1. **OBJETIVO**

Difundir las políticas y estándares de seguridad informática a todo el personal de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas para que sea de su conocimiento y cumplimiento de los recursos informáticos utilizados o asignados.

1. **ALCANCE**

Usuarios responsables de equipos de cómputo, aplicaciones y servicios informáticos de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Franca.

1. **RESPONSABLE**

Proceso Gestión Tecnología e Informática.

1. **DESCRIPCIÓN DEL PROCESO**

El presente documento tiene como finalidad dar a conocer las políticas y estándares de tecnología e informática que deberán cumplir los usuarios de bienes y servicios, para proteger adecuadamente el hardware y software de la compañía.

**4.1 Socialización del manual de tecnología e informática.**

4.1.1 Los empleados que ingresen como personal nuevo a la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas deberán recibir la inducción del presente manual, a través del proceso de G-T.I, en la cual indique cuales son las políticas, procedimientos y obligaciones, medidas de seguridad y el uso adecuado de los medios informáticos.

4.1.2 El proceso de tecnología e Informática implementara diferentes estrategias para capacitar al personal con el fin de socializar las políticas y estándares del presente manual, que deberán cumplir todos los usuarios de T.I.

**4.2 Medidas disciplinarias.**

4.2.1 Cuando el proceso de Tecnología e Informática identifique incumplimiento al presente manual, emitirá el reporte correspondiente a Gestión Administrativa para los efectos de su competencia y atribuciones establecidas en el reglamento de trabajo.

4.2.2 Se consideran faltas en el presente manual, la pérdida de recursos tecnológicos como: Memorias USB, discos duros, periféricos, o modificaciones en su hardware y software, instalar o desinstalar programas de manera no autorizada y sin contar con su respectivo licenciamiento, aprovechar los recursos tecnológicos de la empresa para realizar prácticas que atenten contra la seguridad informática de la compañía, adelantar pruebas de software o dispositivos tecnológicos sin contar con la aprobación del proceso de Gestión Tecnología e Informática.

* 1. **Uso de recursos tecnológicos.**

4.3.1 Consultar la política de uso de los recursos informáticos.

**4.4 Adquisición de nuevos equipos de cómputo y sistemas de información.**

4.4.1 Toda compra de nuevos equipos, sistemas de hardware, software o nuevos componentes para los sistemas existentes, debe realizarse de acuerdo a las políticas de seguridad, e indicaciones técnicas del proceso Gestión tecnología e informática y siguiendo los protocolos establecidos por el Procedimiento de compras correspondiente para su compra.

4.4.2 Dando cumplimiento a la Ley 603 del 2000, está prohibido uso de aplicaciones clonadas dentro de la compañía con el fin de preservar los derechos de autor y garantizar un mayor rendimiento en los equipos tecnológicos.

**4.5 Protección y ubicación de los equipos.**

* + 1. Consultar la política de uso de los recursos informáticos.

**4.6 Mantenimiento Preventivo de HW y SW.**

4.6.1 El formato FO-TI-07 cronograma de mantenimiento preventivo se programara por parte del proceso de G.T.I en las primeras dos semanas del año dejando así establecido el cronograma que se implementará para los mantenimientos y será notificado a los usuarios con el fin de agendarse un tiempo de 30 minutos para su ejecución, la limpieza se realizará dos veces al año por equipo, si algún proceso requiere con antelación dicho mantenimiento, deberá solicitarlo a través del formulario de solicitudes de soporte técnico.

4.6.2 Sólo el personal del proceso de Gestión Tecnología e Informática podrá realizar el mantenimiento de hardware, software y reparación de equipos de cómputo, y dejaran registrado el procedimiento realizado en el formato FO-TI-02 mantenimiento preventivo.

**4.7 Daños en equipos de cómputo.**

Los equipos de cómputo o cualquier recurso tecnológico, que sufra algún daño deberán ser reportados a través del formulario de soporte técnico, el proceso de Gestión Tecnología e Informática será el encargado de realizar la revisión o solicitar la garantía correspondiente ante el proveedor.

