HIDALGO
IEE
INSTITUTO ESTATAL ELECTORAL

POLÍTICAS Y LINEAMIENTOS DE GESTIÓN DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

Unidad de Tecnologías de la Información y Comunicaciones

CONTENIDO

MARCO LEGAL

Constitución Política de los Estados Unidos Mexicanos.

Constitución Política del Estado de Hidalgo.

Código Penal para el Estado de Hidalgo.

Ley General de Responsabilidades Administrativa.

Ley de Responsabilidades Administrativas del Estado de Hidalgo.

Ley General de Transparencia y Acceso a la Información Pública.

Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo.

Ley de Entrega Recepción de los Recursos Públicos del Estado de Hidalgo.

Estrategia Digital Nacional.

Modelo Estatal de Marco Integrado de Control Interno para el Sector Público del Estado de Hidalgo.

DEFINICIONES, SIGLAS Y ACRÓNIMOS

A. Definiciones

Activos: Información relacionada con el tratamiento de la misma que tenga valor para el Instituto.

Activos informáticos: Recursos de software y hardware propiedad del Instituto, así como la infraestructura tecnológica y todos los elementos que componen el proceso de comunicación, desde la información, el emisor, el medio de transmisión y receptor.

Activos de información: Información que son esenciales o críticos para la operación y el cumplimiento de objetivos, y que por su importancia deben ser protegidos conforme al valor que representen.

Alfabeto-Fonético: Conjunto de palabras usadas por usuarios para deletrear en transmisiones por radio o teléfono para evitar que se produzcan errores de comprensión.

Alfanuméricas: Término formado por letras y números conjuntamente, las letras pueden ser mayúsculas o minúsculas.

Ancho de Banda: Cantidad de datos que pueden transmitirse a través de una conexión en un período de tiempo determinado

Antivirus: Software creado con el objetivo de detectar y eliminar virus informáticos como**:** malware, spyware, troyanos, etc.

Bloqueo: Mecanismos para evitar el acceso no permitido a equipos de telefonía móvil institucionales que sean asignados al personal del Instituto.

Centro de Datos: Espacio donde se concentran conectados, todo tipo de servidores dedicados para el procesamiento o almacenamiento de la información del Instituto.

Código Abierto *(Open Source):* Código fuente de un programa o software que está disponible públicamente para que el personal de la UTIC pueda leerlo, modificarlo, y redistribuirlo.

Código Fuente: Código de un programa desarrollado por la UTIC o por terceros.

Confidencialidad: Propiedad que indica que la información esté disponible y no sea divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: Datos, informes y demás información pertinente se encuentran lista y accesible para los usuarios cuando sea necesario.

Enlace: Medio de conexión entre dos inmuebles para ofrecer servicio de internet, video, voz y datos de forma segura para los usuarios de tecnologías del Instituto.

Extraoficial: Forma de hacer uso de cuentas de correo electrónico personales, con la autorización correspondiente.

Fibra Óptica: Medio físico que permite la transmisión a distancias y en un ancho de banda más grandes que los cables de cobre.

Hardware: Total de los elementos materiales, tangibles que forman parte de un equipo informático.

Infraestructura en la Nube: Recursos de hardware y software que permiten alojar y ejecutar aplicaciones y servicios en la nube de internet.

Instituto: Instituto Estatal Electoral de Hidalgo.

Inobservancia: Incumplimiento a las disposiciones cometidas por las personas servidoras públicas, adscritos al Instituto.

Intransferible: Credenciales, cuentas de acceso, claves telefónicas, cuentas de correo institucional o servicios que no pueden transferirse a terceras personas.

Integridad: Información es protegida contra su modificación o destrucción indebida, incluidos la irreductibilidad y autenticidad de la información.

La Nube: Red global de servidores que almacenan y gestionan datos y aplicaciones, permitiendo a los usuarios acceder a ellos desde cualquier dispositivo conectado a Internet.

Mantenimiento Correctivo: Acciones que corrigen los defectos observados en la infraestructura tecnológica del Instituto.

Mantenimiento Preventivo: Acciones de conservación de la infraestructura tecnológica del Instituto que garanticen su buen funcionamiento y fiabilidad.

Mesa de Servicio: Área de la UTIC destinada a la alta, seguimiento y conclusión de reportes de usuarios, en materia de Tecnologías de la Información.

Perfiles: Atributos personalizados, específicamente asignados para los usuarios del Instituto.

Personas servidoras públicas: Personas que desempeñen un empleo, cargo o comisión adscritas a las diferentes unidades administrativas del Instituto.

Pista de Auditoría: Registro secuencial de eventos y acciones que se llevan a cabo en los sistema o aplicaciones, permitiendo rastrear y verificar las transacciones y cambios realizados.

Redes Inalámbricas: Conexión de nodos que se da por medio de ondas electromagnéticas, situadas en las instalaciones del Instituto, con accesos limitados.

Respaldo: Copia de seguridad de información realizada en periodos de tiempo determinado, teniendo control para su acceso.

Servidores de respaldo: Computadoras con alta capacidad de almacenamiento.

Sistema Operativo: Software principal de un equipo de cómputo.

Sites: Espacio con adecuaciones físicas diseñadas para albergar equipos de telecomunicaciones y computo del Instituto que garanticen la seguridad de la información y de la propia infraestructura tecnológica.

Software: Soporte lógico de cualquier sistema informático; es la contraposición a los componentes físicos (hardware).

Software libre: Programa informático cuyo código fuente puede ser estudiado, modificado, y utilizado libremente, autorizado para su uso en el Instituto, cumpliendo con las medidas de seguridad.

Telecomunicaciones: Transmisión y recepción de señales electromagnéticas, gestionadas por los usuarios del Instituto.

Telefonía Móvil: Telefonía celular a través de un medio de comunicación inalámbrico proporcionado a personal autorizado adscrito al Instituto.

Unidad Administrativa: Áreas del Instituto que son referenciadas en el Reglamento Interior del Instituto Estatal Electoral.

Usuario: Persona que interactúa con sistemas y dispositivos tecnológicos propiedad del Instituto.

Videoconferencia: Comunicación de audio y vídeo, que permite mantener reuniones con grupos de personas situadas en lugares alejados entre sí, utilizada por el personal de las unidades administrativas del Instituto.

Vulnerabilidad: Riesgos que un sistema o activo pudiera presentar frente a eventualidades inminentes dentro del Instituto.

B. Siglas y Acrónimos

DEA: Dirección Ejecutiva de Administración

LGIPE: Ley General de Instituciones y Procedimientos Electorales

URL: Por sus siglas en ingles Localizador Uniforme de Recursos, es la dirección única que se les asigna a las páginas web o sistemas informáticos institucionales.

NAG: Normativa del Archivo General del IEEH

SE: Secretaría Ejecutiva del IEEH

UTIC: Unidad de Tecnologías de la Información y Comunicaciones.

UTCS: Unidad Técnica de Comunicación Social

TIC: Tecnologías de la Información y Comunicación

VPN: Red Privada Virtual para proporcionar servicios de conexión a través de un canal seguro.

ANTECEDENTES

En términos del artículo 24, fracción III de la Constitución Política de Estado De Hidalgo, el Instituto Estatal Electoral de Hidalgo es un organismo público autónomo, dotado de personalidad jurídica y patrimonio propios. Tiene a su cargo en forma integral y directa las actividades relativas a la organización de las elecciones locales, así como la declaración de validez y otorgamiento de Constancias en las Elecciones Locales. En el ejercicio de esta función estatal, la Certeza, Legalidad, Independencia, Imparcialidad, Máxima Publicidad y Objetividad serán principios rectores en términos de lo dispuesto en los artículos 46, 47 y demás relativos del Código Electoral del Estado de Hidalgo, así como los artículos 98 numeral 1 y 99 numeral 1 de la LGIPE.

