MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Gestión Tecnológica y Comunicaciones

INTRODUCCIÓN

La seguridad informática es hoy en día una disciplina y una práctica que toda organización sin importar su dimensión (Grande, Medina o Pequeña), debe desarrollar intrínsecamente con el fin blindar las operaciones que se apalanquen a través de la infraestructura tecnológica con la que se dispone.

El Manual de Políticas de Seguridad de la Información es un conjunto de directrices, normas y procedimientos que guía las actuaciones de trabajo y define los criterios de seguridad para que sean adoptados por la institución, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como en el tecnológico. A partir de sus principios, es posible hacer de la seguridad de la información un esfuerzo común, en tanto que todos puedan contar con un documento informativo y normalizado, dedicado al cómo debería ser la operación de cada uno de las personas involucradas en la gestión de la seguridad de la información.

La información del INFOTEP debe protegerse de acuerdo a su valor e importancia. Deben emplearse medidas de seguridad sin importar como se guarda la información (en papel o en forma electrónica) o como se procesa (PCs, servidores, correo de voz, etc.), o como se transmite (correo electrónico, conversación telefónica). Tal protección incluye restricciones de acceso a los usuarios según su cargo.

El personal encargado de la seguridad debe llevar a cabo cada año, un análisis de riesgos y revisar las políticas de seguridad con el fin de mantearlas actualizadas, por otro lado debe capacitar y dar información a los funcionarios y contratistas sobre temas de seguridad de la información para que ellos puedan proteger y manejar adecuadamente los recursos informáticos de la institución.

El objetivo de las políticas de seguridad de la información es proporcionar instrucciones específicas sobre cómo mantener más segura la información de la institución. El no cumplimiento de dichas políticas puede acarrear medidas disciplinarias.

TABLA DE CONTENIDO

OBJETIVO

Brindar los lineamientos que deben seguir los funcionarios, colaboradores y terceros que permitan proteger la Información del INFOTEP, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital.

MARCO NORMATIVO

ISO 27001	Estándar para la seguridad de la información. Permite el aseguramiento, la confidencialidad e integridad de los datos y de la información
DECRETO 1008 DE 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley 594 de 2000.	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
Decreto 1747 de 2000.	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: “Las entidades de certificación, los certificados y las firmas digitales”.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Decreto 2573 del 12 de diciembre de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Directiva presidencial 02 de 2012	Derechos de Autor y los derechos conexos, "Utilización de software o programas informáticos"

ALCANCE

El alcance de las Políticas de Seguridad y Privacidad de la información del Instituto Nacional de Formación Técnica Profesional INFOTEP de San Andrés Islas aplica a toda la entidad, sus funcionarios, estudiantes, contratistas y terceros del INFOTEP y la ciudadanía en general.

RESPONSABLE:

Área de Tecnologías de la información y las comunicaciones - Oficial de Seguridad.

NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa del INFOTEP SAI incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

DEFINICIONES

Para efectos de la comprensión la política de seguridad de la Información del Instituto Nacional de Formación Técnica Profesional, se establecen los siguientes significados de las palabras empleadas en el texto:

- **Seguridad de la Información:** se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan. (ISO27001).
- **Políticas:** directrices u orientaciones por las cuales la alta dirección define el marco de actuación con el cual se orientará la actividad pública en un campo específico de su gestión, para el cumplimiento de los fines constitucionales y misionales de la entidad, de manera que se garantice la coherencia entre sus prácticas y sus propósitos.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

1.1. POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

1.1.1. *POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN*

La dirección de INFOTEP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para INFOTEP, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la

disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica al INFOTEP SAI según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de su comunidad académica y funcionarios.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y toda la comunidad académica del INFOTEP.
- Garantizar la continuidad del servicio frente a incidentes.
- INFOTEP ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la institución, y a los requerimientos regulatorios.

1.1.2. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

El INFOTEP se compromete a otorgar los recursos necesarios para garantizar y dar cumplimiento a la ley 1581 de 2012 sobre protección de datos personales.

El INFOTEP tiene presente que los datos personales son de propiedad de las personas a las que se refieren y solamente ellas pueden decidir sobre los mismos. Así mismo, se hará uso de dichos datos solamente para las finalidades para las que se encuentra debidamente facultada.

1.1.3. *POLÍTICA DE ROLES Y RESPONSABILIDADES*

Objetivo: Definir los Roles y Responsabilidades en Seguridad de la Información en el INFOTEP.

Todos los funcionarios, colaboradores y terceros que ejercen funciones en el INFOTEP y previamente han sido autorizados para acceder a los recursos tecnológicos y de procesamiento de información de la Entidad, son responsables del cumplimiento de las políticas, procedimientos y normatividad vigente definida por el INFOTEP.

Es responsabilidad de todos los funcionarios, colaboradores y terceros almacenar la información en la carpeta designada para ello(Google Drive), los documentos resultado de sus funciones laborales, ya que de esta forma se garantiza las copias de respaldo, lo que no se encuentre allí no queda dentro de la política.

