PROPÓSITO:

Conocer las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información, para proteger adecuadamente los activos tecnológicos y la información de FARMART LTDA IPS.

INTRODUCCIÓN

Este documento se encuentra estructurado en cinco políticas generales de seguridad para usuarios de informática, con sus respectivos estándares que consideran los siguientes puntos:

- Seguridad de Personal.
- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Cumplimiento.

OBJETIVO

Difundir las políticas y estándares de seguridad informática a todo el personal, para que sea de su conocimiento y cumplimiento en los recursos informáticos utilizados o asignados

BENEFICIOS

Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información de la Empresa.

1. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD DEL PERSONAL

POLITICA

Todo usuario de bienes y servicios informáticos al ingresar como personal de FARMART acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos, así como el estricto apego al Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

Los usuarios deberán cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

1.1 OBLIGACIONES DE LOS USUARIOS

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

1.2 ENTRENAMIENTO EN SEGURIDAD INFORMÁTICA

Todo empleado de nuevo ingreso deberá contar con la inducción sobre el "Manual de Políticas y Estándares de Seguridad Informática para Usuarios", donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

1.3 MEDIDAS DISCIPLINARIAS

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

2. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD FÍSICA Y AMBIENTAL

POLITICA

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de FARMART IPS sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones.

2.1 Resguardo y protección de la información

2.1.1 El usuario deberá reportar de forma inmediata al Área de Tecnologías de información cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio u otros.

2.1.2 El usuario tiene la obligación de proteger las unidades de almacenamiento que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.

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

2.2 CONTROLES DE ACCESO FÍSICO

2.2.1 Cualquier persona que tenga acceso a las instalaciones de la Empresa, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la FARMART IPS, en el área de recepción, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

2.2.2 Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá salir de las instalaciones de la Empresa únicamente con la autorización de salida del área de Sistemas anexando el acta de salida.

2.3 SEGURIDAD EN ÁREAS DE TRABAJO

2.3.1 Los centros de cómputo de la Empresa son áreas restringidas, por lo que sólo el

personal autorizado por el Área de Tecnologías de la Información puede acceder a él.

2.4 PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS

2.4.1 Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del Área de Tecnologías de la Información, en caso de requerir este servicio deberá solicitarlo.

2.4.2 El Área de Inventarios será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el Área de Tecnologías de la Información.

2.4.3 El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la Empresa.

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

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

2.4.6 El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reacomodo de cables con el personal de Tecnologías de la Información

2.4.7 Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de Tecnologías de la Información a través de un plan detallado.

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

2.5 MANTENIMIENTO DE EQUIPO

2.5.1 Únicamente el personal autorizado por el Área de Tecnologías de la Información podrá llevar a cabo los servicios y reparaciones al equipo informático.

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

2.6 PÉRDIDA DE EQUIPO

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

2.6.2 El préstamo de laptops tendrá que solicitarse en el Área de Tecnologías de la Información, con el visto bueno del Coordinador de Sistemas o su equivalente en las dependencias de la Coordinación.

2.6.3 El usuario deberá dar aviso inmediato al Área de Tecnologías de la Información, e Inventarios de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

2.7 USO DE DISPOSITIVOS ESPECIALES

2.7.1 El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

2.7.2 El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

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

2.8 DAÑO DEL EQUIPO

2.8.1 El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, se levantara un reporte de incumplimiento de políticas de seguridad.

3. POLÍTICAS Y ESTÁNDARES DE SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO

POLITICA

Los usuarios deberán proteger la información que reside y utiliza la infraestructura tecnológica de la Empresa. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Empresa o hacia redes externas como Internet.

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

red.

3.1 USO DE MEDIOS DE ALMACENAMIENTO

3.1.1 Los usuarios de informática de la Empresa deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

3.1.2 Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información de la Empresa son registradas y susceptibles de auditoría.

3.2 INSTALACIÓN DE SOFTWARE

3.2.1 Los usuarios que requieran la instalación de software que no sea propiedad de la Empresa,

deberán justificar su uso y solicitar su autorización por el Área de Tecnologías de la Información indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.

3.2.2 Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Empresa, que no esté autorizado por el Área de Tecnologías de la Información.

3.3 IDENTIFICACIÓN DEL INCIDENTE

3.3.1 El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de Tecnologías de la Información lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

3.3.2 Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar al Área de Tecnologías de la Información.

3.3.3 Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información de la FARMART debe ser reportado al Área de Tecnologías de la Información.

3.4 ADMINISTRACIÓN DE LA CONFIGURACIÓN

3.4.1 Los usuarios de las áreas de la Empresa no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Empresa, sin la autorización del Área de Tecnologías de la Información.

3.5 SEGURIDAD PARA LA RED

3.5.1 Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Área de Tecnologías de la Información, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la FARMART, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

3.6 USO DEL CORREO ELECTRÓNICO

3.6.1 Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la de FARMART, a menos que cuente con la autorización del Área de Tecnologías de la Información.

