OBJETIVO:

Describir procesos para el uso adecuado de los equipos de tecnología informática, servicios y aplicativos de la red de datos de la compañía que permitan una seguridad de la información contenida o manejada por ellos.

ALCANCE:

Estas políticas se aplicarán a todas las áreas de la empresa en donde exista al menos un equipo de tecnología informática y a los usuarios del sistema de Control de Inventarios. También regula el uso del Internet al interior de la compañía.

DEFINICIONES:

- Backup: Copia de respaldo
- Password: Palabra secreta o contraseña.
- Software: Programas, aplicativos.
- Firewall: Muro de Fuego, barrera de seguridad.
- Proxy: Software que permite el acceso a Internet a todos los usuarios de la red local a través de una sola conexión.
- Clave de acceso: Código o palabra que se utiliza para acceder a datos restringidos de un sistema software o hardware.
- Troyanos: Programas que prometen ser algo y realizan otra cosa muy diferente, comprometiendo la seguridad del usuario.
- Puerta trasera: Programa que permite a los vándalos informáticos acceder a la red y a los equipos de forma sencilla y reiterativa.
- Spam: Nombre que se le da al correo electrónico no solicitado, la mayoría de las veces de carácter meramente publicitario. También se conoce con ese término a las técnicas encauzadas al envío masivo e indiscriminado de mensajes electrónicos.
- VPN: Red Privada Virtual. Canal virtual que se establece a través de internet entre al menos dos equipos.

REGISTROS:

1. Revisión Software equipos de Tecn. Informática (Formato S-F24-N03)
2. Bitácora Mantenimiento por equipo electrónico (Formato S-F25-N02)
3. Bitácora de Backups 1 (Formato S-F22-PR08)
4. Bitácora de Backups 2 (Formato S-F23-PR08)
5. Registro de Help Desk (Formato S-F26-N02)
6. Acta de Entrega de Equipos de TI (Formato S-F92-N02)
7. Solicitudes o Requerimientos al Depto de Sistemas (Formato S-F104-N02)
8. Acuerdo de uso de licencia (Formato S-F119-N02)
9. Bitácora de control de backups pc's (Formato S-F31-PR08)

NORMAS:

I. Usuarios

Son todas aquellas personas pertenecientes a la compañía o a empresas calificadas como usuarios de la Zona Franca, las cuales hacen uso de los recursos informáticos de la misma, para cuyo efecto se diferenciarán como usuarios internos y externos correspondientemente.

*. Cada usuario interno tendrá asignado un nombre de usuario y una contraseña en el equipo bajo el cual estará autorizado a trabajar y el uso de la misma será responsabilidad de cada usuario. La solicitud de creación o retiro de las cuentas del usuario en los diferentes sistemas de información que posee la compañía, debe realizarla el área administrativa, al momento de la vinculación o retiro del empleado de la compañía.

*. Los usuarios calificados de la Zona Franca del Pacífico y/o los Usuarios de las Zonas Francas especiales, deberán solicitar la asignación, cambio o retiro de usuarios a través del área de Operaciones de ZONA FRANCA DEL PACIFICO S.A., quien los redireccionará al área de Tecnología, en donde se procederá a la asignación y comunicación de los logins solicitados y requeridos para el acceso al Sistema de Control de Inventarios.

*. Es requisito para usar el sistema de control de inventarios, que cada persona asignada por parte del Usuario calificado para operar el mismo, cuente con el certificado de capacitación que entrega la Zona Franca del Pacífico S.A. Usuario Operador de Zona Franca, de lo contrario no será viable la interacción entre estas y el usuario operador. Así mismo debe ser actualizado de acuerdo a la rotación del personal de cada compañía.

*. Todos los usuarios externos del Sistema de Control de Inventarios accederán inicialmente a la red de Zona Franca a través de una VPN con un Código de usuario y un password, una vez validado el acceso, ingresarán al aplicativo usando el login , password y base de datos asignado por el área de Sistemas de tecnología de Zona Franca. El password tiene una vigencia de 30 días, al cabo de los cuales, el sistema le solicitará sea reemplazado por otro.

*. Los usuarios externos del Sistema de Control de Inventarios, solo podrán tener una sesión activa.

*. Ningún usuario externo podrá hacer uso de los equipos de la compañía sin la previa autorización del Departamento de Sistemas o de la Coordinación de Operaciones.

II. Claves de acceso (contraseñas)

Las claves de acceso son la protección más común en contra de accesos no autorizados a cualquier sistema. Los usuarios pueden definir su propio sistema para elegir la clave, lo importante es que siga los siguientes parámetros:

*. No colocar como clave de acceso el nombre, apellido o cualquier otro dato personal o familiar.

*. No utilizar palabras simples que se puedan encontrar en un diccionario, ni palabras de otros idiomas.