Todos los funcionarios, colaboradores y terceros del INFOTEP deben hacer buen uso de la información que se genera del desempeño de sus funciones laborales y bajo ninguna circunstancia podrán divulgar información con categoría CONFIDENCIAL o RESERVADA en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre del INFOTEP. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por el INFOTEP.

Todos los activos de información del INFOTEP deben tener su propietario, su custodio y usuarios que deben estar debidamente identificados.

El proceso de gestión tecnológica y comunicaciones, Talento Humano y Seguridad de la Información, deben definir la Matriz de Roles y Responsabilidades para cada activo de sistemas de información e infraestructura tecnológica, en la cual se deben incluir los roles y sus privilegios, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.

Si después de revisar la solicitud, se identifica que los privilegios solicitados no están definidos en la Matriz de Roles y Responsabilidades de los activos de información, se debe solicitar aprobación por parte del dueño del activo.

Todas las solicitudes deben tener fecha de finalización y cuando sean roles que no se encuentren en la Matriz serán considerados como Privilegios Temporales.

El proceso de gestión tecnológica y comunicaciones debe informar a través de los mecanismos de comunicación seleccionados, que el usuario fue creado y que fueron asignados los privilegios solicitados.

Se debe capacitar a todos los usuarios solicitantes de accesos a componentes tecnológicos sobre el uso y la responsabilidad que implica contar con esos privilegios.

La Matriz de Roles y Responsabilidades debe ser actualizada periódicamente o cada vez que surja un cambio, de acuerdo a un requerimiento formal por parte del Líder del Proceso o Responsable del Activos de Información.

Todos los requerimientos deben ser solicitados formalmente a través del procedimiento establecido de creación de cuentas de usuarios.

1.1.4. *POLÍTICA DE DISPOSITIVOS MÓVILES*

Objetivo: Proteger la información almacenada en dispositivos móviles de los funcionarios del INFOTEP SAI.

Todos los dispositivos móviles propiedad de los funcionarios, colaboradores y terceros, que requieran tener acceso a los componentes tecnológicos como el correo electrónico del INFOTEP SAI, deben solicitar autorización mediante el procedimiento formal de autorización de ingreso a la red y estar debidamente identificados, con el fin de llevar el control y garantizar que se implementen las medidas de aseguramiento necesarias definidas por el proceso de Tecnologías de Información y las Comunicaciones, de esta forma se puede garantizar la preservación de la disponibilidad, confidencialidad e integridad de la información del INFOTEP.

1.1.5. *SEGURIDAD DE LOS RECURSOS HUMANOS*

Objetivo: Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del personal que trabaja para el INFOTEP, a través de mecanismos de validación y concientización del recurso humano que hará uso de la misma.

Control y Política del Personal

Se deben definir controles de verificación del personal en el momento en que se postula al cargo. Estos controles incluirán todos los aspectos legales y de procedimiento que dicta el proceso de contratación del INFOTEP.

Acuerdo de Confidencialidad

Todos los funcionarios del INFOTEP y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de INFOTEP a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

Selección de personal

Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes, de acuerdo a la reglamentación.

Se deben aplicar los controles establecidos por el INFOTEP SAI para otorgar el acceso a la información CONFIDENCIAL o RESERVADA por parte del personal que resulte vinculado a la misma.

El área de Talento humano y Contratación son los responsables de realizar la verificación de antecedentes disciplinarios, fiscales y judiciales y que se anexe la documentación requerida para la contratación.

Términos y condiciones Laborales

Todos los funcionarios, colaboradores y terceros del INFOTEP SAI deben dar cumplimiento a las políticas y normatividad establecida en seguridad y privacidad de la información y debe ser parte integral de los contratos o documentos de vinculación a que haya lugar.

Todos los funcionarios, colaboradores y terceros, durante el proceso de vinculación al INFOTEP SAI, deberán recibir una inducción sobre las Políticas y Lineamientos de Seguridad y Privacidad de la Información.

Entrenamiento, concientización y capacitación

Todos los funcionarios, colaboradores y terceros del INFOTEP deben ser entrenados y capacitados para las funciones, actividades y cargos que van a desempeñar, esto con el fin de sensibilizar a los usuarios sobre la protección adecuada de los recursos y la información de la Entidad. Así mismo, se debe garantizar la comprensión del alcance y contenido de las políticas y lineamientos de Seguridad de la información y la necesidad de respaldarlas y aplicarlas de manera permanente e integral desde su función.

Formación y Capacitación en Materia de Seguridad de la Información

Todos los funcionarios, colaboradores y terceros cuando sea el caso, que trabajan para el INFOTEP SAI deben recibir una adecuada capacitación y actualización periódica en materia de las políticas, normas y procedimientos de Seguridad y privacidad de la Información. Dentro del contenido se deben contemplar los requerimientos de seguridad y las responsabilidades legales, así como la capacitación sobre el uso adecuado de las instalaciones de procesamientos de información y los recursos tecnológicos informáticos que les provee la Entidad para el desempeño de sus funciones laborales y contractuales.

Procesos disciplinarios

Todos los incidentes de seguridad de la información presentados en el INFOTEP deben tener el tratamiento adecuado y establecido en el procedimiento de atención de incidentes de seguridad de la información, con el fin de determinar sus causas y responsables.