Que la Estrategia Digital Nacional establece el Principio de Seguridad de la Información, cuyo objetivo específico es promover una cultura de seguridad de la información que genere certeza y confianza a las personas usuarias de los servicios tecnológicos institucionales y gubernamentales; y que busca mediante una política general de seguridad de la información la procuración de la preservación de la confidencialidad, disponibilidad e integridad de la información resguardada por las Instituciones.

El Artículo 25 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados dispone que con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad. Así como lo dispuesto en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados para el Estado de Hidalgo y demás disposiciones que resulten aplicables en la materia.

El artículo 30, inciso b), del Reglamento Interior del Instituto Estatal Electoral establece que la Unidad de Tecnologías de la Información y Comunicaciones beberá proponer políticas y establecer los mecanismos necesarios para garantizar la confiabilidad y continuidad de los sistemas y servicios informáticos institucionales.

El Modelo Estatal de Marco Integrado de Control Interno para el Sector Público del Estado de Hidalgo, establece que se deben diseñar las actividades de control sobre la infraestructura de las TIC’s para soportar la integridad, exactitud y validez del procesamiento de la información mediante el uso de TIC’s; se debe diseñar actividades de control para la gestión de la seguridad sobre los sistemas de información con el fin de garantizar el acceso adecuado, de fuentes internas y externas a éstos.

OBJETIVO

Establecer las Políticas y Lineamientos en materia de Gestión de Sistemas de Información y Comunicaciones en el Instituto Estatal Electoral de Hidalgo para el cumplimiento de sus objetivos institucionales, la seguridad, el procesamiento y la detección de riesgos en la información y los activos informáticos.

ALCANCE

Las presentes Políticas y Lineamientos de Gestión de Tecnologías de Información y Comunicaciones son de observancia obligatoria para las personas servidoras públicas del Instituto y a toda persona o empresa externa tengan acceso autorizado a información, instalaciones, infraestructura y servicios de este.

RESPONSABLE DE SU APLICACIÓN

La Unidad de Tecnologías de la Información y Comunicaciones es responsable de implementar mecanismos de control y supervisar el cumplimiento de las Políticas y Lineamientos de Gestión de Sistemas de Información y Comunicaciones del Instituto Estatal Electoral de Hidalgo, con el fin de garantizar la integridad, disponibilidad, confidencialidad y trazabilidad de la información institucional, así como de promover el uso eficiente y seguro de los recursos tecnológicos.

POLÍTICAS

1. POLÍTICA DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

Controlar y monitorear los accesos a los medios de información para proteger la confidencialidad, integridad y disponibilidad de la información; incluyendo controles de acceso, cifrado de datos, y medidas para prevenir accesos no autorizados, pérdida o alteración de la información.

1.1 Manejo de la información documental física y digital

1.1.1 La información será tratada de acuerdo con la POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN descrita en el presente documento.

1.1.2 Los usuarios que tengan acceso a información institucional estarán obligados con el uso responsable de ésta conforme a la normatividad vigente y las presentes Políticas y Lineamientos.

1.1.3 Las personas titulares de las unidades administrativas implementarán métodos y medidas para administrar, organizar y conservar de manera homogénea los documentos de archivo que reciban, produzcan, obtengan, adquieran, transformen o posean, derivado de sus facultades, competencias o funciones.

1.1.4 La UTIC, con el apoyo de las unidades administrativas será la responsable de instrumentar procesos sistematizados que disminuyan el uso de papel en los trabajos de impresión y fotocopiado, en cumplimiento a las medidas de austeridad institucionales.

1.1.5 Los responsables de gestionar la disponibilidad, localización expedita, integridad y conservación de los documentos del archivo físico serán de conformidad con la normatividad del archivo general del Instituto.

1.1.6 Las Personas servidoras públicas evitarán dejar documentación o medios de almacenamiento en los dispositivos de impresión, fotocopiado o digitalización de uso compartido.

1.1.7 Las personas servidoras públicas podrán tener acceso a la información de otras áreas que les permita realizar su trabajo por lo que estarán comprometidos con el uso responsable de ésta.

1.1.8 Las personas servidoras públicas deberán garantizar que los documentos de archivo electrónico o digital posean las características de confidencialidad, integridad y disponibilidad.

1.1.9 Las unidades administrativas deberán usar la nomenclatura estándar para el manejo de carpetas y archivos electrónicos conforme la Normatividad del Archivo General del Instituto.

1.2 Inventario de activos de información

1.2.1 Una vez que se ha realizado la clasificación y etiquetado de los activos de información, se remitirá a la SE la documentación en formato físico y digital para integrar los datos al inventario de activos de información.

1.2.2 Los cambios en la clasificación, baja o alta de nuevos activos, se harán conforme a la NAG.

1.3 Seguridad de Recursos Humanos

Las personas servidoras públicas del Instituto realizarán el procedimiento de entrega recepción formal, al concluir su empleo, cargo o comisión, ante su superior jerárquico, en la cual deberán proporcionar la información y documentación debidamente ordenada, clasificada y legalizada, conforme a la normatividad aplicable.

La información relativa a los recursos humanos, materiales, financieros e informáticos que se entreguen; se registrará en los formatos autorizados por el Órgano Interno de Control correspondiente, los cuales deberán generarse por cuadruplicado y contener la firma autógrafa, o en caso de tenerla implementada en el Instituto, la firma electrónica avanzada de quienes intervengan en el acto de entrega recepción.

1.4 Difusión de las Políticas y Lineamientos de Seguridad de la Información

1.4.1 La UTIC será la responsable de implementar medidas de formación sobre la seguridad de la información entre el personal del Instituto.
1.4.2 La UTCS será la responsable de implementar medidas de difusión y sensibilización sobre la seguridad de la información entre el personal del Instituto.
1.4.3 Las personas titulares de las unidades administrativas serán responsables de fomentar la difusión de las Políticas y Lineamientos de Seguridad de la Información a las personas servidoras públicas de nuevo ingreso.
1.4.4 Las personas servidoras públicas serán responsables de aplicar las Políticas y Lineamientos de Seguridad de la Información en su entorno laboral.
1.4.5 Las personas servidoras públicas estarán obligados a informar a su superior jerárquico las posibles vulnerabilidades detectadas en Seguridad de la Información.

1.5 Protección de la información

1.5.1 Las personas servidoras públicas que, por asignación del cargo o comisión, administren, capturen, consulten, recaben o transfieran información, estarán obligados a salvaguardarla y conservarla, a fin de cumplir con los criterios de confidencialidad, integridad y disponibilidad.

1.5.2 Las personas servidoras públicas de nuevo ingreso firmarán un acuerdo de confidencialidad de la información.

1.6 Cambio de funciones

En el caso de cambios de adscripción o asignación de nuevas funciones, las personas servidoras públicas serán las responsables de realizar el procedimiento de entrega recepción formal.

1.7 Conclusión de la relación laboral

1.7.1 Las personas servidoras públicas al concluir su relación laboral con el Instituto dejarán de conservar en su poder los activos de información y activos informáticos; que, por motivos del cargo o funciones, tenían bajo su resguardo, lo cual quedará asentado en el Acta de los sujetos obligados a la Entrega y Recepción.

1.7.2 La o el servidor público o la persona que tenga bajo su resguardo o responsabilidad el desarrollo, administración u operación de sistemas de información automatizados o infraestructura tecnológica del Instituto, y que deje de prestar sus servicios, debe realizar de manera formal la entrega a su jefe inmediato o responsable del proyecto, toda la documentación relacionada, consistente en; manuales, archivos de código

fuente, respaldos, bases de datos, cuentas de acceso, contraseñas y todo archivo almacenado en medios magnéticos e impresos.