3.6.2 Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como

información de propiedad de FARMART. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

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

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

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

3.7 CONTROLES CONTRA CÓDIGO MALICIOSO

3.7.1 Para prevenir infecciones por virus informático, los usuarios de la FARMART no deben hacer uso de software que no haya sido proporcionado y validado por el Área de Tecnologías de la Información.

3.7.2 Los usuarios de la FARMART deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Área de Tecnologías de la Información.

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

3.7.4 Ningún usuario, empleado o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización del Área de Tecnologías de la Información.

3.7.5 Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al Área de Tecnologías de la Información para la detección y erradicación del virus.

3.7.6 Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la FARMART en: Antivirus, Outlook, office, Navegadores u otros programas.

3.7.7 Debido a que algunos virus son extremadamente complejos, ningún usuario de FARMART debe intentar erradicarlos de las computadoras.

3.8 INTERNET

3.8.1 El acceso a Internet provisto a los usuarios de la FARMART es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

3.8.2 Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por la FARMART, en caso de necesitar una conexión a Internet especial,

ésta tiene que ser notificada y aprobada por el Área de Tecnologías de la Información.

3.8.3 Los usuarios de Internet de FARMART tienen que reportar todos los incidentes de seguridad informática al Área de Tecnologías de la Información inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.

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

- Serán sujetos de monitoreo de las actividades que realiza en Internet.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
- Saben que existe la prohibición de descarga de software sin la autorización del Área de Tecnologías de la Información.
- La utilización de Internet es para el desempeño de su función y puesto en FARMART y no para propósitos personales

4. POLÍTICAS Y ESTÁNDARES DE CONTROLES DE ACCESO LÓGICO

POLITICA

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

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de FARMART, debe ser proporcionado por el dueño de la información, con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

4.1 CONTROLES DE ACCESO LÓGICO

4.1.1 Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

4.1.2 Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Área de Tecnologías de la Información antes de poder usar la infraestructura tecnológica de la FARMART.

4.1.3 Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la FARMART, a menos que se tenga el visto bueno del dueño de la información y del Área de Tecnologías de la Información y la autorización del secretario de la oficina de la FARMART o su equivalente en las dependencias de la Coordinación.

4.1.4 Cada usuario que acceda a la infraestructura tecnológica de la FARMART debe contar con un identificador de usuario (UserID) único y personalizado. Por lo cual no está permitido el uso de un mismo UserID por varios usuarios.

4.1.5 Los usuarios son responsables de todas las actividades realizadas con su identificador de usuario (UserID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el UserID de otros.

4.1.6 Está prohibido hacer cambios de contraseñas en los equipos de cómputo corporativos sin autorización previa de Tecnología informática, debe conservar la misma asignada en su entrega.

4.2 ADMINISTRACIÓN DE PRIVILEGIOS

4.2.1 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados a el Área de Tecnologías de la Información, para el cambio de privilegios.

4.3 EQUIPO DESATENDIDO

4.3.1 Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el Área de Tecnologías de la Información cuando no se encuentren en su lugar de trabajo.

4.4 ADMINISTRACIÓN Y USO DE CONTRASEÑA

4.4.1 La asignación de contraseñas debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.

4.4.2 Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al Área de Tecnologías de la Información para que se le proporcione una nueva contraseña.

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

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

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

4.4.6 Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

4.5 CONTROL DE ACCESOS REMOTOS

4.5.1 La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del Área de Tecnologías de la Información.

5. POLÍTICAS Y ESTÁNDARES DE CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

El área de Tecnologías de la Información tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información automatizada en general.

5.1 REVISIONES DEL CUMPLIMIENTO

5.1.1 El área de Tecnologías de la Información realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

5.1.2 El área de Tecnologías de la Información 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 en la política de Seguridad de Personal.

5.1.3 Los jefes y responsables de los procesos establecidos en FARMART deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

5.2 VIOLACIONES DE SEGURIDAD INFORMÁTICA

5.2.1 Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el Área de Tecnologías de la Información.

5.2.2 Ningún usuario de FARMART debe probar o intentar probar fallas de la Seguridad Informática o conocidas, a menos que estas pruebas sean controladas y aprobadas por el Área de Tecnologías de la Información.

5.2.3 No se debe intencionalmente 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 o acceso a las computadoras, redes o información de la FARMART.

6. HISTORIAL DE CAMBIOS

VERSION	DESCRIPCIÓN DEL CAMBIO	MOTIVO DEL CAMBIO	FECHA
01	Elaboración del documento	N/A	08-10-2020

ELABORÓ	REVISÓ	APROBÓ
Nombre: JOSE ANTONIO ROA Cargo: COORDINADOR DE SISTEMAS Firma	Nombre: LUCILA LOAIZA MILLAN Cargo COORDINADOR DE CALIDAD Firma	Nombre: MARTHA LUCIA OVALLE SUAZA Cargo GERENTE GENERAL Firma