Del resultado de los procesos derivados de los reportes y del análisis de los Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

1.1.6. *POLÍTICA DE USO DE CORREO ELECTRÓNICO*

Objetivo: Definir las directrices generales del buen uso del correo electrónico en el INFOTEP.

Usos aceptables del servicio

Se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales a desempeñar en el INFOTEP y no se debe utilizar para otros fines.

Se debe utilizar de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información e imagen de la INFOTEP.

Todos los funcionarios, colaboradores y terceros que son autorizados para acceder a la red de datos y los componentes de Tecnologías de Información son responsables de todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.

Todos los funcionarios, colaboradores y terceros deben dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos, así mismo evitar prácticas o usos que puedan comprometer la seguridad de la información del INFOTEP.

El servicio de correo electrónico debe ser empleado para servir a una finalidad operativa y administrativa en relación con el INFOTEP. Todas las comunicaciones establecidas mediante este servicio, sus buzones y copias de seguridad se consideran de propiedad del INFOTEP y pueden ser revisadas por el administrador del servicio o cualquier instancia de vigilancia y control, en caso de una investigación o incidentes de seguridad de la información.

Cuando un Proceso tenga información de interés institucional para divulgar, lo debe hacer a través del área de Comunicaciones del INFOTEP o el medio formal autorizado para realizar esta actividad.

Todos los mensajes enviados deben respetar el estándar de formato e imagen institucional definido por el INFOTEP y deberán conservar en todos los casos el mensaje legal institucional.

El único servicio de correo electrónico controlado en la entidad es el asignado directamente por el área de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

Los demás servicios de correo electrónico son utilizados bajo responsabilidad directa y riesgo de los usuarios.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo a los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo a la Clasificación y Etiquetado de la Información establecida en el INFOTEP SAI.

El tamaño del buzón de correo electrónico se asigna de manera estandarizada, la capacidad específica es definida y administrada por el área de Tecnologías de la Información y las Comunicaciones.

Todos los funcionarios, colaboradores y terceros son responsables de informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro del INFOTEP, para que de esta forma el área de Tecnologías de la Información y las Comunicaciones realicen el ajuste de permisos requerido.

El usuario debe reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus al área de Tecnologías de la Información y las Comunicaciones, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así el área de Tecnologías de la Información y las Comunicaciones hacen el análisis para evaluar el origen y así tomar las medidas pertinentes.

Cuando un usuario se retire del INFOTEP, y se le haya autorizado el uso de una cuenta con acceso a la red y al servicio de correo de la institución, debe abstenerse de continuar empleándolas y debe verificar que su cuenta y acceso a los servicios sean cancelados.

Los mensajes y la información contenida en los buzones de correo son de propiedad del INFOTEP.

Cada usuario se debe asegurar que en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son. Si tiene listas de distribución también se deben depurar. El envío de información a personas no autorizadas es responsabilidad de quien envía el mensaje de correo electrónico.

Las cuentas institucionales (Ejemplo: Comunicaciones, Servicio Cliente, Apoyo sistemas, control interno etc.) deben tener una persona responsable que haga depuración del buzón periódicamente.

Todo usuario es responsable de reportar los mensajes cuyo origen sean desconocidos, y asume la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En los casos en que el Funcionario, Colaborador o Tercero desconfíe del remitente de un correo electrónico debe remitir la consulta al Fresh Desk (sistema de tickets para la solución de problemas).

Si una cuenta de correo es interceptada por personas mal intencionado o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), el área de Tecnologías de la Información y Comunicaciones actuará según sea el caso.

El área de Tecnologías de la Información y las Comunicaciones se reserva el derecho de filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo.

Ningún Funcionario, Colaborador o Tercero debe suscribirse en boletines en líneas, publicidad o que no tenga que ver con sus actividades laborales, con el correo institucional.

El Funcionario, Colaborar o Tercero no debe responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario debe notificar al área de Tecnologías de la Información y las Comunicaciones, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo del INFOTEP.

Todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.

Usos no aceptables del servicio

Envío, reenvío o intercambio de mensajes no deseados o considerados como SPAM, cadena de mensajes o publicidad.

Envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

Envío o intercambio de mensajes que promuevan la discriminación sobre la raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de activos.

Envió de mensajes que contengan amenazas o mensajes violentos.

Divulgación no autorizada de información propiedad del INFOTEP.

Enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización.

Abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización.

Adulterar o intentar adulterar mensajes de correo electrónico.

Cualquier otro propósito inmoral, ilegal o diferente a los considerados en el apartado “Usos aceptable del servicio” de la presente política.

1.1.7. *POLÍTICA DE USO DE INTERNET*

Objetivo: Definir los lineamientos generales para el buen uso del internet y asegurar una adecuada protección de la información.

Usos aceptables del servicio

Este servicio debe utilizarse exclusivamente para el desempeño de las funciones y actividades desarrolladas durante la contratación en el INFOTEP y no debe utilizarse para ningún otro fin.