1.8 Seguridad Física y Ambiental

La DEA establecerá controles de acceso físico a las instalaciones del Instituto. Por otra parte, las personas titulares de las unidades administrativas serán los responsables de gestionar la conservación de las áreas de trabajo; asimismo, las personas servidoras públicas serán los responsables de mantener los espacios de trabajo libres de obstrucciones para prevenir daños a la infraestructura tecnológica, evitando así, poner en riesgo la seguridad de la información y la continuidad de la operación.

1.8.1 Acceso físico a oficinas e instalaciones.

1.8.1.1 La DEA establecerá medidas de control de acceso a las instalaciones, tanto en áreas comunes como en áreas restringidas. Los Centros de Datos y Sites que albergan infraestructura tecnológica deberán ser consideradas de acceso restringido; teniendo únicamente acceso personal autorizado de la UTIC.

1.8.1.2 El acceso de toda persona externa al Instituto deberá contar con la autorización de las personas titulares de las unidades administrativas.

1.8.1.3 Toda persona externa al Instituto que permanezca dentro de las instalaciones deberá portar un identificador de visitante, y estar acompañado en todo momento de una persona Servidora Pública.

1.8.1.4 Las personas servidoras públicas que cumplan sus funciones en oficinas o despachos, las cerrarán con llave al final de la jornada laboral.

1.8.1.5 La DEA instruirá la utilización de la identificación oficial visible para las personas servidoras públicas, así como para terceros que permanezcan dentro de los inmuebles Institucionales.

1.8.1.6 La persona titular de la UTIC a través de la o el Servidor Público que designe restringirá o supervisará el ingreso a los Centros de Datos y Sites, de dispositivos de almacenamiento externo y video.

1.8.1.7 Las personas titulares de las unidades administrativas, a su consideración, fomentarán la restricción cuando por motivo de la sensibilidad de la información se justifique, el uso de dispositivos electrónicos en las áreas laborales.

1.8.1.8 La DEA establecerá controles documentales de acceso físico, tales como bitácoras de acceso a las instalaciones, los cuales se revisarán periódicamente.

1.9 Seguridad de la infraestructura.

1.9.1 Las personas titulares de las unidades administrativas con apoyo de la UTIC establecerán mecanismos de protección de la infraestructura tecnológica que las

personas servidoras públicas tengan asignada para desempeñar sus labores, atendiendo los siguientes lineamientos:

1.9.1.1 Los equipos de cómputo no deberán estar expuestos a la luz solar por tiempos prolongados.
1.9.1.2 Deberán mantener despejadas las áreas de ventilación donde se ubique la infraestructura tecnológica.
1.9.1.3 La infraestructura tecnológica sólo podrá ser reubicada por el personal técnico autorizado por la UTIC.
1.9.1.4 Las personas servidoras públicas evitarán comer o beber en su espacio de trabajo donde se encuentre instalado el equipo tecnológico usado para el desarrollo de sus actividades.

1.9.2 Los activos informáticos que se encuentren conectados a las tomas de corriente regulada deberán estar protegidos contra cualquier corte o variación de voltaje, para ello se atenderán las siguientes indicaciones:

1.9.2.1 Las tomas de corriente a las que se conecten los activos informáticos permanecerán siempre en buenas condiciones, las personas servidoras públicas que detecten fallas o defectos en éstas deberán reportarlo al Titular de la Unidad Administrativa para que gestione su corrección.
1.9.2.2 Las personas titulares de las unidades administrativas evitarán que se conecten a equipos de protección eléctrica cualquier aparato eléctrico que genere variación de voltaje, como pueden ser: ventiladores, calentadores de agua, refrigeradores, hornos de microondas, aspiradoras, por mencionar algunos.
1.9.2.3 El cableado de los activos informáticos deberá estar ordenado, ajustado mediante cinchos y sin obstruir el paso.

1.9.3 El mantenimiento preventivo y correctivo de los activos informáticos del Instituto estarán a cargo de la UTIC, misma que proporcionará los medios para su reporte y seguimiento.

1.9.3.1 Las personas servidoras públicas del Instituto, estarán impedidos para abrir o verificar internamente los activos informáticos.
1.9.3.2 La reubicación de los activos informáticos únicamente lo efectuará el personal de la UTIC, a través del personal de Soporte Técnico.

1.9.4 La DEA establecerá los mecanismos de inspección de la entrada y salida de los activos informáticos a las instalaciones del Instituto.

1.9.5 Las personas servidoras públicas serán responsables de los activos informáticos que tengan bajo su resguardo, dentro y fuera de las instalaciones.

1.9.6 Las personas titulares de las unidades administrativas supervisarán que las personas servidoras públicas mantengan el equipo tecnológico asignado para el trabajo libres de objetos que puedan interferir con su adecuada operación.

1.9.6.1 Al ausentarse de su espacio de trabajo, las personas servidoras públicas, cuando el mobiliario y el espacio físico así lo permita, evitarán dejar documentos que contengan información institucional a la vista.

1.9.7 Las personas servidoras públicas mantendrán bloqueados sus equipos de cómputo cuando se encuentren alejados de su espacio de trabajo.

1.10 Control de Accesos Lógicos

La UTIC establecerá los mecanismos de acceso a los activos informáticos, que deberán cumplir los usuarios, manteniendo la confidencialidad y el uso responsable de la información.

1.11 Gestión de acceso de usuario

La UTIC implementará un procedimiento para otorgar accesos a usuarios autorizados, e impedir accesos no autorizados, asignando los permisos que correspondan; considerando la clasificación de información en base a su impacto y confidencialidad requerida.

1.11.1 Gestión de registro de usuario

La UTIC realizará el alta de usuarios de acuerdo con el procedimiento establecido, con el objeto de habilitar la asignación de perfiles de acceso a los activos informáticos del Instituto, los cuales deben permitir identificar y autenticar a los usuarios, evitando accesos no autorizados.

1.11.2 Revisión de derechos de acceso de los usuarios

La UTIC deberá supervisar periódicamente los derechos de acceso otorgados conforme a los perfiles de usuario, mediante monitoreo de actividades y eventos realizados por los usuarios.

1.11.3 Retirada o adaptación de los derechos de acceso

En caso de ser detectada alguna actividad sospechosa o inusual en la cuenta del usuario que pueda comprometer la integridad o confidencialidad de la información institucional, se suspenderá temporalmente el acceso, y solo será habilitado después de tomar las medidas que considere necesarias la UTIC.

Al concluir la relación laboral, o por cambio de adscripción de los usuarios, las personas titulares de las unidades administrativas y la DEA notificarán a la UTIC para que esta retire los accesos a los usuarios o terceros que ya no deban tenerlo.

1.12 Responsabilidades del usuario

El conocimiento y cumplimiento de estas Políticas y Lineamientos son de carácter obligatorio para todos los usuarios. Los activos informáticos deberán ser operados bajo los principios de confidencialidad y reserva, realizando un uso adecuado y responsable en los mismos.

1.12.1 Uso de contraseñas

1.12.1.1 Los usuarios deberán aplicar las buenas prácticas de seguridad respecto a la nomenclatura y uso de las contraseñas, considerando las siguientes recomendaciones:

- Las contraseñas se deberán mantener como confidenciales en todo momento.
- Las contraseñas son personales e intransferibles.
- Debe evitarse escribir las contraseñas en papeles de fácil acceso.
- Inhabilitar la opción “recordar clave en este equipo”.
- Las contraseñas deberán estar compuestas por una combinación de al menos ocho (8) caracteres alfanuméricos, incluyendo un carácter especial.
- Cambiar su contraseña de manera periódica.
- Cuando se sospeche la violación de la contraseña, el usuario deberá notificarlo de inmediato a la UTIC mediante el Sistema de Gestión de Servicios.
- Cuando el usuario olvide, bloquee o extravíe sus contraseñas deberá realizar el procedimiento de restablecimiento de contraseñas, o de ser necesario, reportarlo a la UTIC mediante el Sistema de Gestión de Servicios.