* + 1. Toda solicitud deberá dejarse registrada en el formulario de solicitudes de soporte técnico, estas solicitudes se atenderán según su orden de llegada y urgencia, la escala de urgencia es del 1 al 3 siendo 1 muy urgente y 3 menos urgente, se consideran urgentes solicitudes que requieran ser atendidas lo más rápido posible ya que se está viendo afectada la productividad de su proceso, la escala se torna menos urgente cuando el error o problema puede dar tiempo para ser cerrada ya que no interfiere con un impacto fuerte en sus labores, para las solicitudes urgentes se tendrá máximo un día para ser atendidas, las solicitudes con urgencia media tendrán 2 días para ser cerradas y las solicitudes de prioridad baja tendrán 4 días para su cierre, solicitudes que requieran un desarrollo o participación de terceros se dejara seguimiento por correo electrónico pero estas no serán medidas en el indicador de solicitudes de soporte técnico, esta prioridad la determina el personal de G.T.I, las solicitudes que sean registradas durante los últimos 5 días del mes serán tenidas en cuenta como insumo para ese mes sin importar que su cierre sea realizado durante los primeros días del mes siguiente.
    2. Los equipos tecnológicos que sufra algún daño por uso, descuido o negligencia del usuario que resguarda el equipo, este asume la responsabilidad de cubrir el valor de la reparación o reposición del equipo o accesorio afectado.
    3. Los usuarios de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas que hagan uso de equipo de cómputo, y encuentren alertas sospechosas relacionadas con virus informáticos deberán reportar al proceso de G.T.I para aplicarse las medidas pertinentes que ayuden a neutralizar el virus informático aplicando protocolos de seguridad.
  1. **Uso de medios de almacenamiento.**

4.8.1 Consultar la política de uso y manejo de información confidencial.

**4.9** **Instalación de software.**

4.9.1 Los usuarios que requieran la instalación de software que no sea propiedad de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, deberán justificar su uso y solicitar autorización al proceso de Gestión tecnología e informática emitida por el director del proceso, indicando el equipo de cómputo, dónde se instalará el software y el período de tiempo que permanecerá dicha instalación.

4.9.2Se considera falta grave que los usuarios instalen cualquier tipo de programa (software) en suscomputadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, que no esté autorizado por el proceso de Gestión Tecnología e Informática, utilizando algún método informático para vulnerar los bloqueos que se tienen para la instalación de software.

4.9.3 El uso de software free (gratuito) se podrá instalar en los equipos de cómputo siempre y cuando cuenten con el visto bueno de Gestión Tecnología e Informática, para prevenir infecciones y daños por motivos de virus.

**4.10 Administración de redes.**

4.10.1 El personal del proceso de Gestión Tecnología e Informática son los únicos autorizados para crear y diseñar redes locales, conexiones remotas a redes internas y externas, intercambio de información con otros equipos de cómputo utilizando el (FTP), protocolo de transferencia de archivos.

4.10.2 Cualquier persona que tenga acceso a las instalaciones de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas., y necesite conexión del servicio de internet deberá solicitar la clave al proceso de Gestión Tecnología e Informática, se deberán conectar a la red ZFIP-VISITANTES.

**4.11 Uso del Correo electrónico.**

4.11.1 Los correos, conversaciones y demás archivos adjunto están considerados como información de uso y propiedad exclusiva de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas.

4.11.2 En caso de encontrar sospecha o vulnerabilidad de filtración de información de los correos corporativos, se aplicaran medidas pertinentes con el fin de entrar y revisar las cuentas de los usuarios implicados en compañía de la autoridad competente.

4.11.3 Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas. se reserva el derecho de acceder y revelar mensajes enviados por correos electrónicos para cualquier propósito y revisar las comunicaciones de personal que ha comprometido la seguridad o violado las políticas de seguridad informática de la compañía realizada acciones no autorizadas en caso de que estas se presenten y en compañía de la autoridades correspondiente.

4.11.4 Se considera falta grave falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico, revelar o ayudar a terceros a interceptar las comunicaciones electrónicas.

4.11.5 Está prohibido a cualquier usuario de la compañía facilitar a personas no autorizadas la cuenta de usuario y contraseñas.