Los usuarios autorizados para hacer uso del servicio de Internet son responsables de evitar prácticas o usos que puedan comprometer los recursos tecnológicos de la Entidad o que afecte la seguridad de la información del INFOTEP.

Todas las comunicaciones establecidas mediante este servicio pueden ser revisadas y/o monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control.

El navegador autorizado para el uso de Internet en la red del INFOTEP es el instalado por la Oficina de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.

No se permite la conexión de módems externos o internos en la red del INFOTEP.

Todo usuario es responsable de informar el acceso a contenidos o servicios no autorizados o que no correspondan al desempeño de sus funciones o actividades dentro del INFOTEP.

Para realizar intercambio de información de propiedad del INFOTEP con otras entidades, se debe seguir un proceso formal de requisición de la información, el cual debe contar con la previa autorización del dueño de la información.

EL INFOTEP se reserva el derecho de realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.

Todos los usuarios que se encuentren autorizados son responsables de dar un uso adecuado de este recurso y por ninguna razón pueden hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, la seguridad de la información, entre otros.

Los funcionarios y colaboradores y tercero del INFOTEP SAI no deben asumir en nombre de esta, posiciones personales en encuestas de opinión, foros u otros medios similares.

Este recurso puede ser utilizado para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información del INFOTEP.

Usos no aceptables del servicio

Envío o descarga de información masiva de un tamaño grande o pesado que pueda congestionar la red a menos que el desempeño de las funciones lo amerite.

Envío, descarga o visualización de información con contenidos restringidos y que atenten contra la integridad moral de las personas o instituciones.

Cualquier otro propósito diferente al considerado en el apartado de Usos aceptables del servicio de la presente política.

Todos los usuarios invitados que tengan acceso al servicio de internet, deben cumplir estrictamente con las políticas de seguridad de la información, de lo contrario asumirán las acciones pertinentes.

No se permite la descarga, uso, intercambio o instalación de juegos, música, videos, películas, imágenes, protectores y fondos de pantalla, software de libre distribución, información o productos que atenten contra la propiedad intelectual, archivos ejecutables que comprometan la seguridad de la información, herramientas de hacking, entre otros.

1.1.8. *POLÍTICA DE USO DE REDES SOCIALES*

Objetivo: Definir los lineamientos generales para el uso del servicio de Redes sociales por parte de los usuarios autorizados en el INFOTEP.

Usos aceptables del servicio

Todos los usuarios autorizados para hacer uso de los servicios de Redes Sociales son responsables de evitar prácticas o usos que puedan comprometer la seguridad de la información del INFOTEP.

El servicio autorizado debe ser utilizado exclusivamente para el desarrollo de las actividades relacionadas con el INFOTEP. Todas las comunicaciones establecidas mediante este servicio pueden ser monitoreadas por el administrador del servicio o cualquier instancia de vigilancia y control que lo requiera.

Es permitido el uso de redes sociales utilizando video conferencia y streaming (descarga de audio y video), siempre y cuando no interfiera o altere la operación normal de los sistemas de información del INFOTEP SAI.

EL INFOTEP facilita el acceso a estas herramientas, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medio y para el desempeño de las funciones y actividades a desempeñar por parte de funcionarios, colaboradores y terceros , sin embargo es necesario hacer buen uso de estas herramientas de forma correcta y moderada.

No se deben descargar programas ejecutables o archivos que puedan contener software o código malicioso.

No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo a través del servicio de Redes Sociales.

No se debe practicar e intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de Internet del INFOTEP, o aprovechar el acceso a Redes Sociales para fines ilegales.

Es claro que no se puede difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.

Todos los funcionarios, colaboradores y terceros del INFOTEP, deben seguir los procedimientos y planes de comunicaciones interna y externa.

El área de Tecnologías de la Información y las Comunicaciones, será el encargado de determinar las directrices y lineamientos para el uso de las diferentes herramientas o plataformas de redes sociales en el INFOTEP, previo acuerdo con el Proceso de Gestión con Grupos de Interés y Comunicaciones.

1.1.9. *POLÍTICA DE USO DE RECURSOS TECNOLÓGICOS*

Objetivo: Definir los lineamientos generales para el uso aceptable de los recursos tecnológicos del INFOTEP SAI.

Usos aceptables del servicio

El INFOTEP SAI asigna los recursos tecnológicos necesarios como herramientas de trabajo para el desempeño de las funciones y actividades laborales de los funcionarios, colaboradores y terceros de ser necesario.

El uso adecuado de estos recursos se establece bajo los siguientes criterios:

La instalación de software se encuentra bajo la responsabilidad del área de Tecnologías de la Información y las Comunicaciones y por tanto son los únicos autorizados para realizar esta actividad.

Ningún usuario debe realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo. Estos cambios únicamente deben ser realizados por el área de Tecnologías de la Información y las Comunicaciones.

El área de Tecnologías de la Información y las Comunicaciones es el responsable de definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en el INFOTEP SAI para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación del cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo el personal autorizado por el área de Tecnologías de la Información y las Comunicaciones podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del INFOTEP;

las conexiones establecidas para este fin, utilizan los esquemas de seguridad establecidos por la entidad.