1.12.2 Equipo informático de usuario desatendido

El usuario deberá asegurar el bloqueo por contraseña del equipo informático evitando accesos no autorizados durante su ausencia.

1.13 Control de acceso a sistemas operativos y aplicativos

La UTIC deberá garantizar el acceso exclusivo a los usuarios autorizados, implementando medidas de seguridad en sus sistemas y aplicativos que minimicen la divulgación, modificación, sustracción o intromisión en los activos de información e informáticos.

1.13.1 Restricción de acceso a la información

Los activos informáticos serán tratados con reserva y confidencialidad de acuerdo con la clasificación otorgada; únicamente los usuarios autorizados tendrán acceso a ellos, de acuerdo con las funciones que desempeñen.

1.13.2 Procedimientos seguros de inicio de sesión

Es obligatorio que los activos informáticos utilizados por las unidades administrativas del Instituto cuenten con mecanismos de autenticación en el acceso de los mismos.

Para ello la UTIC:

- Establecerá controles de autenticación, que eviten la visualización de contraseñas.
- Implementará controles que detecten múltiples intentos de autenticación fallida.
- Implementará controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.

1.13.3 Gestión de contraseñas de usuario

La administración de usuarios y contraseñas se deberá realizar por medio de procedimientos formales de gestión a cargo de la UTIC, tomando en cuenta lo siguiente:

- Remitir la solicitud con los datos del usuario mediante medios formales de comunicación institucional.
- El usuario y contraseña deberán otorgarse de manera personal y confidencial.

La UTIC, realizará la implementación de un inicio seguro de sesión, mediante la asignación de contraseñas predeterminadas para los usuarios, basándose en los criterios siguientes:

- La confidencialidad de la contraseña.
- Validación de los datos de acceso.
- Identificación del número de intentos fallidos de conexión, para bloquear el acceso, si rebasa el máximo permitido.
- Ocultando los datos de la contraseña digitados.

La UTIC, creará en los sistemas que desarrolle, un proceso para restablecimiento de contraseñas rápido y fácil de usar, que además proteja la información del usuario.

1.13.4 Control de acceso al código fuente de los programas

La UTIC controlará el acceso al código fuente de los programas y sistemas de información que desarrolle, llevando un control de los cambios autorizados y aplicados

en el código fuente. Se asegurará que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, estableciendo procedimientos y controles tales como registros de actividad.

Los desarrolladores internos o externos estarán sujetos al acceso controlado y/o limitado a los activos de información e informáticos que se encuentren en los ambientes de producción.

1.13.5 Aislamiento de sistemas sensibles

La UTIC supervisará que los sistemas y activos informáticos sensibles o críticos dispongan de un entorno informático dedicado (propio), evitando que tengan acceso por vía remota o red, solo se permitirá el acceso presencial en el lugar donde se encuentre dicho activo.

2. POLÍTICA DE GESTIÓN DE LA CALIDAD DE LA INFORMACIÓN

Se garantizará que la información generada, administrada y difundida por el Instituto cumpla con los principios de veracidad, oportunidad, confiabilidad, accesibilidad, integridad, legalidad y transparencia. Para ello, la UTIC será responsable de coordinar, supervisar y evaluar los mecanismos necesarios para asegurar que la información institucional:

2.1 Sea precisa y verificable, evitando errores que puedan afectar la toma de decisiones o la percepción pública.
2.2 Esté disponible de manera oportuna, para satisfacer las necesidades de los usuarios internos y externos.
2.3 Se resguarde adecuadamente, protegiendo su confidencialidad y evitando accesos no autorizados.
2.4 Cumpla con los estándares normativos de seguridad, establecidos en la Ley de Transparencia y Acceso a la Información Pública para el Estado de Hidalgo y demás disposiciones aplicables.
2.5 Sea difundida en formatos abiertos y reutilizables, promoviendo el gobierno abierto y la transparencia proactiva.
2.6 Se mantenga actualizada, mediante procesos periódicos de revisión y validación.

3. POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Se clasificará la información para mantener su confidencialidad, disponibilidad e integridad, independientemente que se encuentre en formato físico o digital, facilitando su control, manejo y preservación.

Las personas titulares de las unidades administrativas serán responsables de clasificar la información a su alcance, previo análisis con la persona Oficial de Datos Personales, de acuerdo con las funciones asignadas considerando que el manejo de la información personal de usuarios, partidos políticos y ciudadanía cumpla con las leyes de protección de datos para garantizar la privacidad de la información; y posteriormente presentarla ante el Comité de Transparencia para que confirme, modifique o revoque dicha información.

3.1 **Clasificación de la información**

Las personas titulares de las unidades administrativas que conforman el Instituto clasificarán los activos de información de acuerdo con los siguientes criterios:

Confidencialidad

a) Información pública: Cuando sea de uso general, que por su contenido o contexto no requiere de protección especial y su distribución ha sido permitida a través de canales autorizados por la Institución. Esta deberá ser de libre acceso, publicarse y difundirse de manera universal, permanente y actualizada en sus formatos físico o digital
b) Información reservada: Cuando deba restringirse conforme a criterios en materia de Transparencia y Acceso a la Información Pública.
c) Información confidencial: Conforme los criterios en materia de Transparencia y Acceso a la Información Pública.

Integridad

Se consideran cuatro niveles para la clasificación:

a) Alta: Información cuya pérdida ocasionaría un gran impacto en la operación de la Unidad Administrativa.
b) Media: Información cuya pérdida representaría retraso en la operación de la Unidad Administrativa.
c) Baja: Información cuya pérdida ocasiona un impacto no significativo en la operación de la Unidad Administrativa.
d) No clasificada: Información que aún no ha sido clasificada o que está en ese proceso.

Disponibilidad

Se consideran tres niveles para la clasificación:

a) Alta: La no disponibilidad de la información puede conllevar un impacto en la operación de la Unidad Administrativa.

b) Media: La no disponibilidad de la información puede conllevar a un retraso en la operación de la Unidad Administrativa.
c) Baja: La no disponibilidad de la información puede afectar en lo mínimo la operación.

Se evitará el acceso, distribución, comercialización, publicación y difusión general de la información, con excepción de las autoridades competentes que, conforme a la Ley, tengan acceso a ella y de los particulares titulares de dicha información.

4. POLÍTICA DE USO ACEPTABLE DE RECURSOS INFORMÁTICOS

Se establecerán las pautas para el uso de sistemas de información y comunicaciones del Instituto, promoviendo un ambiente seguro y productivo que garantice su buen uso.

La UTIC será la responsable de mantener la operación de los activos de información e informáticos, supervisando que el uso adecuado, mantenimiento y actualización de estos, sean controlados y documentados; minimizando riesgos en los activos referidos y protegiendo la información.

4.1 Responsabilidades y procedimientos de operación.

4.1.1 La UTIC regulará los procedimientos de operación de los activos de información e informáticos del Instituto, verificando que se realicen conforme a las presentes Políticas y Lineamientos.

4.1.2 La UTIC será la responsable de supervisar que los procedimientos de operación de los activos de información e informáticos cuenten con la documentación técnica respectiva.

4.1.3 Los desarrollos de sistemas de información, diseños, contenidos y productos realizados por las personas servidoras públicas o usuarios en el ejercicio de sus funciones serán propiedad del Instituto.

