato-hgo.edu.mx
subdir.tic@bachillerato-hgo.edu.mx
Cto. Ex-hacienda la Concepción Lote 17, San Juan Tilcuautla
San Agustín Tlaxiaca, Hidalgo, México