Los funcionarios, colaboradores y terceros del INFOTEP SAI son responsables de hacer buen uso de los recursos tecnológicos del INFOTEP y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros funcionarios, colaboradores y terceros, legislación vigente y políticas y lineamientos de seguridad de la información establecidas por el INFOTEP.

La información clasificada como personal almacenada en los equipos de cómputo, medios de almacenamiento o cuentas de correo institucionales, debe ser guardada en su totalidad en una carpeta especificada para tal fin, la cual debe ser nombrada como "PERSONAL".

Todo activo de propiedad del INFOTEP, asignado a sus funcionarios, colaboradores y terceros del INFOTEP, debe ser entregado al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), y la información que tenga almacenada en dispositivos removibles.

1.1.10. *POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN*

Objetivo: Asegurar que la información del INFOTEP SAI es clasificada, con el fin de que sea tratada y protegida adecuadamente.

Esquema de Clasificación de la Información

Toda la información del INFOTEP debe ser identificada y clasificada de acuerdo a los niveles de clasificación definidos por la entidad.

El área de Tecnologías de la Información y las Comunicaciones, Gestión Documental y Gestión Legal administrativa y financiera son los responsables de definir las directrices de clasificación de la información y las medidas de tratamiento y manejo de la información.

De acuerdo a la clasificación establecida por el INFOTEP SAI el manejo y almacenamiento de la información, se debe tener en cuenta lo siguiente:

- Acceso a la información sólo de personal autorizado.
- Llevar un registro formal de acceso a la información.
- Conservar y mantener los medios de almacenamiento de información en un ambiente seguro.

Etiquetado y manejo de Información

Todos los funcionarios, colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por Gestión Documental.

Rector, Vicerrector y Coordinadores deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los funcionarios, colaboradores y terceros cuando sea el caso del INFOTEP SAI son responsables de la organización, conservación, uso y manejo de los documentos.

Los archivos de Gestión de las oficinas del INFOTEP deben custodiar sus documentos de acuerdo a lo especificado en las tablas de Retención Documental.

La plataforma tecnología usada para salvaguardar, conservar y facilitar la información de los documentos en medios magnéticos, debe garantizar los principios fundamentales de la seguridad como son la integridad, confidencialidad y disponibilidad de la información y por gestión documental usabilidad y acceso.

Se debe definir procedimientos de etiquetado de la información, de acuerdo con el esquema de clasificación definido por el INFOTEP.

El etiquetado de información debe incluir la información física y electrónica.

Las etiquetas de la información, se deben identificar y reconocer fácilmente.

Se debe garantizar la conservación, uso y recuperación de la información contenida en medios digitales, físicos y otros.

Usos no aceptables

Hacer caso omiso, retardar o no entregar de manera oportuna las respuestas a las peticiones, quejas, reclamos y solicitudes de igual forma retenerlas o enviarlas a un destinatario que no corresponde o que no esté autorizado, que lleguen por los diferentes medios, presencial, verbal, escrito, telefónico, correo y web.

Dañar o dar como perdido los documentos o archivos que se encuentren bajo su administración por la naturaleza de su cargo.

Divulgación no autorizada de los documentos, información o archivos.

Realizar actividades tales como borrar, modificar, alterar o eliminar información del INFOTEP de manera malintencionada.

1.1.11. *POLÍTICA DE GESTIÓN DE MEDIOS DE ALMACENAMIENTO*

Objetivo: Proteger la información del INFOTEP velando por la protección de la confidencialidad, integridad y disponibilidad de la información que se encuentra en unidades de almacenamiento.

Gestión y Disposición de medios removibles

Todos los dispositivos y unidades de almacenamiento removibles, tales como cintas, CD's, DVD's, dispositivos personales "USB", discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red del INFOTEP SAI uso hasta finalización de su contrato o cese de actividades.

Toda la información clasificada como CONFIDENCIAL o RESERVADA que sea almacenada en medios removibles y que se requiera de protección especial, debe cumplir con las directrices de seguridad emitidas por el área de Tecnologías de la Información y las Comunicaciones.

El área de Tecnologías de la Información y las Comunicaciones puede restringir que medios de almacenamiento removibles se conecten a los equipos de cómputo que sean propiedad del INFOTEP o que estén bajo su custodia, y puede llevar a cabo cualquier acción de registro o restricción, con el fin de evitar fuga de información a través de medios removibles.

Los medios de almacenamiento removibles que se conecten a la red de datos del INFOTEP o que se encuentren bajo su custodia, están sujetos a monitoreo por parte del área de Tecnologías de la Información y las Comunicaciones.

Todos los retiros de medios de almacenamiento de las instalaciones del INFOTEP, como discos duros externos, se deben realizar con la autorización del propietario del proceso misional, estratégico, mejora continua o de apoyo, definidos de acuerdo al mapa de procesos del INFOTEP, a través del formato orden de salida de elementos.

Todos los medios de almacenamiento removibles propiedad del INFOTEP, deben estar almacenados en un ambiente seguro.