4.2 Protección contra código malicioso

4.2.1 Controles contra el código malicioso.

La UTIC a través del personal de Soporte Técnico, será la responsable de realizar y supervisar:

a) La instalación de software en los activos informáticos.
b) La realización periódica de un escaneo en los equipos de cómputo, con el fin de verificar que no exista código malicioso.

c) La permanencia de las configuraciones de seguridad para detectar virus en programas o aplicaciones tales, como son:
   - Sistema operativo
   - Correo Electrónico
   - Herramientas de productividad
   - Navegadores

d) La instalación de antivirus en los equipos de cómputo.

4.3 Copia de seguridad

4.3.1 La información será respaldada independientemente de su clasificación, en los medios de almacenamiento que las personas titulares de las unidades administrativas autoricen, incluyendo dispositivos de almacenamiento externo.

4.3.2 Los usuarios serán responsables de realizar los respaldos de información en periodos de tiempo determinados, según el procedimiento establecido y de acuerdo con la clasificación de la información que tengan bajo su resguardo.

4.3.3 Las personas titulares de las unidades administrativas implementarán un registro (bitácora) de los respaldos generados, que contenga la siguiente información:

- Número de folio o consecutivo del respaldo
- Fecha de respaldo
- Hora de respaldo
- Unidad Administrativa
- Titular de la Unidad Administrativa
- Área que genera la información
- Nombre del responsable que realizó el respaldo
- Nombre del jefe inmediato.

Esto, con la finalidad de que las Áreas cuenten con un registro de los respaldos de la información que generen.

4.3.4 El personal designado por las personas titulares de las unidades administrativas verificará que la información respaldada, al ser restaurada se conserve íntegra.

4.3.5 Para el caso de sistemas informáticos desarrollados por personal del Instituto, la UTIC será la responsable de generar respaldos del código fuente, bases de datos, contraseñas y demás componentes que aseguren su integridad y continuidad.

4.4 Correo electrónico

4.4.1 La administración de las cuentas de correo electrónico institucional será llevada a cabo exclusivamente por la UTIC.

4.4.2 La UTIC establecerá controles que permitan garantizar la seguridad de la plataforma de correo electrónico contra código malicioso.

4.4.3 La UTIC concientizará al personal del Instituto y terceros en temas de seguridad que deben adoptar para el intercambio de información, por medio del correo electrónico.

4.4.4 Las cuentas de correo electrónico institucional serán de uso individual, intransferible y para uso exclusivo del personal del Instituto o personas autorizadas.

4.4.5 Para el intercambio de información en actividades laborales, se deberá hacer mediante el correo electrónico institucional.

4.4.6 Las personas servidoras públicas serán cuidadosos de la información contenida en los buzones de correo, debido a que es propiedad del Instituto; de igual forma mantendrán en ellos solo la información relacionada a las funciones asignadas.

4.4.7 Las personas servidoras públicas, respetarán el formato establecido e imagen institucional definidos; así como, conservar en todos los casos el criterio de confidencialidad, bajo los términos normativos y de transparencia relacionados con el tratamiento de información.

4.4.8 Será responsabilidad de las personas servidoras públicas cerrar su cuenta de correo al dejar de utilizarlo, para evitar que otros usuarios puedan hacer uso de él.

4.4.9 Las personas servidoras públicas, respaldarán la información contenida en su cuenta de correo, o si es el caso, solicitarán a la UTIC la asesoría para realizar los respaldos.

4.4.10 Las personas servidoras públicas serán responsables de reportar a la UTIC mediante el Sistema de Gestión de Servicios, cualquier mensaje de correo de procedencia desconocida o sospechosa, con el fin de evitar posibles infecciones por código malicioso o virus.

4.4.11 Las personas servidoras públicas reportarán oportunamente a la UTIC cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseña, o cualquier comportamiento anormal en este, a fin de poder tomar las medidas pertinentes.

4.4.12 El uso de las cuentas de correo compartidas estará permitido, serán creadas para las diferentes unidades administrativas o funcionarios públicos, que, por sus

funciones u objetivos de la actividad, justifiquen la operación grupal; su administración será responsabilidad de las personas titulares de las mismas.

4.4.13 Se debe evitar utilizar la cuenta de correo institucional para darse de alta en páginas que sean ajenas a las funciones laborales asignadas, excepto cuando se tenga autorización expresa de las personas titulares de las unidades administrativas.

5. POLÍTICA DE GESTIÓN DE LA INFORMACIÓN EN PROCESOS INTERNOS

Se implementarán medidas de gestión de la información apoyados de herramientas tecnológicas que permitan recopilar, almacenar, procesar, distribuir y administrar información de manera eficiente, para con ello contribuir a la transparencia, la rendición de cuentas y el cumplimiento de objetivos institucionales.

5.1 En el Instituto se implementarán y administrarán sistemas de gestión de información según el diseño obtenido para satisfacer las necesidades de consumo de información de las unidades administrativas del Instituto, ubicados en plataformas y soportes informáticos heterogéneos que garanticen su registro, clasificación, distribución, disposición y trazabilidad.

5.2 Los sistemas informáticos implementados en el Instituto serán el medio para la obtención de información de calidad proveniente de fuentes internas y externas, podrán ser desarrollados con recursos propios o tercerizados.

5.3 Se diseñarán e implementarán sistemas de información y comunicación seguros que permitan la generación, obtención, uso y comunicación de información veraz, completa, exacta y accesible, tanto interna como externa.

5.4 La UTIC será la única Unidad Administrativa responsable de la administración, registro, renovación y gestión de los nombres de dominio y subdominios institucionales existentes y nuevos; incluyendo, pero no limitándose a, dominios principales, subdominios para micrositios, sistemas informáticos, correo electrónico y cualquier otro servicio en línea.

5.5 En los sistemas informáticos se hará uso de gestores de bases de datos que regulen la manipulación, y aseguren la organización y recuperación eficiente de la información.

5.6 Para el diseño y desarrollo de sistemas informáticos se deberán tomar en consideración los requerimientos específicos de las unidades administrativas, sus funciones, procesos clave y el entorno en el que operan para alinearlos a los objetivos institucionales de tipo operativos, financieros o de cumplimiento.

5.7 Se creará y mantendrá información escrita que describa los sistemas informáticos, incluyendo su diseño, funcionamiento, uso y mantenimiento.

5.8 Se procurará mantener los procesos de flujo de información internos y externos con herramientas específicas, para garantizar la trazabilidad de los contenidos, tal información debe tener la capacidad de comunicarse a todos los niveles del Instituto.

5.9 Cuando se den intercambios de información confidencial o reservada entre entes internos y externos se emplearán acuerdos de confidencialidad, en los cuales se comprometan las partes a no revelar, ni utilizar para otros fines que no sean los especificados en el acuerdo.

5.10 El Instituto promoverá el uso de plataformas digitales de colaboración y productividad para facilitar la comunicación, coordinación y ejecución de tareas institucionales; de las cuales la UTIC será responsable de administración.

6. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

Establecer los lineamientos para la identificación, evaluación, mitigación, seguimiento y respuesta ante riesgos relacionados con la información, con el fin de garantizar la continuidad operativa, la protección de los activos de información y el cumplimiento de las obligaciones legales y normativas aplicables.

6.1 Identificación y Evaluación de Riesgos

6.1.1 Se deberán realizar evaluaciones periódicas para identificar riesgos asociados al manejo de la información, tales como:

- Pérdida o destrucción de datos
- Acceso no autorizado
- Corrupción o alteración de datos
- Fallos tecnológicos o humanos
- Riesgos derivados de terceros o proveedores
- Capacitación continua en seguridad de la información para el personal del Instituto.

