**POLÍTICAS DE SEGURIDAD DE LOS RECURSOS INFORMÁTICOS**

**FEDERACIÓN COLOMBIANA DE PRODUCTORES DE PAPA – FEDEPAPA EN CALIDAD DE ADMINISTRADOR DEL FNFP**

La masiva utilización de recursos informáticos (Computadores, impresoras, redes de datos, etc.) como medio para almacenar, transferir y procesar información, se ha incrementado desmesuradamente en los últimos años, al grado de convertirse en un elemento esencial para el funcionamiento de la sociedad y de las diferentes empresas como FEDEPAPA. En consecuencia, la información, y por consiguiente los recursos mencionados anteriormente, se han convertido en un activo de altísimo valor, de tal forma que, la empresa no puede ser indiferente y se hace necesario proteger, asegurar y administrar la información para garantizar su integridad, confidencialidad y disponibilidad, de conformidad con lo establecido por la ley.

En los últimos años se ha incrementado el uso de aplicaciones electrónicas que comprenden: correo electrónico, internet, transacciones, firmas y certificados digitales, comunicaciones seguras, Software ERP, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores.

La seguridad informática aplica las técnicas fundamentales para preservar la información y los diferentes recursos informáticos con que cuenta la empresa.

La política de seguridad informática es el conjunto de normas, reglas, procedimientos y prácticas que regulan la protección de la información contra la pérdida de confidencialidad, integridad o disponibilidad, tanto de forma accidental como intencionada, al igual que garantizan la conservación y buen uso de los recursos informáticos con que cuenta FEDEAPA.

Para efectos del presente documento se entiende por**:**

**Administrador del sistema.** Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está en cabeza del Ingeniero de Sistemas de la compañía.

**Administrador de correo.** Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un *servidor.*

**Buzón.** También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

**Chat.** (Tertulia, conversación, charla). Comunicación simultánea entre dos o más personas a través de Internet.

**Computador.** Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

**Contraseña o pastor.** Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

**Correo electrónico.** También conocido como e-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

**Cuentas de correo**. Son espacios de almacenamiento en un servidor de correo, para guardar información de correo electrónico. Las cuentas de correo se componen de un texto parecido a este **dpinzon@fedepapa.com** donde " dpinzon " es nombre o sigla identificadora de usuario, " FEDEPAPA " el nombre de la empresa con la que se crea la cuenta o el dominio y ".com" una extensión propio de Internet según el dominio.

**Edición de cuentas de correo.** Mirar o leer el contenido de los correos recibidos o enviados por un usuario.

**Downloads.** Descargar, bajar. Transferencia de información desde Internet a una computadora.

**Electricidad estática**. La corriente estática se presenta cuando no existe ninguna fuerza externa (voltaje) que impulse a los electrones o si estos no tienen un camino para regresar y completar el circuito, la corriente eléctrica simplemente "no circula". La única excepción al movimiento circular de la corriente la constituye la electricidad estática que consiste en el desplazamiento o la acumulación de partículas (iones) de ciertos materiales que tienen la capacidad de almacenar una carga eléctrica positiva o negativa.

**Elementos de tecnología.** Se consideran los siguientes, siendo el Ingeniero de Sistemas responsable de su administración.

* Computadores de escritorio y portátiles: conformados por CPU (Discos duros, memorias, procesadores, main borrad, bus de datos), cables de poder, monitor, teclado, mouse.
* Impresoras, UPS, escáner, lectores, fotocopiadoras, teléfonos, radioteléfonos.
* Equipos de redes comunicaciones como: Switch, router, Hub, Conversores de fibra y demás equipos de redes y comunicaciones.

**Hacker.** Persona dedicada a lograr un conocimiento profundo sobre el funcionamiento interno de un sistema, de una PC o de una red con el objeto de alterar en forma nociva su funcionamiento.

**Internet:** Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

**Intranet.** Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que solo es de uso interno.

**Lan.** (Local Area Network). (Red de Area Local). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

**Log.** Registro de datos lógicos, de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el fin de mantener información histórica para fines de control, supervisión y auditoría.

**Megabyte MB.** Es bien un millón de bytes ó 1.048.576 bytes.

**Messenger:** Opción de mensajería instantánea disponible en Internet. Puede traer problemas en las redes y sistemas privados, por cuanto puede convertirse en una herramienta de tráfico de virus y publicidad no solicitada así como una canal vulnerable para la seguridad de redes y servidores.