Se debe hacer seguimiento a los medios de almacenamiento removibles como Discos Duros con el fin de garantizar que la información sea transferida a otro medio antes de que esta quede inaccesible por deterioro o el desgaste que sufren a causa de su vida útil.

Borrado seguro

Todos los medios de almacenamiento que sean de propiedad de terceros y que sean autorizados por el INFOTEP para su uso dentro de la red de la institución, deben contar con su respectivo soporte.

Todos los medios de almacenamiento que contengan información del INFOTEP y que salgan de la misma que no se les vaya a dar más uso, deben seguir el procedimiento de borrado seguro definido por el INFOTEP, el cual garantiza que la información no es recuperable (Aplica para medios de almacenamiento de equipos, discos duros externos, etc.).

Los medios de almacenamiento que contengan información del INFOTEP SAI que vayan a ser dados de baja o reutilizados, deben seguir el procedimiento de borrado seguro definido

por el INFOTEP, el cual garantiza que la información no se es recuperable (Aplica para medios de almacenamiento externos o de equipos que son reasignados, formateados, reinstalados o que por degaste o falla son retirados o dados de baja).

Eliminar de forma segura (destrucción o borrado) los medios de almacenamiento que no se utilicen y que contengan información del INFOTEP SAI.

POLÍTICA DE CONTROL DE ACCESO

Objetivo: Definir las directrices generales para un acceso controlado a la información del INFOTEP SAI.

Control de Acceso a Redes y Servicios en Red

El INFOTEP SAI suministra a los usuarios las contraseñas de acceso a los servicios de red, servicios y sistemas de información que requiera para el desempeño de sus funciones laborales.

Las claves son de uso personal e intransferible y es responsabilidad del usuario el uso de las credenciales asignadas.

Sólo el personal designado por el área de Tecnologías de la Información y las Comunicaciones está autorizado para instalar software o hardware en los equipos, servidores e infraestructura de tecnología del INFOTEP.

Todo actividad que requiera acceder a los servidores, equipos o a las redes del INFOTEP, se debe realizar en las instalaciones. No se debe realizar ninguna actividad de tipo remoto sin la debida autorización el área de Tecnologías de la Información y las Comunicaciones.

La conexión remota a la red de área local del INFOTEP debe ser establecida a través de una conexión VPN segura aprovisionada por la entidad, la cual debe ser autorizada por el área de Tecnologías de la Información y las Comunicaciones.

La creación y retiro de usuarios en los sistemas de información debe seguir un procedimiento de Creación, Edición y Eliminación de Usuarios.

Gestión de Acceso a Usuarios

Se establece el uso de contraseñas individuales para determinar las responsabilidades de su administración.

Los usuarios pueden elegir y cambiar sus claves de acceso periódicamente, inclusive antes de que la cuenta expire.

Las contraseñas deben contener Mayúsculas, Minúsculas, números y por lo menos un carácter especial y de una longitud mayor a 8 caracteres.

El sistema debe obligar al usuario a cambiar la contraseña por lo mínimo 1 vez cada 45 días.

Todos los usuarios en su primer inicio de sesión deben cambiar las contraseñas suministrada por la mesa de soporte.

Todos los usuarios deben dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.

Cambiar todas las claves de acceso que vienen predeterminadas por el fabricante, una vez instalado y configurado el software y el hardware (por ejemplo appliance, impresoras, routers, switch, herramientas de seguridad, etc.).

No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, Jefes u otras personas que lo soliciten.

Todos los usuarios deben dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados.

Las contraseñas no deben ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.

Reportar al área de Tecnologías de la Información y las Comunicaciones sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado.

Reportar al área de Tecnologías de la Información y las Comunicaciones sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.

Las contraseñas de acceso a los servidores y administración de los Sistemas de Información deben ser cambiadas mínimo cada cuatro (4) meses.

El acceso a Bases de Datos, Servidores y demás componentes tecnológicos de administración de la Plataforma y Sistemas de Información, debe estar autorizado por el área de Tecnologías de la Información y las Comunicaciones.

Retiro de los derechos de acceso

Cada uno de los procesos de la Entidad es responsable de comunicar al área de Talento Humano y Contratación, el cambio de cargo, funciones o actividades o la terminación

contractual de los Colaboradores pertenecientes al proceso. El área de Talento Humano y Contratación son las encargadas de comunicar al área de Tecnologías de la Información y las Comunicaciones sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información.

1.1.12. *POLÍTICA SEGURIDAD FÍSICA Y DEL ENTORNO*

Objetivo: Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información del INFOTEP

Perímetro de Seguridad Física

Todas las entradas a los lugares de almacenamiento y procesamiento de información deben permanecer cerradas y es responsabilidad de todos los funcionarios, colaboradores y terceros autorizados evitar que las puertas se dejen abiertas.

Todos los funcionarios, colaboradores y terceros cuando sea el caso, sin excepción deben portar su carnet en un lugar visible mientras permanezcan dentro de las instalaciones del INFOTEP.

Es responsabilidad de todos los funcionarios, colaboradores, docentes y terceros del INFOTEP borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo y Catedra. Igualmente, no se debe dejar documentos o notas escritas sobre las mesas al finalizar las reuniones.