4.11.6 Prohibido enviar mensajes con direcciones de otros funcionarios y/o desde otros equipos a nombre de terceros, en general es ilegal manipular las cabeceras de correo electrónico saliente.

4.11.7 Para la difusión de información a grupos de personas que existen en el grupo de trabajo Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, se deben conservar las siguientes directrices:

* En ningún caso se podrán utilizar las listas de distribución para la distribución de información ajena a las finalidades de la compañía. (Cadenas, presentaciones, invitaciones, etc.).
* En los mensajes a las listas se debe evitar incluir archivos binarios como por ejemplo documentos de tamaño elevado para evitar la degradación del servicio de correo y el llenado involuntario del espacio de los usuarios.
  + 1. Está prohibido realizar cualquiera de los tipos definidos de abuso de correo electrónico, además de las siguientes actividades:
* Utilizar el correo electrónico para cualquier propósito comercial o financiero ajeno a las funciones propias de la compañía.
* No se debe participar en la propagación de cartas encadenadas o participar en esquemas piramidales o temas similares de distribución masiva de información ajena a la compañía.
* Distribuir de forma masiva grandes cantidades de mensajes que sean o no de contenido laboral a direcciones externas a la compañía.
* Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona no se encuentre en la empresa) el usuario ausente debe solicitar al proceso de tecnología e informática re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, a menos que cuente con la autorización de la gerencia y el procedimiento solo lo puede hacer el proceso de G.T.I.

**4.12 Controles contra código malicioso.**

4.12.1 Para prevenir infecciones por virus informáticos, los usuarios de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas no deben hacer uso de cualquier clase de software que no haya sido proporcionado y validado por el proceso de Tecnología e Informática.

4.12.2 Los usuarios de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas deben verificar que la información y los medios de almacenamiento, como los discos flexibles, CD, DVD, memorias USB, estén libres de cualquier tipo de código malicioso, para lo cual deben realizar el software antivirus autorizado por el proceso de Gestión tecnología e informática antes de ejecutar cualquier proceso donde se involucre el medio de almacenamiento externo (CD, DVD, USB).

4.12.3 Todos los archivos digitales que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que requieran ser descomprimidos, debe verificarse que estén libres de virus utilizando el software antivirus correspondiente.

4.12.4 Ningún usuario de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas debe escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñados para auto replicarse, dañar, en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema o software. Mucho menos probarlos en cualquiera de los ambientes ò plataformas de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas. El incumplimiento de este estándar será considerado una falta grave.

4.12.5 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo e informar al proceso de Gestión Tecnología e Informática para la detección y erradicación del virus.

4.12.6 Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar al proceso de tecnología e informática periódicamente las actualizaciones del software antivirus.

4.12.7 Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantados por Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas en: antivirus, Outlook, office, navegadores u otros programas.

4.12.8 Debido a que algunos virus son extremadamente complejos, ningún usuario de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas debe intentar eliminarlos de las computadoras, ya que puede causar perdida de la información. En caso de presentarse esta situación se debe reportar de inmediato al proceso de Gestión Tecnología e Informática.

**4.13 Internet.**

4.13.1 El acceso a Internet provisto a los usuarios de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

4.13.2 Este servicio está habilitado a todo el personal de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas que administre un equipo de cómputo.

4.13.3 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, en caso de necesitar una nueva conexión a Internet debe ser solicitada al proceso de Gestión Tecnología e Informática.

4.13.4 Los usuarios de Internet de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas deben reportar todos los incidentes de seguridad informática al proceso de Gestión tecnología e informática, inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

4.13.5 En caso de que se detecte un uso excesivo o inapropiado de sitios web como redes sociales o plataformas de video el proceso de G.T.I tiene la potestad de realizar los respectivos bloqueos en los equipos que se identifiquen.

4.13.6 Los usuarios del servicio de navegación en Internet:

* Se monitoreara el acceso a páginas no autorizadas reportadas por nuestro UTM.
* Deben acogerse a la prohibición de transmisión de archivos reservados ó confidenciales no autorizados.
* Está prohibido la descarga e instalación de software sin la autorización del proceso de tecnología e informática.