*. Utilizar combinaciones de letras y números.

*. Es personal e intransferible, es decir, no comentar con nadie la clave de acceso al sistema, tampoco dejarla escrita en un lugar visible a cualquier persona.

*. La clave debe tener como mínimo 6 caracteres de longitud.

*. Debe cambiarse periódicamente, mínimo una vez al mes.

*. Evitar el uso de caracteres especiales tales como * % # ? ‘ “

*. En caso de detección de accesos no autorizados, el área de tecnología verificará su procedencia, si la misma es externa a la compañía y proveniente de uno de sus clientes, la Zona Franca podrá iniciar un proceso legal contra dicha compañía o individuo con la evidencia de la intrusión, si lo considera pertinente. Si por el contrario, la intrusión proviene del interior de la red de Zona Franca, el funcionario responsable de la misma, será sancionado por la Gerencia de acuerdo a la gravedad de las acciones realizadas en la intrusión y las consecuencias de la misma.

III. Software

*. Los empleados de la Zona Franca del Pacifico utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

*. Para la utilización de programas de licencias de uso libre tipo GNU GPL o similares se debe tener autorización explicita del Área encargada de Tecnología Informática.

*. Los empleados de la Zona Franca del Pacifico no descargarán ni ejecutarán programas informáticos no autorizados a través de Internet.

*. El área de Tecnología debe llevar inventario del software legal o en su defecto una carpeta con los números de las licencias actuales, identificando los equipos en el que se encuentren instalados.

*. El servidor central debe contar con las licencias necesarias de Sistema operativo y de base de datos, adecuados al número de usuarios que accedan al sistema.

*. El Departamento de Sistemas debe llevar registro de los cambios o actualizaciones que se han hecho al software de Control de Inventarios, los cuales, se deben llevar en una carpeta ya sea física o lógica según sea el caso.

*. El personal del área de tecnología es responsable por los medios (CD, DVD, cintas) originales del software de la compañía.

*. El área de Sistemas debe realizar dos veces al año, la verificación del software instalado en los diferentes equipos que posea la compañía, de forma electrónica a través de software especializado, dejando la evidencia del mismo en el formato Revisión Software equipos de Tecnología Informática (Formato S-F24-N03). De ser encontrado software no autorizado, este será removido del equipo del usuario sin previo consentimiento. Los resultados de dicha revisión serán informados a la gerencia de la compañía.

*. El área de Tecnología debe entregar el Formato de acuerdo de uso de Licencia (Formato S-F119-N02) a todos los usuarios del parque industrial a los cuales se les asigne un login de base de datos.

IV. Internet y correo electrónico

*. Las compañías Usuarias de Zona Franca, deben adquirir su internet a través de los diferentes proveedores que ofrecen sus servicios en el parque industrial y no es responsabilidad de ZONA FRANCA DEL PACIFICO S.A.

*. El servicio de Internet de ZONA FRANCA DEL PACIFICO S.A. es para uso exclusivo tanto del sistema Pacífico como de sus empleados, y como tal está condicionado a las normas de seguridad que rigen la red corporativa.

*. Para la red corporativa, se contará con un Proxy y un Firewall, administrados por el Departamento de Sistemas, con el fin de autorizar o restringir el acceso a los diferentes sitios de Internet, para los usuarios de la red local.

*. El Departamento de Sistemas otorga los derechos de acceso a Internet, para los usuarios que estén conectados a la red de área local.

*. Las descargas de archivos mayores a 1.5 MB deben realizarse en horas no laborales o comuníquese con el Área de Sistemas. El uso indiscriminado del Internet puede generar un retardo en el tráfico de la información y producir inconvenientes innecesarios en los procesos de la Zona Franca del Pacifico.

*. No instalar programas descargados de Internet no autorizados por el administrador de la red, ya que pueden generar caos en materia de seguridad para toda la red de la empresa. Estos programas pueden ser troyanos, virus o puertas traseras que le dan acceso a los vándalos informáticos para realizar alguna labor concreta.

*. Está prohibido el acceso a páginas con contenido pornográfico, violento o terrorista, al igual que el uso de programas de mensajería instantánea y el acceso a redes sociales (MSN, Yahoo, Google,Facebook,hi5,etc) debido a que son fuente de troyanos y virus.

*. Quien sea sorprendido haciendo mal uso del Internet, recibirá inicialmente un aviso de advertencia (tarjeta amarilla), si reincide, se dará a conocer su falta a todos los usuarios de la red. De repetirse la situación, se le suspenderá el servicio de Internet.

*. Cada cliente interno tendrá una dirección de correo electrónico, sin embargo, se tendrá una cuenta general para la compañía, la cual será responsabilidad de la Secretaria de Gerencia.