Los visitantes que requieran permanecer en las oficinas del INFOTEP SAI por periodos superiores a dos (2) días deben ser presentados al personal de oficina donde permanecerán.

Los dispositivos removibles, así como toda información CONFIDENCIAL del INFOTEP SAI, independientemente del medio en que se encuentre, deben permanecer guardados bajo seguridad durante horario no hábil o en horarios en los cuales los funcionarios, colaboradores o terceros responsable no se encuentren en su sitio de trabajo.

Las instalaciones del INFOTEP deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de funcionarios, colaboradores, terceros y visitantes.

Controles de Acceso Físico

Las áreas seguras, dentro de las cuales se encuentran el Centro de Datos, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información.

En las áreas seguras, bajo ninguna circunstancia se puede fumar, comer o beber.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por un funcionario o colaborador del proceso. El personal de limpieza se debe capacitar acerca de las precauciones mínimas a seguir durante el proceso de limpieza.

Ubicación y Protección de los equipos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Se debe instalar sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia. Así

mismo, se debe proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.

Seguridad de los equipos fuera de las instalaciones

Los equipos portátiles no deben estar a la vista en el interior de los vehículos. En casos de viaje siempre se debe llevar como equipaje de mano.

En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente al área de Tecnologías de la Información y las Comunicaciones y debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de la misma.

Cuando los equipos portátiles se encuentren desatendidos deben estar asegurados con una guaya, dentro o fuera de las instalaciones del INFOTEP.

Seguridad en la reutilización o eliminación de los equipos

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información que se encuentre almacenada. Posteriormente debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.

Retiro de Activos

Ningún equipo de cómputo, información o software debe ser retirado del INFOTEP sin una autorización formal.

1.1.13. *POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA*

Objetivo: Definir los lineamientos generales para mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información del INFOTEP.

Todo el personal debe conservar su escritorio libre de información propia de la entidad, que pueda ser copiada, utilizada o estar al alcance de terceros o por personal que no tenga autorización para su uso o conocimiento.

Todo el personal debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de ellos o que por cualquier motivo deban dejar su puesto de trabajo.

Todos los usuarios al finalizar sus actividades diarias, deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

En horario no hábil o cuando los lugares de trabajo se encuentren desatendidos, los usuarios deben dejar la información CONFIDENCIAL protegida bajo llave.

1.1.14. *POLÍTICA DE GESTIÓN DE CAMBIOS*

Objetivo: Asegurar que los cambios a nivel de infraestructura, aplicaciones y sistemas de información realizados en el INFOTEP se realicen de forma controlada.

Se deben establecer procedimientos para el control de cambios ejecutados en la entidad.

Toda solicitud de cambio en los servicios de procesamiento de información del INFOTEP, se debe realizar siguiendo el Procedimiento de gestión de cambios, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.

Se debe llevar una trazabilidad del control de cambios solicitados.

Se debe establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.

Los cambios sobre sistemas de información deben ser planeados para asegurar que se cuentan con todas las condiciones requeridas para llevarlo a cabo de una forma exitosa y se debe involucrar e informar a los funcionarios, colaboradores o terceros que por sus funciones tienen relación con el sistema de información.

Previo a la aplicación de un cambio se deben evaluar los impactos potenciales que podría generar su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.

Los cambios realizados sobre sistemas de información deben ser probados para garantizar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.

Se debe disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.

1.1.15. *POLÍTICA DE PROTECCIÓN CONTRA CÓDIGO MALICIOSO*

Objetivo: Definir las medidas de prevención, detección y corrección frente a las amenazas causadas por códigos maliciosos en El INFOTEP.

Toda la infraestructura de procesamiento de información del INFOTEP, debe contar con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.

Se debe restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores del INFOTEP.

Todos los funcionarios, colaboradores y terceros que hacen uso de los servicios de tecnología de la información y comunicaciones del INFOTEP son responsables del manejo del antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.

El INFOTEP debe contar con el software necesario como antivirus para protección a nivel de red y de estaciones de trabajo, contra virus y código malicioso, el servicio es administrado por el área de Tecnologías de la Información y las Comunicaciones.

El antivirus adquirido por el INFOTEP, sólo debe ser instalado por los responsables del área de Tecnologías de la Información y las Comunicaciones.

Los equipos de terceros que son autorizados para conectarse a la red de datos del INFOEP deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados la red del INFOTEP pueden ser monitoreados y supervisados por la Oficina de Tecnologías de la Información y las Comunicaciones.

Se debe mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.

Se debe hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma automática con una periodicidad mensual y su correcta ejecución y revisión estará a cargo del área de Tecnologías de la Información y las Comunicaciones.

La Entidad debe contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, contenido de correo electrónico, etc.

Se deben hacer campañas de sensibilización a todos los funcionarios, colaboradores y terceros del INFOTEP, con el fin de generar una cultura de seguridad de la información.

