OBJETIVO

Constituir la base del entorno de seguridad de una empresa y definir las responsabilidades, los requisitos de seguridad, las funciones y las normas a seguir por los funcionarios de la entidad.

Es responsabilidad de los usuarios el aprovechamiento de los recursos informáticos ofrecidos para realizar las labores diarias dentro de la empresa.

El usuario es responsable de seguir las políticas de seguridad y procedimientos para el uso de los servicios, recursos informáticos, evitando cualquier práctica o uso inapropiado que pudiera poner en peligro la información de la empresa.

ALCANCE

- Esta política está dirigida a los funcionarios, consultores y demás miembros de Infotic S.A., incluyendo el personal vinculado con firmas que prestan servicios a la entidad que utilicen tecnología de información.

- Estas políticas aplican a equipos de cómputo propios de Infotic S.A. y de propiedad de personas que sean conectadas a la red de la entidad.

- La garantía del cumplimiento de esta política será responsabilidad de cada miembro de Infotic S.A. pues su desacato afecta a toda la entidad.

- No se permite el uso de los **bienes y servicios informáticos** para:

    - Llevar a cabo actividades fuera de la ley
    - Exportar software, información técnica en contra de leyes de control regional o internacional.
    - Hacer copia no autorizada de material protegido por derechos de autor.
    - Fines particulares en ningún momento.
    - Violar esta u otras políticas o reglamentos internos de la empresa.
    - Utilizar los recursos sin tener autorización o autoridad para hacerlo.
    - Permitir o facilitar que usuarios no autorizados hagan uso de los recursos de la empresa.
    - Utilizar los discos duros para almacenar archivos de música, fotos, videos, juegos o similares.
    - Utilizar memorias USB, DVD, CD, cámaras, celulares o cualquier otro dispositivo cuyo contenido sea desconocido en el equipo, sólo

debe tener acceso a estas unidades externas el administrador del sistema, debido a que pueden contener virus, robar la base de datos, ingresar troyanos, realizar posibles fraudes, etc.

- Utilizar dispositivos USB, disquetes o CDs prestados por alguien para instalar programas o abrir archivos, ya que este proceso es inseguro e igualmente sólo lo debe hacer la persona encargada de sistemas.
- Entregar, distribuir o divulgar a terceros información confidencial reservada o estratégica de la entidad, salvo autorización previa y expresa y que tenga que ver con el cumplimiento de las funciones de cada empleado.
- Usar, alterar o acceder sin autorización a los datos de otros usuarios.
- Suplantar a otras personas, haciendo uso de las claves de acceso ajenas a los servicios.
- Interceptar o alterar la información que se transmite.
- Sacar o tomar prestados los recursos informáticos sin la debida autorización.
- Interferir deliberadamente el sistema o el trabajo de otros, por ejemplo ejecutando códigos dañinos tales como virus.
- Acceder remota o directamente a un equipo sin el debido permiso del usuario, cuando se requiera acceder remotamente a un equipo de la empresa, se deberá utilizar únicamente conexiones seguras creadas por el área de sistemas.
- Realizar tareas no relacionadas con actividades propias de la empresa.
- Utilizar la infraestructura de tecnología de información de Infotic S.A. para conseguir o transmitir material con ánimo de lucro.
- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de Infotic S.A.
- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran, acceder a datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado.
- Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad informática pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.
- Instalar software sin estar debidamente autorizado para ello, sea o no, propiedad de la empresa.
- Dejar equipos que contengan información de la empresa en sitios diferentes a ella.

- Se debe tener en cuenta el manejo de un **antivirus** de la siguiente manera:

    - Todos los equipos pertenecientes a la empresa deben tener un antivirus efectivo y actualizado.
    - Los equipos con acceso a Internet deberán actualizar y ejecutar el antivirus de manera constante.
    - Todos los equipos de la empresa, deberán ser examinados en su totalidad, una vez a la semana, por el antivirus.
    - Revisar todo elemento que ingrese a la entidad.
    - Cualquier archivo de origen ajeno al equipo, debe ser revisado por el antivirus, sin importar el medio de almacenamiento de éste (CD, USB o compartido en red).
    - Revisar el contenido de archivos comprimidos y correos electrónicos.
    - Si durante el proceso de revisión de algún medio de almacenamiento se detecta algún virus, el archivo debe ser inmediatamente eliminado.
    - Los equipos que no son de propiedad de Infotic S.A. pero que de igual manera se conecten a la red deben ejecutar un software de antivirus actualizado.