*. El Departamento de Sistemas de la Zona Franca del Pacifico se reserva el derecho de vigilar o monitorear el uso del sistema de correo electrónico con el fin de evitar el uso indebido del mismo, el cual incluye, pero no se limita a:

- Enviar o recibir deliberadamente material pornográfico, indecente u otro material sexual.
- Enviar información confidencial de la Zona Franca del Pacifico, o secretos comerciales sin la autorización pertinente.
- Utilizar el correo electrónico para acoso sexual.
- Enviar correo electrónico con insultos.
- Enviar cartas en cadena o correo electrónico “basura” (Spam).
- Enviar correo electrónico que incluya discriminación sexual o racial.
- Enviar correo electrónico religioso o político.
- Utilizar el correo electrónico de la Zona Franca del Pacifico para actividades comerciales privadas o publicidad no oficial.

*. No dirigir ni responder correo SPAM (Correo electrónico basura), acosador o cartas en cadena, si se recibe este tipo de correos, éstos deben borrarse sin siquiera abrirse.

*. La responsabilidad del uso del correo electrónico es de cada usuario y cualquier inconveniente que surja por el mal uso de este, deberá ser asumido por el usuario.

*. No adjuntar archivos muy grandes al correo electrónico. Los mensajes largos y voluminosos aumentan considerablemente el tráfico de la red, representan mas carga para los recursos tecnológicos y son difíciles de leer. Los anexos deben comprimirse utilizando herramientas como winzip u otras equivalentes.

*. Se deben borrar periódicamente los correos viejos del buzón de correo, y las copias de correos enviados si ya no los necesita, sobre todo los que tienen archivos adjuntos. Es muy importante no sobrepasar el tamaño de almacenamiento que se le ha asignado a su correo porque esto causa que sus correos dejen de llegar.

*. Todos los correos que envíe deben tener siempre un tema, asunto o subject significativo y acorde para su correo. Si se reciben correos sin asunto, estos deben borrarse inmediatamente sin abrirse e informar al remitente para que este repita el envío de forma correcta.

*. Los mensajes no deben escribirse en letras mayúsculas, ello implica mal genio o que está gritando a la otra persona.

*. Utilizar las casillas “CC (copia a) y CCO (copia oculta a)” y la opción “Responder a todos” con moderación. Informar sólo a quienes necesitan saberlo. Cada copia creada para una persona crea un mensaje adicional en la red.

*. El correo electrónico es un documento de validez legal y prueba de evidencia de acuerdo a la validez jurídica que le otorga la ley 527 del 1999 a los mensajes de

datos digitales. Por consiguiente, tiene el mismo efecto legal que otro medio de correspondencia escrita.

*. Todas las leyes que rigen los derechos de autor, difamación, discriminación y otras formas de comunicación escrita, también se aplican al correo electrónico.

Backups y archivos propios

*. Los backups del Sistema de Control de Inventarios y se realizarán con una periodicidad diaria; Si se cuenta con el servicio de almacenamiento externo, se enviarán 2 copias semanales de la información del Sistema.

*. Cada usuario interno que tenga computador asignado, y que tenga información sensible para la compañía, es responsable por la generación y almacenamiento de las copias de respaldo de su información.

*. Para los equipos de la red corporativa de ZF, se tendrá una unidad central en la cual se realizarán de forma programada a través de un agente de software instalado en cada equipo, las copias de respaldo de las carpetas Mis Documentos y correo de los funcionarios, sin embargo, el dueño de la información debe verificar que la información se almacene de forma correcta.

*. Los funcionarios de las ZF especiales, y en donde no cuenten con un mecanismo centralizado para la realización de copias de respaldo, deben realizarse como mínimo una vez al mes una copia de respaldo de sus archivos en DVD, entregando una copia de las mismas al Depto de Sistemas, el cual tendrá en su poder al menos 1 DVD por cada equipo que irá rotando hasta que su vida útil lo permita, teniendo como regla la devolución al usuario del medio con fecha más antigua, una vez reciba la copia reciente. Para la verificación de la realización y entrega de la correspondiente copia al Depto de Sistemas, se debe diligenciar la Bitácora de control de backup PC's. formato S-F31-PR08.

*. Los DVD's utilizados para la realización de los backups se guardarán en la caja fuerte del área de tecnología.

*. Para el caso del backup del Sistema de Control de Inventarios, las cintas se marcarán con el día de la semana y la fecha a la que corresponde el backup de la información, utilizándose siempre para la elaboración del backup, la cinta con fecha más antigua.

*. Los backups serán acumulativos, no incrementales, es decir, en caso de alguna falla o suceso catastrófico, solo se perderían las operaciones realizadas después del último backup (día o parte del mismo).