**4.14 Configuración del equipo.**

4.14.1 Los equipos de cómputo deberán mantener nombre de usuario y Password asignados por cada proceso, los protectores de pantalla (screensaver) deberán ser previamente instalados y autorizados por el proceso de Gestión tecnología e informática.

* 1. **Pérdida de Equipo.**
     1. El resguardo para las computadoras, tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.
     2. El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia, y deberá dar aviso inmediato a las proceso de Gestión Tecnología e Informática, y administrativo , si llega a ocurrir el robo o extravío del equipo de cómputo o accesorios.
  2. **Uso de dispositivos especiales.**
     1. El uso de quemadores de discos compactos es de uso exclusivo para las actividades necesarias propias de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, por ningún motivo se permitirá el uso de estos para una actividad diferente a la establecida.

**4.17 Administración y uso de Password.**

4.17.1Se delegará en cada empleado la responsabilidad de administrar el control de acceso (contraseña) de los sistemas y equipos de cómputo que le sea asignado, correo electrónico y/o contraseñas de aplicaciones que estén directamente ligadas a sus funciones laborales.

4.17.2 Todas las contraseñas serán registradas en el formato FO-TI-10 “Actualización de Contraseñas”, así mismo se debe dejar el registro del usuario correspondiente para el inicio de sesión, con el fin de deshabilitar las cuentas de manera oportuna, en caso de desvinculación por parte de un trabajador de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas.

4.17.3Cuando un funcionario de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas olvide o extravié las contraseñas y requiera copia del formato FO-TI-10 “Actualización de Contraseñas”, deberá realizarlo mediante una solicitud formal a la persona designada para tal fin, informando el motivo de la solicitud.

4.17.4A cada empleado se le delega la responsabilidad de administrar el control de acceso a su equipo de cómputo, así mismo será responsable de cambiar la contraseña cumpliendo con los lineamientos establecidos en el numeral 4.17 y su anexo, posteriormente deberá allegar la contraseña en el formato FO-TI-10 “Actualización de Contraseñas” a la persona responsable de administrarla.

4.17.5El uso de contraseñas compartidas está permitido siempre y cuando los sean dentro del mismo proceso con los funcionario que desempeñen funciones compartidas de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas.

4.17.6Todo usuario que tenga la sospecha de que su password es conocido por otra persona ajena a la compañía, deberá realizar el cambio inmediatamente, de acuerdo al numeral 4.17 y entregarlo a la persona encargada.

4.17.7 Las solicitudes de reasignación de contraseñas de email corporativo deberán notificarse al proceso de Tecnología e Informática por medio del Director de cada proceso a través de un correo electrónico.

4.17.8Todos los usuarios deberán conservar los siguientes lineamientos para la construcción de sus contraseñas:

Anexo tabla:

LISTADO

FRECUENCIA CAMBIO

MES PROPUESTO

NÚMERO DE CARACTERES

COMPUESTA POR:

APORTES EN LINEA

ANUAL

JUNIO

8

MAYUSCULAS, MINUSCULAS, NUMEROS

APPOLO

SEMESTRAL

MAYO - NOVIEMBRE

8

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

ARL

ANUAL

JUNIO

6

MAYUSCULAS, MINUSCULAS, NUMEROS

CAMARAS

ANUAL

JUNIO

10

ALFA NÚMERICA

CAPRENDIZAJE

ANUAL

JUNIO

8

ASIGNADA POR EL PORTAL

COMFAMILIAR

ANUAL

JUNIO

7

ASIGNADA POR EL PORTAL

COOMEVA

ANUAL

JUNIO

8

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

CORREO ELECTRONICO

SEMESTRAL

JUNIO - DICIEMBRE

12

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

CUENTA DE COMPUTADOR

SEMESTRAL

JUNIO - DICIEMBRE

12

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

MESA DE AYUDA JIRA

ANUAL

JULIO

8

ALFA NÚMERICA

INTEGRA 32

ANUAL

JULIO

12

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

LEGISCOMEX

ANUAL

JULIO

8

ALFA NÚMERICA

SADOC

ANUAL

JULIO

4

NÚMERICA

NUEVA EPS

ANUAL

JULIO

6

ALFA NÚMERICA

PORVENIR

ANUAL

JULIO

6

ALFA NÚMERICA

RED WIFI

SEMESTRAL

MAYO - NOVIEMBRE

6

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

INGRESOS ZFIP

ANUAL

DICIEMBRE

4

NÚMERICA

ANTIVIRUS

ANUAL

DICIEMBRE

8

ALFA NÚMERICA

SIGLO XXI

SEMESTRAL

MAYO - NOVIEMBRE

8

ALFA NÚMERICA

PRUEBA VERITAS

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

CELULAR CORPORATIVO

SEMESTRAL

MAYO - NOVIEMBRE

4

ALFA NÚMERICA

REDES SOCIALES

ANUAL

DICIEMBRE

8

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

UTP

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

TIGO UNE

ANUAL

DICIEMBRE

8

MAYUSCULAS, MINUSCULAS, NUMEROS,CATACTERES

ACTUALICESE

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

MEDIACOMERCE

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

SUPER NOTARIADO Y REGISTRO

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

ADM/ SURA ARL

ANUAL

DICIEMBRE

8

ASIGNADA POR EL PORTAL

ZEUS

SEMESTRAL

MAYO - NOVIEMBRE

12

MAYUSCULAS, MINUSCULAS, NUMEROS,CARTACTERES

* Deben ser difíciles de adivinar, esto implica que los password no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y de control.
* No deben ser idénticos o similares a password que hayan usado previamente.
* No utilizar las funciones de recordar las contraseñas que poseen algunas aplicaciones (por ejemplo, Eudoro, Outlook, Netscape, Messenger, internet Explorer, etc.)

4.17.9 Todos los empleados de la Zona Franca Internacional de Pereira S.A.S. Usuario Operador y de la Agrupación Zona Franca Internacional de Pereira que administren contraseñas de aplicaciones están obligados a cambiar las contraseñas de las aplicaciones el último día hábil del mes relacionado en la tabla anexa del numeral 4.17.8

4.17.10 Después de finalizado el tiempo estipulado para realizar el cambio de contraseñas, la persona designada verificará cuáles funcionarios no lo realizaron y procederá a enviar un correo informativo con copia al director de proceso del cual hace parte y a Gestión Administrativa, en donde se le notifica al funcionario del incumplimiento de la solicitud. Adicionalmente se realizara bloqueo del correo corporativo, todos los incumplimientos a los requerimientos establecidos en el presente manual serán sancionados de acuerdo al grado de faltas establecidas en el Reglamento del Trabajo.

4.17.11 Los empleados que se encuentren en licencia, vacaciones, incapacidad y en caso de que en su tiempo de ausencia hubo cambio de contraseñas deberán realizarlo e informarlo inmediatamente se reintegren a sus labores, esto no indica que el tiempo de realizar el cambio empiece a contar desde la fecha de modificación, debe acogerse a las fechas estipuladas por la empresa para tal fin.

4.17.12 En todos los casos donde se considere necesario el cambio de contraseñas, así no estén relacionados con retiro de personal, el proceso de G.T.I tendrá la potestad de solicitarlos o realizarlos de manera oportuna, esto para prevenir riesgos de vulneraciones y perdida de accesos a plataformas.

**4.18 Control de accesos remotos.**

4.18.1 Está prohibido el acceso a redes externas (WI-FI), cualquier situación que lo requiera deberá ser documentada y contar con el visto bueno del proceso de Tecnología e Informática.

4.18.2 La administración remota de equipos conectados a internet solo se permite si se cuenta con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del proceso de Gestión Tecnología e Informática.

**4.19 Derechos de propiedad intelectual.**

4.19.1 El proceso de Gestión Tecnología e informática tiene la responsabilidad de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

4.19.2 Está prohibido por las leyes de derechos de autor y por Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas, realizar copias no autorizadas de software, ya sea adquirido o desarrollado dentro de la empresa.

4.19.3 Los sistemas desarrollados por personal interno o externo que controle el proceso de sistemas son propiedad intelectual de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas.

**4.20 Revisiones del cumplimiento.**

4.20.1 El proceso de Gestión Tecnología e Informática realizará acciones de verificación al cumplimiento del procedimiento de políticas y estándares de seguridad informática, de acuerdo a lo establecido en el programa anual de trabajo del sistema de gestión.