- No compartir carpetas, solo cuando sea absolutamente necesario y con las personas que lo necesiten, dándole seguridad a los datos. Tarea que deberá realizar el administrador de la red.

- Realizar **copias de seguridad**:

    - Se deben realizar copias de seguridad de los sistemas de información en forma periódica (diaria, semanal, quincenal o mensual) dependiendo de la importancia de la información, estas a su vez deben tener otra copia que será almacenada en un lugar externo a la sede.
    - Se deben realizar copias de seguridad de las bases de datos del sistema de información de **Cobro Coactivo** en forma mensual.
    - Se deben realizar copias de seguridad de las bases de datos del sistema de información de **Patios y Grúas** en forma mensual.
    - Se debe realizar copias de seguridad de los servidores locales y carpetas de cada usuario en forma quincenal o mensual dependiendo de la importancia de la información.

- Backup de la **Página Web:** Todo el directorio raíz que contiene la estructura, base de datos, contenido y multimedia. En forma mensual.

- Tener en cuenta el **uso de contraseñas** seguras:

  - Todas las contraseñas son de carácter confidencial, intransferibles y de uso individual.
  - No compartir las contraseñas de acceso con otros usuarios de los sistemas.
  - No revelar las contraseñas ó código de su cuenta por ningún medio de comunicación ó directamente a otros (por ejemplo, su cuenta de correo electrónico, su usuario de bases de datos o permitir su uso a terceros para actividades ajenas a la misión de Infotic S.A. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario cuando la actividad se realiza desde el hogar (por ejemplo, computadores portátiles, teléfonos celulares).
  - No utilizar las funciones “recordar contraseña” que poseen algunas aplicaciones.
  - No escribir las contraseñas en ningún documento que se encuentre en su lugar de trabajo.
  - Se debe evitar utilizar la misma contraseña siempre en todos los sistemas o servicios
  - Para la definición de contraseñas, tener en cuenta lo siguiente:

    - Usar caracteres en mayúsculas y minúsculas (por ejemplo: a-z, A-Z)
    - Contener caracteres especiales (por ejemplo: 0-9,^&*()_+|~=\`{}[]:";'<>?,./).
    - El establecimiento de una contraseña debe ser al menos de 8 caracteres.
    - Las claves de los usuarios con privilegios (administradores de servidores) deben cambiarse mínimo cada mes y las claves de los usuarios sin privilegios deben cambiarse mínimo cada dos meses.
    - No debe estar basada en información personal, nombres de familia, número de cédula, fecha de nacimiento etc.
    - Las contraseñas no deben ser nunca almacenadas en un equipo de cómputo.
    - Se debe tratar de crear contraseñas que puedan ser recordadas fácilmente y que pueda escribirse rápidamente, pero que la contraseña no sea una palabra que pueda ser encontrada en un diccionario.

- No se debe dejar ningún tipo de archivo ni de menú abierto mientras se abandona el puesto de trabajo.

- No ingresar información al sistema en horarios no autorizados.

- Esta información no puede ser conocida por terceros sin autorización del responsable de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas y/o los procesos.

- Respecto del **uso de Correo Electrónico** de la Entidad:

  - Está prohibido enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial desde el correo interno (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
  - Está prohibido generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
  - Está prohibido el envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.
  - No utilizar el Internet para descargas de programas o trabajos de dudosa procedencia.
  - No utilizar las cuentas de correo corporativas para recibir o enviar correo personal.
  - No se debe utilizar el correo personal para enviar ó recibir información de la entidad.