*. Todos los computadores de la compañía deben tener instalado el software antivirus aprobado por el área de Sistemas. El mismo debe ejecutarse al menos una vez por semana a todos los discos duros de la PC. Igualmente, todos los discos removibles (diskettes, memory flash, cd's, etc) que se vayan a utilizar en los PC's deben ser verificados antes de trabajar con ellos, aún aquellos que procedan de otros equipos de la compañía. El software antivirus se actualiza de forma automática, sin embargo, si el usuario nota que no se ha realizado dicho proceso, debe comunicarlo al área de Sistemas.

*. La realización y utilización de los backups del Sistema de Control de Inventarios son registrados en la Bitácora de Backups 1 (Formato S-F22-PR08) y Bitácora de Backups 2 (Formato S-F23-PR08).

*. La Zona Franca del Pacífico S.A. no se hará responsable por la información de carácter privado contenida o manipulada en los equipos pertenecientes a la compañía, por lo cual, los datos personales pueden ser extraídos, identificados e incluso eliminados con facilidad si son vistos o manipulados dentro de la red de Zona Franca del Pacífico S.A., esto incluye archivos personales o no autorizados, cuentas de páginas externas, correos electrónicos personales, entre otros.

VI. Equipos

*. El mantenimiento preventivo de los equipos de cómputo debe realizarse cada 3 meses en promedio. Este mantenimiento lo realizará el proveedor con el cual se haya elaborado un contrato; de no contar con ello, el Departamento de Sistemas contactará un proveedor para la realización de tal evento en las fechas establecidas.

*. El mantenimiento de los servidores centrales, debe acordarse con una semana de anticipación y este evento le será notificado a los usuarios inmediatamente se acuerde una fecha con el proveedor.

*. Antes de la ejecución del mantenimiento al servidor central, debe realizarse una copia de respaldo de la información.

*. Para la entrega de equipos de tecnología informática a usuarios internos, el área de Sistemas debe diligenciar el Acta de Entrega de Equipos de TI (Formato S-F92-N02), de la cual entregará copia a Contabilidad para el control de los activos fijos de la compañía.

*. La realización del mantenimiento es registrada en la Bitácora Mantenimiento por equipo electrónico (Formato S-F25-N02).

*. Se ha destinado un equipo para el caso en que se requiera prestar equipos para el uso de usuarios externos, en el área de Servicio al Cliente; de no ser suficiente, y

con previa autorización del responsable del área, se podrá hacer uso de otros equipos de Operaciones para este fin.

*. Todo préstamo de equipos tendrá cobro y debe registrarse en el formato OP-F52-N03.

VII. Soporte técnico

*. Los usuarios internos de la compañía, deben registrar sus inquietudes o incidencias a través del software Eagle, el cual creará un ticket con cada incidencia reportada y le permitirá al mismo realizar el seguimiento de cada uno de ellos. Igualmente, el área de Tecnología registrará las soluciones dadas a cada caso y si las mismas son efectivas, el usuario cerrará el respectivo ticket.

*. El soporte técnico suministrado a los Usuarios es evidenciado en el Registro de Help Desk (Formato S-F26-N02), especificando el problema o solicitud, día, hora, el origen del reporte, quién lo solucionó, día, hora y observaciones.

VIII. Requerimientos a Sistemas

*. Las solicitudes al Departamento de Sistemas que impliquen la realización de nuevos productos o servicios, deben hacerse diligenciando el formato Solicitudes o Requerimientos al Depto de Sistemas (Formato S-F104-N02).

IX. Redes

*. No se permitirá la conexión de equipos ni redes de terceros a la red corporativa de ZONA FRANCA DEL PACIFICO S.A., puesto que no se debe exponer a la compañía a riesgos de piratería de software, virus, programas espías y accesos no autorizados a los datos almacenados en los equipos conectados a la red.

*. La red de Seguridad y CCTV debe estar aislada del resto de la red corporativa, aunque debe ser administrada por el personal de ZONA FRANCA DEL PACIFICO S.A..

*. Cada punto de red perteneciente a la red corporativa de ZFPSA, debe cumplir la normativa o estándares creados para cableado estructurados de datos, con lo cual se garantiza el buen funcionamiento del punto y de la red en general. Igualmente cada punto deberá ser certificado y el respectivo informe generado en dicha labor será archivado por el área de sistemas para comprobaciones futuras. Este procedimiento deberá repetirse cada vez hayan cambios a nivel de puntos de red.

*. Cuando se trate de implementación de centros de datos distribuidos, cada punto deberá constar de gabinete, energía regulada, regleta patch panel, organizador de

cables, patchcords flexibles, switch, y patchcord de la computadora al wallplate (punto de red ubicado en la pared).

*. El cableado estructurado debe ser independiente de las acometidas eléctricas. Cada acometida de datos deberá ser soportada por su respectiva ductería o bandeja debidamente asegurada y administrada, al igual que el cableado para voz y video.