6.1.2 Cada riesgo será evaluado en términos de probabilidad de ocurrencia e impacto potencial, clasificándose en niveles de criticidad (alto, medio, bajo).

6.1.3 Se utilizarán herramientas como matrices de riesgos, entrevistas, análisis de procesos y revisión de incidentes previos.

6.1.4 Las medidas serán revisadas y actualizadas conforme a los resultados de las evaluaciones de riesgo.

6.2 **Mitigación de Riesgos**

Se implementarán medidas administrativas y técnicas que sean de carácter preventivas y correctivas, tales como:

- Establecimiento de políticas, capacitación y segregación de funciones
- Copias de seguridad automáticas y cifradas de información, basadas en las presentes políticas
- Planes de recuperación ante desastres y planes de seguridad
- Controles de acceso físico y lógico
- Monitoreo de sistemas y redes.

6.3 Supervisión y Seguimiento

6.3.1 Se establecerán mecanismos de monitoreo continuo de riesgos y controles implementados

6.3.2 Se realizarán evaluaciones para verificar el cumplimiento de esta política

6.3.3 Se mantendrá un registro actualizado de riesgos, controles y acciones correctivas

6.3.4 Se reportarán periódicamente los resultados a Presidencia

6.4 **Gestión de Incidentes de Seguridad de la Información**

6.4.1 Se definirán procedimientos para la detección, análisis, contención, erradicación y recuperación ante incidentes como:

- Accesos no autorizados
- Pérdida o robo de información
- Ataques cibernéticos (malware, phishing, etc.)
- Fallos en sistemas críticos.

6.4.2 Se establecerán los medios y el equipo de respuesta a incidentes con roles y responsabilidades claras.

6.4.3 Todos los incidentes deberán ser notificados a la UTIC para que sean clasificados, solucionados y documentados.

6.4.4 Los incidentes que vulneren la seguridad institucional serán reportados a las autoridades correspondientes cuando aplique.

7. POLÍTICA DE CAPACITACIÓN Y SENSIBILIZACIÓN

Asegurar que las personas servidoras públicas y terceros conozcan y cumplan las Políticas y Lineamientos de Gestión de la Información y el uso aceptable de recursos informáticos, esto a través de estrategias de capacitación y sensibilización.

Cada servidora o servidor público deberá estar capacitado en los temas siguientes:

- Acceso y claves de accesos (perfiles de usuario)
- Manejo y seguridad de información
- Manejo y seguridad de recursos informáticos
- Riesgos (amenazas) y continuidad en las operaciones
- Lineamientos o planes acorde a su puesto de trabajo

Medios de Capacitación en los que estarán impartidos los temas:

- Manuales
- Videos
- Contenidos en línea
- Cursos
- Etc.

Estos medios podrán ser aplicados de forma presencial o en línea de acuerdo a las necesidades de capacitación.

La capacitación de las personas servidoras públicas se llevará a cabo en los tiempos siguientes:

- Nuevo ingreso, deberá ser capacitado al momento de su ingreso a laborar a la Institución.
- Continuo, deberá ser capacitado en los temas en los que se identifique debilidades o en los casos en que los lineamientos, planes o procesos sufran cambios.

8. POLÍTICA DE GESTIÓN DE PROVEEDORES

Establecer los mecanismos para proteger la información institucional en las relaciones con proveedores de bienes o servicios informáticos, garantizando la confidencialidad, integridad y disponibilidad de los activos de información durante la prestación de servicios o suministro de productos.

8.1 La UTIC debe determinar si el proveedor de servicios o productos tiene la capacidad técnica y experiencia necesarios para asegurar que el Instituto alcance los objetivos planteados y tenga la capacidad de responder a los riesgos asociados.

8.2 La UTIC debe verificar que el proveedor cuente con políticas y controles de seguridad adecuados.

8.3 Toda solicitud de adquisición de bienes informáticos y consumibles deberá ser evaluada previamente por la UTIC, quien emitirá un dictamen técnico que avale la pertinencia, compatibilidad y seguridad del bien solicitado.

8.4 La contratación de personas o empresas externas debe quedar formalizada mediante el establecimiento de instrumentos jurídicos que definan las obligaciones y responsabilidades de las partes involucradas, según la normatividad aplicable para dicho proceso.

8.5 En el Instrumento Jurídico quedará establecida la propiedad intelectual y los derechos de autor, otorgando al Instituto los derechos exclusivos sobre la obra, cuando este aplique.

8.6 Todo Instrumento Jurídico relacionado a proyectos de tecnologías de la información y comunicaciones deberá ser acompañado de los anexos técnicos necesarios que ayude a que las partes involucradas tengan una comprensión clara de las obligaciones y requisitos técnicos del proyecto.

8.7 Las personas o empresas externas firmarán un Acuerdo de Confidencialidad de la Información.

8.8 La UTIC establecerá los mecanismos adecuados para identificar, analizar y evaluar los riesgos potenciales que impidan el cumplimiento de los objetivos, durante este proceso se crearán las estrategias para mitigarlos.

8.9 La UTIC establecerá medidas cuantitativas que permitan evaluar el adecuado desarrollo del proyecto, en función de objetivos planteados; dicha información deberá ser suficiente para identificar oportunidades de mejora y la toma de decisiones acertadas.

8.10 Como parte del seguimiento a los proyectos deberá considerarse reuniones de trabajo periódicas con las persona o empresa en la que se analicen la información cuantitativa y cualitativa que ayude a identificar el correcto cumplimiento de objetivos, la mitigación de riesgos y el acatamiento de responsabilidades contraídas por ambas partes.

8.11 La UTIC dará certidumbre para que la persona o empresa contratada cumpla las normas de conducta que rigen al Instituto.

8.12 Al término del contrato, el proveedor debe devolver o destruir toda la información institucional según se establezca en el Instrumento Jurídico.

8.13 Al finalizar el proyecto, se deberá formalizar la recepción por parte del Instituto, durante dicho proceso se validarán los entregables y se llevará a cabo la aprobación formal para el cierre del proyecto.

9. POLÍTICA DE SOFTWARE

Establecer regulaciones para la adquisición, desarrollo, uso y custodia del software en el Instituto.

Adquisición

9.1 Todo software que se adquiera en el Instituto deberá contar con el dictamen de la UTIC, previo requerimiento del usuario. Este dictamen deberá cumplir con los requerimientos de la Unidad Administrativa solicitante y requerimientos de seguridad. Para el caso de los requerimientos de seguridad, dependerán de un análisis de riesgos.

9.2 Se considerará el uso de software libre siempre y cuando cumpla con las medidas de seguridad lógica establecidas del punto anterior.

9.3 En caso de requerir Aplicaciones con servicios en línea, estas deberán considerar controles adicionales como son el cifrado de información, la autentificación de usuarios.

Desarrollo

9.4 Para el desarrollo de software será necesario la solicitud de la Unidad Administrativa requirente.

9.5 La Unidad Administrativa requirente entregará el proceso técnico operativo y deberá elaborar el documento de requerimientos de necesidades del sistema a desarrollar.

9.6 La UTIC realizará un dictamen de viabilidad; este, deberá considerar los requerimientos de la Unidad Administrativa solicitante, estándares de seguridad y políticas institucionales. Para el caso de los requerimientos de seguridad, dependerán de un análisis de riesgos.

9.7 La UTIC deberá elaborar el Plan de trabajo, Programa de trabajo y para el caso de desarrollo por terceros, un anexo técnico.

9.8 Para el desarrollo de software, la UTIC deberá realizar la metodología de desarrollo, el plan de pruebas por: componente, módulo, aplicación; plan de funcionalidad y/o simulacro y, en su caso, auditoría.