- El **uso de software** deberá regirse por los siguientes términos:

  - El software que se debe usar en los equipos de cómputo debe ser completamente legalizado (compra de licencia para el uso del software).
  - El uso de Software libre está permitido donde el funcionario deberá solicitarlo a su encargado explicando el uso y la descripción del software a instalar.
  - El área de sistemas debe mantener bajo su resguardo el software que se utiliza en Infotic S.A., los medios de instalación CDs originales, licencias, manuales y garantías de equipos.
  - Se deben establecer los controles necesarios para mantener la información protegida. (Firewall, antivirus, monitoreo de puertos, protocolos, copias de respaldo, mantenimiento de equipos, software,

red. Se recomienda el uso de criptografía para la información que los usuarios consideren sensitiva o vulnerable.

- Respecto de la **seguridad del software**:

  - Está prohibido el uso de software malicioso (virus, troyanos, keyloggers, exploits, shell inversa o puerta trasera, escáner de puertos, sniffers), sólo excluye pruebas de seguridad interna.
  - Se deberá pedir autorización para la instalación de herramientas de Pentesting, las cuales deben ir de acuerdo con el plan de auditoría establecido por Infotic S.A.
  - Para bajar páginas de internet, archivos ejecutables, etc., definir siempre en el equipo de cómputo una carpeta o directorio para recibir el material. De ese modo aseguramos que todo lo que bajemos de internet siempre estará en una sola carpeta. Nunca ejecutar o abrir antes del escaneo.
  - Nunca abrir un adjunto de un email sin antes chequearlo con el antivirus. Si el adjunto es de un desconocido que no da avisó previamente del envío del material, directamente borrarlo sin abrir.
  - Se deben tener copias de seguridad en dos sitios diferentes a la entidad.

- Para la **actualización de software**, tener en cuenta lo siguiente:

  - El software instalado debe ser actualizado cada vez que haya una actualización disponible si se considera necesario.
  - Las Actualizaciones Automáticas de los sistemas operativos deberán estar elegidas con la opción de notificación previa para descarga, a partir de esto seleccionar los paquetes de actualización relacionados con parches de seguridad y otras necesarias.

- **Protección** de la Información:

  - Para prevenir la pérdida de datos por corte abrupto de la energía eléctrica, los usuarios deben grabar periódicamente sus archivos de datos cuando se encuentre trabajando en cualquier herramienta o software de propósito específico.
  - No se debe compartir los tomas de su equipo con otros aparatos de diferente especificación como celulares, lámparas, secadores de cabello, brilladoras, taladros, impresoras, sumadoras. Estos pueden provocar cambios transitorios bruscos de voltaje, que pueden llegar a dañar el equipo o producir pérdida de información.

- El equipo se debe conectar únicamente a tomacorrientes que pertenezcan al circuito eléctrico exclusivo para ellos, con protección contra sobrevoltajes transitorios (cortapicos).
- Cuando se presenten tempestades, los equipos se deben desconectar, pues las descargas eléctricas pueden ocasionar daños, especialmente si están conectados a una línea telefónica a través de módem.
- En caso de tener que mover los equipos por cualquier razón verificar que estén apagados, evitar movimientos bruscos o traslados frecuentes que puedan ocasionar problemas; en consecuencia, para evitar que se dañen.
- Nunca conecten o desconecten periféricos o dispositivos como impresoras, monitores, teclados cuando el equipo está prendido, esto podría ocasionar que el puerto o tarjeta en donde se conectan dichos periféricos se dañen.
- Almacenar, solo los archivos de datos que sean estrictamente necesarios y borrar o descargar aquellos que no se requieran de acuerdo con la necesidad y la importancia de cada uno de ellos.

RECOMENDACIONES

- Para dar de baja a un elemento informático debe solicitarse el concepto técnico del área de sistemas.

- Todo elemento informático que ingrese a la entidad debe ser entregado al área de sistemas para su debido chequeo, registro, resguardo o asignación de usuario o uso respectivo.

- Toda adición tanto de software como de hadware a los equipos de cómputo debe solicitarse a la división de sistemas.

- El uso de recursos o servicios informáticos de Infotic S.A. está sujeto a monitoreo por parte del área de sistemas.

- La creación de usuarios, el acceso y privilegios deben ser autorizados por el administrador del sistema.

- Por seguridad, se deben dar los mínimos permisos sobre cada recurso informático a los usuarios que permitan su normal operación.