**Red:** Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

**Seguridad:** Mecanismos de control que evitan el uso no autorizado de recursos.

**Servidor.** Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

**Servidor de correo.** Dispositivo especializado en la gestión del tráfico de correo electrónico. Es un servidor perteneciente a la red de Internet, por lo que tiene conexión directa y permanente a la Red Pública. Su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

**S.O.** (Sistema Operativo). Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

**Software.** Todos los componentes no físicos de una PC (Programas).

**Usuario**. Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

**Virus.** Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

**Monitoreo de Cuentas de correo.** Vigilancia o seguimiento minucioso de los mensajes de correo que recibe y envía un usuario.

**Web Site**. Un Web Site es equivalente a tener una oficina virtual o tienda en el Internet. Es un sitio en Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado y rápido de la comunicación que facilita el suministro de información de productos o entidades.

Un Web Site es también considerado como un conjunto de páginas electrónicas las cuales se pueden accesar a través de Internet.

**Web Mail.** Es una tecnología que permite acceder a una cuenta de Correo Electrónico (E-Mail) a través de un navegador de Internet, de esta forma podrá acceder a su casilla de correo desde cualquier computadora del mundo.

**Nube:** Lugar que permite almacenar y acceder a datos y programas a través de internet, en lugar de utilizar el Disco Duro de la computadora.

**POLÍTICAS ADOPTADAS – FEDEPAPA**

Considerando que la Federación Colombiana de Productores de Papa - FEDEPAPA, se encuentra en la centralización de Procedimientos, y teniendo en cuenta que a través del Proceso de Tecnología de Información se propone administrar, desarrollar y mantener en buen estado las TIC, garantizando el apoyo logístico para el buen desarrollo de la Gestión; se adoptan las siguientes políticas de seguridad informáticas en la empresa:

1. Cuentas de Usuarios
2. Internet
3. Nube CLARO
4. Correo Electrónico
5. Red Interna
6. Políticas de uso de computadores, impresoras y periféricos
7. Legalidad de Software

Mucho se ha hablado de las mejores prácticas que debemos tener para resguardar nuestra organización con respecto al uso de los recursos informáticos, tales como el correo electrónico, redes y de internet. Hay discusiones sobre confidencialidad, propiedad de la información transmitida en los mensajes, códigos de ética y privacidad del correo.

Hemos realizado un listado de pautas que se deben tener en cuenta para dar un uso adecuado a los recursos informáticos (correo electrónico, red interna, internet) provisto por FEDEPAPA:

El área de sistemas auditará de manera periódica los equipos de cómputo y periféricos así como el software instalado.

El propósito de estas políticas es asegurar que los usuarios utilicen correctamente los recursos tecnológicos que la empresa pone a su disposición para el desarrollo de las funciones institucionales.

Dichas políticas son de obligatorio cumplimiento.

El funcionario que incumpla las políticas de seguridad informática, responderá por sus acciones o por los daños causados a la infraestructura tecnológica de la empresa, de conformidad con las leyes penales, fiscales y disciplinarias.

1. **Cuentas de Usuario**

Es la cuenta que constituye la principal vía de acceso a los sistemas de información que posee la empresa; estas cuentas aíslan al usuario del entorno, impidiendo que pueda dañar al sistema o a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros.

Cada persona que acceda al sistema debe tener una sola cuenta de usuario. Esto permite realizar seguimiento y control, evita que interfieran las configuraciones de distintos usuarios o acceder al buzón de correo de otro usuario.

Una cuenta de usuario asigna permisos o privilegios al usuario para acceder a los sistemas de información y desarrollará actividades dentro de ellas. Los privilegios asignados delimitan las actividades que el usuario puede desarrollar sobre los sistemas de información y la red de datos.

Procedimiento para la creación de cuentas nuevas:

* La solicitud de una nueva cuenta o el cambio de privilegios, deberá hacerse por escrito por el jefe inmediato y ser debidamente autorizada por el área de Sistemas.

* Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad informática y acepta sus responsabilidades con relación al uso de esa cuenta.
* No debe concederse una cuenta a personas que no sean funcionarios de la empresa, a menos que estén debidamente autorizados.

* Los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también incluye a los administradores del sistema.
* Atender el Procedimiento de Creación y Bajas de Acceso.
* La Oficina de Talento Humano debe reportar al área de Sistemas, sobre los funcionarios que cesan sus actividades y solicitar la desactivación de su cuenta.