4.20.2 El proceso de Tecnología e Informática podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado por la gerencia.

4.20.3 Los directores de los procesos de la Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas deben apoyar las revisiones del cumplimiento del manual de T.I y las políticas y estándares de seguridad informática verificando que sean apropiados y cualquier otro requerimiento de seguridad.

**4.21 Violaciones de seguridad Informática.**

4.21.1Solo el proceso de G.T.I tiene la competencia para autorizar en el uso de herramientas de hardware o software para violar los controles de seguridad informática.

4.21.2 Está prohibido realizar pruebas a los controles de los diferentes elementos de tecnología de información. Ninguna persona puede probar o intentar comprometer los controles internos. Con excepción de los órganos fiscalizadores que estarían acompañados por los responsables del proceso de T.I.

* + 1. Ningún usuario de Zona Franca Internacional de Pereira S.A.S Usuario Operador de Zonas Francas debe probar ó intentar probar fallas de la seguridad informática identificada ó conocida.
    2. Se considera falta gravísima el intentar escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos ó caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño ó acceso a las computadoras, redes ó información de Zona Franca Internacional de Pereira.

**5 Anexos:**

* FO-TI-02 Mantenimiento preventivo.
* FO-TI-03 Asignación de equipos tecnológicos.
* FO-TI-04 Préstamo.
* FO-TI-07 Cronograma de mantenimiento.
* FO-TI-10 Actualización de contraseñas