9.9 Para la entrega del software, la UTIC deberá elaborar los manuales necesarios y brindar la capacitación correspondiente al personal que utilizará el software.

Uso

Corresponde a la UTIC determinar el software institucional que debe utilizarse en las distintas actividades de procesamiento de información (datos, audio, y video), para la automatización de oficinas; sistemas operativos, administradores de bases de datos, flujos de trabajo, administrador de contenidos, herramientas de desarrollo, antivirus institucional, etc.

9.1 Solo podrá ser instalado el software correspondiente a las funciones y actividades que se realizan de acuerdo con las atribuciones y necesidades de la Unidad Administrativa usuaria.

9.2 La instalación de software de cualquier tipo será realizada estrictamente por personal de la UTIC, previa solicitud de las personas titulares de las unidades administrativas.

Custodia

9.13 La UTIC será la encargada de supervisar, controlar y administrar todas las licencias de software propiedad del Instituto.

10. POLÍTICA DE RED

Establecer las reglas para el comportamiento de los dispositivos en la red del Instituto.

10.1 Gestión de vulnerabilidad técnica

10.1.1 El acceso a la red institucional está destinado exclusivamente para actividades laborales relacionadas con las funciones del IEEH, por lo que su uso estará disponible únicamente para los activos informáticos propiedad del Instituto por lo que no se permite el uso de la red para fines personales, incluyendo, pero no limitado a:

- Navegación en redes sociales no institucionales.
- Descarga de contenido multimedia o software no autorizado.
- Acceso a plataformas de entretenimiento, juegos en línea o servicios de streaming.
- Uso de servicios de mensajería personal que no estén autorizados por el área de tecnologías.

10.1.2 Las personas servidoras públicas autorizadas obtendrán acceso a la infraestructura de red y activos informáticos, como son:

- Centro de Datos
- Sites
- Servidores de Respaldos
- Bases de Datos
- Infraestructura en la Nube.

10.1.2 La UTIC, establecerá mecanismos para proteger la información contra la acción de agentes externos o vulnerabilidades locales; definiendo controles de acceso para equipo tecnológico externo.

10.1.3 Las licencias y paquetes de software deberán ser resguardados por la UTIC.

10.1.4 El personal adscrito a las unidades administrativas del Instituto evitará la divulgación de las rutas de acceso (URL) de los sistemas institucionales, salvo aquellas que sean de acceso público.

10.1.5 Las rutas de acceso (URL) de los sistemas institucionales serán utilizadas únicamente en equipos autorizados por la UTIC.

10.1.6 Tratándose de activos informáticos arrendados por terceros, la UTIC vigilará que los respaldos de información, traslado y sustitución de equipos, así como el mantenimiento preventivo y correctivo se lleven a cabo conforme a las condiciones especificadas en el contrato con los proveedores respectivos.

11. POLÍTICA DE TELECOMUNICACIONES

La UTIC establecerá los mecanismos de uso y operación de las redes y telecomunicaciones, para mantener la confidencialidad de la información que se transmite a los usuarios, a través de las diferentes tecnologías implementadas en el Instituto.

11.1 Telefonía fija

11.1.1 Las claves telefónicas serán proporcionadas por la UTIC, previa solicitud de las personas titulares de las unidades administrativas, quienes dirigirán un Oficio de dicha solicitud a la DEA.

11.1.2 La clave telefónica será de uso individual e intransferible, las personas titulares de las unidades administrativas informarán a la UTIC, cualquier cambio o baja de las personas servidoras públicas, a los que se les asignó.

11.1.3 Los equipos de telefonía fija serán distribuidos según los requerimientos del área y funciones asignadas a las personas servidoras públicas solicitantes.

11.1.4 Las líneas telefónicas se utilizarán exclusivamente como una herramienta de apoyo a las labores encomendadas, por lo que las llamadas deberán ser breves, utilizando un vocabulario apegado al respeto, moral y buenas costumbres.

11.1.5 La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de telefonía, estará a cargo de la UTIC.

11.2 Telefonía móvil

11.2.1 En el supuesto de que el Instituto proporcione teléfonos móviles, el servicio de telefonía móvil será proporcionado de acuerdo con el cargo y función de las personas servidoras públicas en forma gratuita, por lo cual no se podrá solicitar o dar remuneración alguna por cualquier atención otorgada.

11.2.2 Se establecerán mecanismos de bloqueo (por ejemplo, contraseñas, controles biométricos, patrones, etc.) para los equipos de telefonía móvil institucional que sean asignados al personal. Se Instalará una aplicación que permita al Instituto gestionar y proteger los dispositivos móviles.

11.2.3 La instalación, desinstalación, configuraciones, mantenimiento preventivo y correctivo de los equipos de telefonía móvil, estará a cargo del Instituto.

11.2.4 En el uso de teléfonos móviles, las personas servidoras públicas deberán mantener un lenguaje apegado al respeto, moral y buenas costumbres.

11.2.5 Se prohíbe a las personas servidoras públicas el uso de telefonía móvil ajena a la asignada, a excepción de que cuenten con la autorización expresa de su superior inmediato o de las y las personas titulares de las unidades administrativas.

11.2.6 El uso y cuidado del equipo de telefonía móvil es responsabilidad exclusiva de las personas servidoras públicas, a quienes se les asigna.

11.2.7 Las personas servidoras públicas que tengan asignado equipo de telefonía móvil deberán reportar a la UTIC toda falla que presente el equipo.

11.2.8 Las personas servidoras públicas deberán cubrir cualquier gasto generado por reparación del equipo móvil, cuando se detecte que fue dañado por descuido, o negligencia propia.

11.2.9 Las personas servidoras públicas mantendrán actualizados los dispositivos móviles institucionales asignados.

11.3 Redes inalámbricas

Las personas servidoras públicas y terceros requerirán autorización expresa de la UTIC para el acceso a las redes inalámbricas, previa justificación de la solicitud.

11.3.1 Se establecerán procedimientos de autorización y controles para la administración de accesos a las redes inalámbricas, siendo la UTIC, la encargada de esta función.

11.3.2 La UTIC, creará perfiles para el uso de las redes inalámbricas en las unidades administrativas del Instituto.

11.3.3 Se verificarán los perfiles de acceso asignado a las personas servidoras públicas, con el fin de revisar que se les permita el acceso a aquellos recursos que les fueron autorizados.

11.3.4 Para la conexión a la red institucional vía inalámbrica de equipos de cómputo o dispositivos móviles que no sean propiedad del Instituto, las personas titulares de las unidades administrativas, deberá solicitarlo de manera Oficial a la UTIC. Siendo responsabilidad de la persona titular, el uso que se les dé a estos equipos o dispositivos móviles.

11.4 Videoconferencia

11.4.1 Las personas servidoras públicas utilizarán el equipo de videoconferencia para apoyo de sus laborales asignadas, para fines académicos, o actividades que se justifiquen.

11.4.2 Las personas titulares de las unidades administrativas o el personal que designe solicitarán el servicio de videoconferencia de manera anticipada, a fin de verificar su disponibilidad.

11.4.3 Las personas titulares de las unidades administrativas del Instituto que soliciten el equipo de videoconferencia serán responsables del uso adecuado del mismo.

11.4.4 La configuración del equipo de videoconferencia se solicitará a la UTIC.

11.4.5 El personal que participe en la videoconferencia es responsable de la información que se comparta durante la transmisión.

11.5 Internet

11.5.1 La UTIC establecerá las configuraciones autorizadas para los dispositivos que hagan uso de los servicios de internet provistos por el Instituto.

11.5.2 La UTIC otorgará permisos para la navegación a través del servicio de internet, en función de las labores encomendadas a los usuarios, asegurándose de que los equipos que utilicen el servicio sean propiedad del Instituto y cuenten con software antivirus.