Cuentas como:

Cuenta de Usuario, Correo electrónico, Usuario SAP, Usuario SIIGO, Usuario CLARO, cambio de contraseñas de red, cambio claves de alarmas.

* Los privilegios especiales de borrar o depurar los archivos de otros usuarios, sólo se otorgan a los encargados de la administración en la oficina de Sistemas
* No se otorgará cuentas a personal externo, ni permitir su acceso remoto, a menos que el área Talento Humano y Sistemas determine que es necesario. En todo caso, esta facilidad solo debe habilitarse por el lapso requerido para efectuar el trabajo (como por ejemplo, reuniones, juntas o exposiciones).
* No se crearán cuentas anónimas o de invitado.

1. **Internet**

Internet es una herramienta cuyo uso autoriza la empresa en forma laboral, debido al uso de nuestro Software ERP SAP que permite el ingreso de información de cada uno de los puntos de venta y administrativos, al igual que algunas otras aplicaciones de uso corporativo como el correo electrónico, página web y consultas básicas, por otro lado se permite el uso de Internet de forma extraordinaria, puesto que contiene ciertos peligros. Los hackers están constantemente intentando hallar nuevas vulnerabilidades que puedan ser explotadas.

Se aplica esta política de seguridad y se realiza monitoreo constante, por lo que se debe tener en cuenta lo siguiente:

A continuación se describen las políticas adoptadas para el uso adecuado de este importante servicio:

* El acceso a internet en horas laborales (de (7:00 am a 6:00 pm) es de uso solo laboral no personal, con el fin de no saturar el ancho de banda y así poder hacer buen uso del servicio.
* No acceder a páginas de entretenimiento, pornografía, de contenido ilícito que atenten contra la dignidad e integridad humana, redes sociales (Facebook, Twitter, Ask, Messenger) o que estén fuera del contexto laboral.
* Al detectar algún usuario que visite sitios con contenido prohibido, se le dará un aviso y se realizará anotación correspondiente en la bitácora de accesos por usuario. Además de entregar un reporte por escrito a su Jefe inmediato.
* En ningún caso recibir ni compartir información en archivos adjuntos de dudosa procedencia, esto para evitar el ingreso de virus al equipo.
* No descargar programas, demos, tutoriales, que no sean de apoyo para el desarrollo de las tareas diarias de cada usuario. La descarga de ficheros, programas o documentos que contravengan las normas de la Federación sobre instalación de software y propiedad intelectual.
* Ningún usuario está autorizado para instalar software en su ordenador. El usuario que necesite algún programa específico para desarrollar su actividad laboral, deberá comunicarlo al área de Sistemas que se encargará de realizar las operaciones oportunas.
* Los empleados de la Federación tendrán acceso solo a la información necesaria para el desarrollo de sus actividades.
* Ningún empleado debe instalar programas para ver vídeos o emisoras de televisión vía Internet y de música. (Ares, REAL AUDIO, BWV, YouTube etc.).
* No debe usarse el Internet para realizar llamadas internacionales (Dialpad, NET2PHONE, FREEPHONE, etc.). Skype solo a usuarios autorizados.
* Se encuentran en los equipos los siguientes navegadores avalados por el área de Sistemas (Internet Explorer, Mozilla Firefox, Google Chrome, Microsoft Edge).

1. **Nube CLARO**

El propósito de la utilización de esta plataforma en la NUBE llamada **CLARO,** consiste en actuar como un proveedor de almacenamiento en la nube (hasta 50GB en la versión gratuita). En esa nube, y por ahora únicamente desde un navegador web (preferiblemente Chrome por lo que indican las FAQ), se pueden subir, almacenar, gestionar o descargar archivos y datos de todo tipo.

La particularidad que se tiene con esta aplicación, consiste, en que el usuario antes de subir un archivo a CLARO, cifra automáticamente esos datos. Quien luegodescarga el archivo, y sólo una vez descargado, descifra el archivo. La información cifrada se limita al nombre del archivo/carpeta y el archivo en sí, pero no a la información personal asociada a la cuenta por ejemplo el email, la IP, la estructura de carpetas, el propietario del archivo o las credenciales de pago se almacenan y procesan sin cifrar y CLARO tiene acceso a esa información tal cual.

Una vez cifrados y subidos los archivos, pueden compartirse con otros usuarios de FEDEPAPA, requiriéndose en ese caso la exportación y transmisión segura de la concreta clave de cifrado, lo que según CLARO es responsabilidad exclusiva del usuario.