|  |  |  |
| --- | --- | --- |
| **6. Control de Cambios** | | |
| **Versión** | **Fecha** | **Cambios con respecto a la versión anterior** |
| 2 | 19/04/13 | * Se adicionó formato FO-TI-05 Lista de chequeo de los equipos de cómputo. |
| 3  3 | 05/04/14  05/04/14 | * Se realizó una modificación en la entrega del formato FO-TI-04 de solicitud de soporte técnico el cual lo propiciara el encargado de sistemas.   Se adicionaron los siguientes formatos correspondiente a:   * FO-TI-09 consecutivo de solicitud de soporte técnico, el cual nos permite mantener cifras estadísticas de los soportes relacionados en el mismo. * FO-TI-06 copia de seguridadk up, nos muestra los horarios de distribución y las fechas de realización de la copia de seguridad. * FO-TI-O5 lista de chequeo de equipos de cómputo, nos evidencia las configuraciones instaladas por el proceso de tecnología e informática en el momento de asignar un equipo tecnológico. * Se modificó los lineamientos para la creación de contraseñas seguras, la cual quedo por 12 caracteres 2 mayúsculas, 2 minúsculas, 4 números, 2 caracteres y 2 más libres a decisión del usuario tales como (¡”·$%&/\_-.\*/). * Se definió que las solicitudes de reasignación de contraseñas deberán ser notificadas a través de correo electrónico. |
| 4  5 | 15/04/16  6/06/2017 | * Se incluye nuevas políticas, normas y actualizaciones referentes al manejo de las contraseñas, uso de internet, manejo de recursos tecnológicos y de seguridad informática. * Se incluye nuevas políticas, normas y actualizaciones referentes a la realización del Back-up, uso de internet, manejo de recursos tecnológicos y de seguridad informática. |
| 6 | 7/06/2018 | * Se Modifican los nombres de los procesos que aparecen el manual de T.I y se actualiza el numeral 4.10.6 en referencia al periodo de entrega del informe sobre la realización del Back-Up (Mensualmente). |
| 7 | 23/04/2019 | * Se modifica la razón social de la empresa. * Se modificaron los numerales- El numeral 4.3 Uso de los recursos tecnológicos y los numerales 4.3.1 4.3.2 4.3.3 4.4 Resguardo y protección física de la información y dispositivos 4.4.1 4.4.2 4.4.3 4.4.4 4.4.5 se eliminaron de este manual y pasaron a ser parte de la política uso de recursos informáticos, en el numeral 4.3 se hace referencia a dicha política. * El numeral 4.5 Protección y ubicación de los equipos, anteriormente 4.7 desde 4.7.1 hasta 4.7.11 se eliminan y se relaciona la política uso de recursos informáticos.   El numeral 4.6 Mantenimiento preventivo de HW y SW antes numeral 4.8; en el numeral 4.6.1 se hace referencia a la solicitud de mantenimientos preventivos que deberán realizarse por medio del formulario de solicitudes de soporte técnico y no por GLPI mesa de ayuda, se elimina del numeral 4.6 anteriormente 4.8 el subnumeral 4.8.5 correspondiente a Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación, borrar ó hacer back up de la información sensible que se encuentre en el equipo, previendo la pérdida involuntaria de información, que pueda llegar a ocasionar durante el mantenimiento.   * El numeral 4.7 anteriormente 4.9 Daños en los equipos de cómputo se hace referencia al formulario de soporte técnico y en el numeral 4.7.1 indica el nuevo método para realizar las solicitudes de soporte técnico. * El numeral 4.8 antes 4.10 Uso de los medios de almacenamiento se eliminan todos los numerales y se hace referencia a la política de Uso y manejo de información confidencial. * En el numeral 4.9.2 antes 4.11.2 se agrega el enunciado “utilizando algún método informático para vulnerar los bloqueos que se tienen para la instalación de software”. * En el numeral 4.10.2 antes 4.12.2 se anexa el enunciado “se deberán conectar a la red ZFIP-VISITANTES”. * En el numeral 4.11.2 antes 4.13.2 se anexa el enunciado “en compañía de la autoridad competente” y en el numeral 4.11.3 antes 4.13.3 se anexa enunciado “en caso de que estas se presenten y en compañía de la autoridades correspondiente”. * En el numeral 4.13.5 antes 4.15.6 se agregan restricciones a la navegación web. * En el numeral 4.13.6 antes 4.15.7 se cambia el texto “Serán sujetos de monitoreo de las actividades que realiza en internet, de la prohibición al acceso de páginas no autorizadas y otros” por “ Se monitoreara el acceso a páginas no autorizadas reportadas por nuestro UTM” * En el numeral 4.17.2 antes 4.19.2 se anexa enunciado “así mismo se debe dejar el registro del usuario correspondiente para el inicio de sesión” * Se cambia el anexo tabla 4.17.8 periodo de cambio de contraseñas. * En el numeral 5 anexos se relaciona el formato FO-TI-4 Préstamo. |
| 8 | 06/11/2019 | * En el numeral 4.17.8 se actualiza la tabla del periodo de cambio de contraseñas, se añaden nuevas aplicaciones. * Se agrega nueva cláusula para el cambio de contraseñas 4.17.12 |
| 9 | 20/12/2021 | * En el numeral 4.7.1, se anexa enunciado: “las solicitudes que sean registradas durante los últimos 5 días del mes serán tenidas en cuenta como insumo para ese mes sin importar que su cierre sea realizado durante los primeros días del mes siguiente”. |
| 10 | 07/06/2022 | * En el numeral 4.13.5 se suprime Está prohibido el uso de páginas que tengan un contenido no apropiado para la seguridad de la empresa tales como; Roja directa, Facebook, etc. Los cuales disminuyen el ancho de banda de internet y atentan contra la seguridad de la empresa, de estas restricciones están exentos los procesos Gestión Tecnología e Informática, Gestión Comercial, Gestión técnica, Gerencia y G. P.H por las funciones que desarrollan. Y se agrega En caso de que se detecte un uso excesivo o inapropiado de sitios web como redes sociales o plataformas de video el proceso de G.T.I tiene la potestad de realizar los respectivos bloqueos en los equipos que se identifiquen. * En el numeral 4.17.2 se suprime , y posteriormente serán consolidadas en el formato FO-TI-01 “Contraseñas Seguras” y Este archivo deberá estar protegido de manera segura administrado por el funcionario que designe la Gerencia. |

|  |  |  |
| --- | --- | --- |
| ELABORADO POR: | REVISADO POR: | APROBADO POR: |
| Nombre: Dubian Sánchez | Nombre: Yuly Viviana Ríos | Nombre: Dubian Sánchez |
| Fecha: 16/05/2022 | Fecha: 07/06/2022 | Fecha: 07/06/2022 |