11.5.3 Las personas servidoras públicas evitarán hacer uso de servicios de internet público en equipos institucionales (Laptop).

11.5.4 Las personas servidoras públicas y terceros estarán impedidos para compartir o divulgar contraseñas de acceso al servicio de internet que se les haya instalado en sus equipos.

11.5.5 Las personas servidoras públicas y terceros deberán evitar cambiarse a redes de servicio a internet, a las que no estén autorizados.

11.5.6 Las personas servidoras públicas y terceros utilizarán el servicio de red de internet, únicamente para asuntos relacionados con el ámbito laboral.

11.5.7 Las personas servidoras públicas y terceros informarán de manera oportuna a la UTIC sobre el cambio o baja del dispositivo conectado al servicio de internet, así como del cambio de adscripción o baja de la institución del usuario.

11.5.8 Los accesos a la red inalámbrica para visitantes solo tendrán permisos temporales, por lo que se darán de baja de acuerdo con la temporalidad solicitada.

11.6 Redes LAN

11.6.1 La UTIC establecerá procedimientos de autorización y controles para asegurar los accesos a las redes de datos y los recursos de red disponibles en el Instituto.

11.6.2 La UTIC otorgará permisos según el perfil y necesidades para el uso de los recursos de red del Instituto, y será quien brinde el soporte y la atención solicitada en el tema.

11.6.3 La UTIC verificará los permisos de acceso para el personal, con el fin de revisar que tengan acceso únicamente a aquellos recursos de red y servicios de la plataforma tecnológica a los que les fueron asignados.

11.6.4 Las personas servidoras públicas y terceros, antes de contar con acceso lógico por primera vez a la red de datos del Instituto, deberán contar con el procedimiento de creación de cuentas de usuario debidamente autorizado.

11.6.5 Las personas servidoras públicas que se conecten a las redes deberán cumplir con los requisitos o controles para autentificarse en ellas.

11.6.6 La UTIC planeará y desarrollará los proyectos tecnológicos en materia de redes LAN, como parte de los servicios de seguridad de las Tecnologías de Información del Instituto.

11.6.7 La UTIC evaluará constantemente las diferentes tecnologías en materia de telecomunicaciones existentes en el mercado con la finalidad de implementar mejoras que garanticen la eficiencia y seguridad en las redes LAN.

11.6.8 La UTIC será quien defina el uso de las redes LAN, y los controles de seguridad asociados, además garantizará los servicios de voz y datos en las unidades administrativas del Instituto.

11.6.9 La UTIC proporcionará el medio de enlace local para brindar servicios de internet, voz, video y datos de forma segura para las unidades administrativas.

11.6.10 La UTIC impulsará el desarrollo de aplicativos tecnológicos en código abierto (open source), para proporcionar servicios confiables y robustos a las unidades administrativas.

11.6.11 La UTIC controlará los equipos de comunicaciones locales, servidores y sites de comunicaciones, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la integridad de la información.

11.6.12 La UTIC coordinará el mantenimiento preventivo y correctivo en materia de comunicaciones, voz, datos, y video, de los servicios de red proporcionados a las unidades administrativas.

11.7 Redes WAN (Fibra óptica y microondas)

11.7.1 La UTIC, cuando se requiera, planeará y desarrollará los proyectos tecnológicos en materia de redes WAN como parte de los servicios de seguridad de las tecnologías de información y comunicaciones del Instituto.

11.7.2 La UTIC evaluará constantemente los procedimientos de trabajo en materia de telecomunicaciones y seguridad de las redes WAN del Instituto.

11.7.3 La UTIC será la única que definirá el uso de las redes WAN, así como la seguridad en este medio.

11.7.4 La UTIC garantizará los servicios de voz, video y datos en las unidades administrativas del Instituto mediante las redes WAN.

11.7.5 La UTIC evaluará la posibilidad de impulsar y desarrollar servicios tecnológicos a través de redes virtuales privadas (VPN), para proporcionar servicios confiables, robustos y con un costo accesible.

11.7.6 La UTIC controlará los equipos de comunicaciones, servidores y sites de comunicaciones de las redes WAN, con la finalidad de salvaguardar los activos informáticos, así como de garantizar la confidencialidad e integridad de la información.

11.7.7 La UTIC coordinará el mantenimiento preventivo y correctivo en materia de comunicaciones, voz, datos, video y seguridad de las redes WAN del Instituto.

11.7.8 La UTIC estará en constante monitoreo de las redes WAN a fin de brindar un servicio confiable y eficaz para los diferentes edificios pertenecientes al Instituto.

11.7.9 La UTIC dará aviso al o los proveedores encargados de la infraestructura exterior en caso de cortes o actos vandálicos en antenas de microondas o fibra óptica, que afecten las comunicaciones a nivel WAN entre edificios pertenecientes al Instituto.

12. POLÍTICA DE CUMPLIMIENTO

Establecer las reglas para el uso seguro y adecuado de los recursos tecnológicos del Instituto conforme a la normatividad vigente en materia de tecnología.

Las Políticas y Lineamientos en la Gestión de Sistemas de Información y Comunicaciones para el uso, desarrollo o actualización en Tecnologías de la Información y Comunicaciones del Instituto y sus procedimientos deberán regirse bajo el marco legal estipulado en este documento, así como las leyes, regulaciones y normas aplicables al Instituto; asegurando su alineación al Plan Estratégico Institucional y sus objetivos.

Se deberá revisar y actualizar la política periódicamente para reflejar, en su caso, los cambios en las regulaciones vigentes en concordancia con los cambios en la infraestructura o evolución tecnológica a fin de proteger los activos del Instituto, garantizar

la seguridad de la información, cumplir con las leyes y regulaciones, y promover un uso responsable de las tecnologías de la información y comunicación.

Sanciones por Incumplimiento

La inobservancia a lo establecido en el presente documento y demás disposiciones aplicables en la materia, será sancionada administrativa y/o penalmente por las autoridades facultadas para sustanciar el procedimiento administrativo y/o penal respectivo, en los términos de la Ley de Responsabilidades Administrativas del Estado de Hidalgo, el Código Penal para el Estado de Hidalgo y demás normatividad vigente aplicable en la materia. Además, para el incumplimiento de las normas se aplicarán los siguientes criterios:

- De primera vez en el incumplimiento en una determinada Política o Lineamiento se notificará por escrito a la persona responsable de la falta y se le sensibilizará respecto de la normatividad aplicable.

- De presentarse un segundo incumplimiento en la misma Política o Lineamiento por el mismo usuario, se notificará por escrito a su superior inmediato informándole la falta.

- En el caso de reincidir por tercera ocasión en el incumplimiento de la política o lineamiento por parte del usuario, se turnará a las instancias superiores. Adicionalmente la UTIC se reserva el derecho de suspender el acceso a los servicios vulnerados de manera inmediata.

Derechos de propiedad intelectual: Se garantizará el respeto y la protección de los derechos de autor y licencias de software, contenidos digitales y desarrollos tecnológicos utilizados por la entidad.

Protección de los registros: Se establecerán controles para asegurar la integridad, disponibilidad y confidencialidad de los registros administrativos, financieros y operativos.

Protección de los datos y privacidad de la información personal: Se aplicarán los principios de licitud, finalidad, proporcionalidad y responsabilidad en el tratamiento de datos personales, conforme a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Regulación de los controles criptográficos: Se implementarán mecanismos criptográficos para proteger la información sensible, incluyendo cifrado de datos, firmas digitales y autenticación segura.

Revisión independiente de la seguridad de la información: Se realizarán revisiones periódicas para evaluar la eficacia de los controles de seguridad.