A continuación, se relacionan las políticas:

* + El acceso a la aplicación solo estará a cargo por el departamento de Sistemas, ningún usuario deberá realizar descarga o ingreso al aplicativo de manera personal sin la debida autorización.
  + El departamento de Talento Humano será quien solicite al área de Sistemas de Fedepapa los usuarios que estarán autorizados para el uso del aplicativo.
  + El área de Sistemas será quien instale y asigne usuario y contraseña de uso corporativo. Estas contraseñas serán resguardadas por el Ingeniero de Sistemas de la Federación.
  + Ningún usuario deberá tener acceso al aplicativo desde fuera de la Organización, solo será de uso interno para el personal autorizado.
  + Los permisos se colocarán a cada usuario, dependiendo el uso del aplicativo para el cual fue autorizado. No todos los usuarios tendrán los mismos privilegios con que cuenta el aplicativo.
  + Este aplicativo será exclusivamente para uso de documentación necesaria compartida entre diferentes áreas. No se permite la carga de Backup total del equipo.
  + Al detectar algún usuario que incumpla con las políticas brindadas para el Aplicativo CLARO en la Nube, se le dará un aviso al área de talento humano y se realizará anotación correspondiente. Además de entregar un reporte por escrito a su Jefe inmediato.

1. **Correo Electrónico**

El correo electrónico es un privilegio y se debe utilizar de forma responsable. Su principal propósito es servir como herramienta para transmitir las comunicaciones oficiales que apoyen la gestión institucional de la empresa.

Es de anotar que el correo electrónico es un instrumento de comunicación de la empresa y los usuarios tienen la responsabilidad de utilizarla de forma eficiente, eficaz, ética y de acuerdo con la ley.

A continuación se relacionan las políticas:

* Utilizar el correo electrónico como una herramienta de trabajo, y no como nuestra casilla personal de mensajes a amigos y familiares, para eso está el correo personal.
* No facilitar u ofrecer la cuenta y/o buzón del correo electrónico institucional a terceras personas. Los usuarios deben conocer la diferencia de utilizar cuentas de correo electrónico institucionales y cuentas privadas ofrecidas por otros proveedores de servicios en Internet.
* No participar en la propagación de mensajes encadenados o participar en esquemas piramidales o similares.
* No distribuir mensajes con contenidos impropios y/o lesivos a la moral.
* No enviar grandes cadenas de chistes en forma interna.
* Si se recibe un correo de origen desconocido, consulten inmediatamente con el área de Sistemas sobre su seguridad. Bajo ningún aspecto se debe abrir o ejecutar archivos adjuntos a correos dudosos, ya que podrían contener códigos maliciosos (virus, troyanos, keyloogers, gusanos, etc).
* Cuando se contesta un correo, evitar poner "Contestar a todos" a no ser que estemos absolutamente seguros que el mensaje puede ser recibido por "todos" los intervinientes.
* El acceso a las cuentas personales debe ser mínimo (o ninguno) durante nuestra jornada laboral.
* El área de Sistemas validará los usuarios que tienen asignada una cuenta de correo electrónico institucional y se deberá establecer una contraseña cada tres meses, dicha contraseña solo se conocerá por el área de Sistemas, con el fin de hacer uso adecuado del Servidor de almacenamiento.
* Cuando el usuario deje de usar su estación de trabajo deberá cerrar el software de correo electrónico, para evitar que otra persona use su cuenta de correo.
* Los usuarios que tienen asignada una cuenta de correo electrónico institucional, deben mantener en línea el software de correo electrónico (si lo tiene disponible todo el día), y activada la opción de avisar cuando llegue un nuevo mensaje, o conectarse al correo electrónico con la mayor frecuencia posible para leer sus mensajes.
* Se debe eliminar permanentemente los mensajes innecesarios.
* Se debe mantener los mensajes que se desea conservar, agrupándolos por temas en carpetas personales.
* Utilizar siempre el campo “asunto” a fin de resumir el tema del mensaje.
* Expresar las ideas completas, con las palabras y signos de puntuación adecuados en el cuerpo del mensaje.
* Enviar mensajes bien formateados y evitar el uso generalizado de letras mayúsculas.
* Evite usar las opciones de confirmación de entrega y lectura, a menos que sea un mensaje muy importante, ya que la mayoría de las veces esto provoca demasiado tráfico en la red.
* Evite enviar mensajes a listas globales, a menos que sea un asunto oficial que involucre a toda la Federación.
* Los mensajes tendrán una vigencia no mayor de 10 días desde la fecha de entrega o recepción de los mismos. Superada la fecha de vigencia, los mensajes deberán ser eliminados del servidor de correo.
* Si se desea mantener un mensaje en forma permanente, éste debe almacenarse en carpetas personales.
* Queda prohibido el uso del correo Institucional para el uso de correo masivo o publicidad no relacionada con Fedepapa, cualquier tipo de archivo ilegal, archivos de música.