Los funcionarios, colaboradores y terceros del INFOTEP pueden iniciar en cualquier momento un análisis bajo demanda de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los funcionarios, colaboradores y terceros cuando sea necesario siempre podrán consultar al área de Tecnologías de la Información y las Comunicaciones sobre el tratamiento que debe darse en caso de sospecha de malware.

Los usuarios no podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.

Todo usuario es responsable por la destrucción de archivos o mensajes, que le haya sido enviado por cualquier medio provisto por el INFOTEP, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe COPIAR y enviar el correo a la cuenta sgsi@infotepsai.edu.co, sistemas@infotepsai.edu.co

El único servicio de antivirus autorizado en la entidad es el asignado directamente por el área de Tecnologías de la Información y las Comunicaciones, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura.

El área de Tecnologías de la Información y las Comunicaciones es el responsable de administrar la plataforma tecnológica que soporta el servicio de Antivirus para los equipos de cómputo conectados a la red del INFOTEP.

El área de Tecnologías de la Información y las Comunicaciones se reserva el derecho de monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso.

El área de Tecnologías de la Información y las Comunicaciones se reserva el derecho de filtrar los contenidos que se trasmitan en la red del INFOTEP SAI, con el fin de evitar amenazas de virus.

Todos los correos electrónicos serán revisados para evitar que tengan virus. Si el virus no puede ser eliminado, la información será borrada.

1.1.16. *POLÍTICA DE BACKUP*

INFOTEP debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el área de Tecnología y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Institución, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El área de Tecnología establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Registro de Respaldo de Información

Debe existir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldada.
La información respaldada debe ser probada como mínimo dos veces al año, asegurando que es confiable, integra y que se estará disponible en el evento que se requiera para su utilización en casos de emergencia.

Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

Se debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.

El área de Tecnologías de la Información y las Comunicaciones, a través del Ingeniero, debe aplicar los siguientes lineamientos:

Restaurar por lo menos cada seis meses, el escenario adecuado para probar las copias de respaldo de los Servidores.

Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.

1.1.17. *POLÍTICA DE EVENTOS DE AUDITORIA*

Objetivo: Asegurar que los registros de los eventos y las operaciones realizadas sobre los sistemas de información y plataforma tecnología del INFOTEP que permitan contar con evidencia necesaria para la gestión de incidentes de seguridad de la información.

Registro de eventos

Todos los accesos de usuarios a los sistemas, redes de datos y aplicaciones del INFOTEP, deben ser registrados.

Se deben habilitar los log de eventos requeridos y deben ser revisados con regularidad.

Se debe hacer copia de respaldo de información de los eventos de auditoria, ya que en caso de un incidente de seguridad de la información deben estar disponibles.

Registro del administrador y del Operador

Todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información del INFOTEP SAI deben estar debidamente registradas.

Los administradores de la infraestructura tecnología y de procesamiento de información deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración.

1.1.18. *POLÍTICA DE GESTIÓN DE SEGURIDAD DE LAS REDES*

Objetivo: Establecer los controles necesarios para proteger la información del INFOTEP transportada desde la red interna.

El área de Tecnologías de la Información y las Comunicaciones es la responsable de administrar y gestionar la red del INFOTEP.

El área de Tecnologías de la Información y las Comunicaciones es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

El INFOTEP proporcionara a los funcionarios, colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales, por lo cual no es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red institucional, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el área de Tecnologías de la Información y las Comunicaciones.

Separación de las Redes

El INFOTEP debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

1.1.19. *POLÍTICA DE SEGURIDAD DE INTERCAMBIO DE INFORMACIÓN Y RELACIÓN CON LOS PROVEEDORES*

Objetivos: Establecer los criterios de seguridad la información para la información accedida por los proveedores.

INFOTEP firmará acuerdos de confidencialidad con los funcionarios, comunidad académica y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Institución. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo funcionario de INFOTEP es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad.

1.1.20. *POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN*

Objetivo: Gestionar todos los incidentes de seguridad de la información reportados en el INFOTEP, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Reporte sobre los eventos y las debilidades de la seguridad de la información

Todos los funcionarios, colaboradores y terceros de la entidad y terceras partes tienen la responsabilidad de reportar de forma inmediata los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Se debe dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados.

Se deben establecer las responsabilidades en la Gestión de Incidentes de Seguridad de la Información.

Se debe definir el procedimiento de atención de incidentes de seguridad de la información del INFOTEP.

Se debe llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos.

Se debe recolectar las evidencias (Fiscalía, colcert, mintic) necesarias lo más pronto posible después del reporte del incidente.

Escalar los incidentes a niveles superiores en caso de que sea requerido.

Se debe hacer evaluaciones de los incidentes presentados ya que se puede necesitar de controles adicionales.

Se deben documentar todos los incidentes de seguridad reportados.

Se debe realizar sensibilización a todos los usuarios sobre incidentes de seguridad de la información.

2. Control de Cambios

FECHA	ACTUALIZACIÓN	CAMBIOS
Julio de 2018	01	Se crea política, fin y usos, derechos y compromiso institucional.

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Jhonathan Fernando Marín Medicis	Juan Camilo Cárdenas	Comité institucional