- Cada usuario del equipo informático en forma compartida o individual son responsables de éste, de velar por su integridad, del uso que se le da a la cuenta de red, correo y acceso a Internet. Al igual que los datos son de su exclusiva responsabilidad.

- Los usuarios deben asignar a los directorios, subdirectorios y archivos, nombres que tengan relación clara y directa con el contenido de los mismos.

- No utilizar las unidades de red para manejo de información personal, fotos, música, videos.

- No comer cerca de teclados, tomar bebidas, colocar vasos sobre o cerca de los equipos ni fumar cerca de éstos, ya que se pueden ocasionar daños en los integrados.

- Los dispositivos (token) utilizados para ingreso a páginas de bancos deben estar en sitios seguros.

- Las chequeras, CDTs y sellos deben estar en sitios seguros fuera del alcance de personas no autorizadas.

GLOSARIO

- **Criptografía:** La criptografía consiste en cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.

- **Keylogger:** Registro de teclas presionadas por un usuario.

- **Exploit:** Explotar o aprovechar, secuencia de comandos con el fin de causar un error o un fallo en una aplicación

- **Puerta Trasera:** Conexión de una máquina destino a una cliente sin que la víctima pueda detectarlo.

- **Pentesting:** Técnica utilizada para evaluar la seguridad en redes.

- **Antivirus**: Software que detecta, limpia y/o elimina los virus informáticos existentes en el computador.

- **Freeware**: Software de libre distribución, sin embargo, sus derechos de copia no pueden ser incorporados a ningún tipo de desarrollo de software.

- **Licencia de software**: Documento que comprueba el derecho de uso de software.

- **Shareware**: Software que se puede instalar sin licencia como versión inicial de prueba, pero es necesario adquirir la licencia para tener derecho de uso definitivo.

- **Software de dominio público**: Software sin derechos de autor; sus autores desean compartirlo con la comunidad mundial de desarrolladores. Es de libre uso y puede ser incorporado a cualquier tipo de desarrollo de software no comercial

- **Software de automatización de oficina**: Es aquel software requerido para desarrollar las actividades diarias, tales como elaboración de documentos, correo electrónico, diagramas de flujo, hojas de cálculo, etc.

- **Virus:** Es un programa o un segmento de código creado con el objetivo de causar daños en los computadores, el cual puede ocasionar graves consecuencias para el computador que lo almacena. Se puede dividir en las siguientes ramas:

    - Virus de Macros/Código Fuente: Se adjuntan a los programas fuente de los usuarios y, a las macros utilizadas por: Procesadores de Palabras (Word, Works, WordPerfect), Hoja de Cálculo (Excel, Quattro, Lotus).
    - Gusanos: Son programas que se reproducen a sí mismo y no requieren de un anfitrión, pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posesionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borradas los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdidas de datos.
    - Caballos de Troya: Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de algún tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones.
    - Autorreplicables: Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se autoreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programada o cada determinado tiempo, contado a partir de su última ejecución, o simplemente al "sentir" que

se les trata de detectar. Un ejemplo de estos es el virus del viernes 13, que se ejecuta en esa fecha o se borra (junto con los programas infectados), evitando así ser detectado.

- Infectores del área de carga inicial: Infectan los diskettes o el disco duro, alojándose inmediatamente en el área de carga. Toman el control cuando se enciende la computadora y lo conservan todo el tiempo.
- Infectores del sistema: Se introducen en los programas del sistema, por ejemplo COMMAND.COM y otros se alojan como residentes en memoria. Los comandos del Sistema Operativo, como COPY, DIR o DEL, son programas que se introducen en la memoria al cargar el Sistema Operativo y es así como el virus adquiere el control para infectar todo disco que sea introducido a la unidad con la finalidad de copiarlo o simplemente para ver sus carpetas (también llamadas: folders, subdirectorios, directorios).
- Infectores de programas ejecutables: Estos son los virus más peligrosos porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras). La infección se realiza al ejecutar el programa que contiene al virus, que en ese momento se posesiona en la memoria de la computadora y a partir de entonces infectará todos los programas cuyo tipo sea EXE o COM, en el instante de ejecutarlos, para invadirlos autocopiándose en ellos.