1. **Red Interna**

**Oficina Central Administrativa**

* Se deja equipos periféricos (Impresoras) conectados a la red interna para uso exclusivo del personal de la Federación.
* No utilizar la red con fines propagandísticos o comerciales.
* No modificar ni manipular archivos que se encuentren en la red que no sean de su propiedad.
* No guardar en la red música, videos o demás archivos de uso personal ni material innecesario.
* Se realzará una copia de Seguridad, según clasificación de usuarios determinada por el área de Sistemas.

1. **Políticas de Seguridad de uso de Computadores, Impresoras y Periféricos.**

* La infraestructura tecnológica: servidores, computadores, impresoras, UPS, escáner, lectoras y equipos en general; no puede ser utilizado en funciones diferentes a las institucionales.
* Los usuarios no pueden instalar, suprimir o modificar el software originalmente entregado en su computador. Es competencia del área de sistemas la instalación de software.
* No se puede instalar ni conectar dispositivos o partes diferentes a las entregadas en los equipos. Es competencia de la Oficina de sistemas, el retiro o cambio de partes.
* Cada vez que se ingrese una memoria USB, deberá ser vacunada de inmediato por el antivirus con que cuenta su computadora.
* No es permitido destapar o retirar la tapa de los equipos, por personal diferente a la Oficina de sistemas o bien sus asistentes o sin la autorización de esta.
* Los equipos, escáner, impresoras, lectoras y demás dispositivos, no podrán ser trasladados del sitio que se les asignó inicialmente, sin previa autorización del área de sistemas.
* Se debe garantizar la estabilidad y buen funcionamiento de las instalaciones eléctricas, asegurando que los equipos estén conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra.
* Es estrictamente obligatorio, informar oportunamente al área de sistemas la ocurrencia de novedades por problemas técnicos, eléctricos, de planta física, líneas telefónicas, recurso humano, o cualquiera otra, que altere la correcta funcionalidad de los procesos. El reporte de las novedades debe realizarse tan pronto se presente el problema.
* Los equipos deben estar ubicados en sitios adecuados, evitando la exposición al sol, al polvo o zonas que generen electricidad estática.
* Ningún funcionario, podrá formatear los discos duros de los computadores.
* Ningún funcionario podrá retirar o implementar partes sin la autorización del área de sistemas.
* Si hace falta algo en su puesto de trabajo correspondiente al área de Sistemas, se debe informar via e-mail al Ingeniero encargado, con el fin de darle trámite en caso de ser aprobado por el área.

1. **Legalidad de Software**

* Cualquier licencia de software propiedad de FEDEPAPA, deberá ser registrada en la base de datos del Departamento de Sistemas de la Información, conocida como Control de Licencias de Software.
* Es atribución exclusiva del área de Sistemas dimensionar las necesidades de software de FEDEPAPA.
* Las licencias propiedad de FEDEPAPA deberán ubicarse físicamente en un lugar específico único para Licencias, bajo resguardo del Departamento de Sistemas.
* La instalación de Software a equipos de cómputo se realizará exclusivamente con licencias propiedad de FEDEAPA.
* Bajo ninguna circunstancia se instalarán licencias propiedad del usuario o de alguna otra entidad. Excepción a este artículo serán las licencias de prueba (Shareware) o libres (Freeware).
* Es facultad exclusiva del área de Sistemas realizar la instalación de software en los equipos de cómputo.

.

* Bajo ninguna circunstancia se permitirá al usuario realizar instalaciones de software, esto con el fin de garantizar el buen desempeño del software y de gestionar las licencias de propiedad de FEDEPAPA.
* La solicitud de software especializado deberá ser solicitado al Ingeniero de Sistemas y este a su vez deberá incluir una lista de actividades a realizar con esta licencia.

***“El correcto manejo de los equipos de sistemas de la empresa es responsabilidad directa de sus trabajadores”.***

**DAVID PINZÓN ROJAS**

Ingeniero de Sistemas