	NOMBRE	CARGO	FIRMA
ELABORÓ	Juan Carlos Hoyos Avendaño	Profesional de Servicios TI	
REVISÓ	Liliana Patricia Mejía Zapata	Coordinadora de Servicios Administrativos	
	Ana María Espinosa Ángel	Directora Administrativa y Financiera	
	Adrián Alberto Castañeda Sánchez	Jefe Jurídico	
APROBÓ	Claudia Elena Gómez Rodríguez	Directora Ejecutiva	

CONTROL DE CAMBIOS

Versión	Fecha de Aprobación	Descripción del Cambio (Qué y Por qué)
02	20/10/2008	Actualización
03	11/07/2018	Actualización

CONTENIDO

INTRODUCCIÓN

La seguridad informática, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que atiendan las necesidades de la Institución en materia de seguridad, apoyando el cumplimiento de los objetivos planteados y los enmarcados en la misión y visión de la Fundación EPM.

Toda la información que genera, procesa o intercambia la Fundación EPM, es de su propiedad y constituye parte de su activo. Los usuarios deben proteger la información a la cual tiene acceso contra el uso indebido, la divulgación o modificación por parte de personas no autorizadas, so pena de incurrir en las sanciones que establece la ley. Los servicios informáticos son de uso exclusivo para actividades relacionadas con la Fundación EPM y podrán ser monitoreadas por ésta.

La información es uno de los recursos principales de las organizaciones, por ello es de suma importancia darle el manejo adecuado con el fin de mitigar los riesgos.

Las políticas son directrices documentadas que rigen el modo como se adelantan ciertos procesos dentro en la Entidad. También, orientan sobre el tratamiento que se debe dar en el caso de presentarse una dificultad o una situación adversa.

La política de Seguridad Informática, Es el conjunto de criterios que se deben cumplir en la Fundación para salvaguardar la información, propender por el uso correcto de las herramientas informáticas y mantener la continuidad de la Fundación EPM en caso de presentarse un incidente de seguridad.

1. Objetivo

Contribuir a mantener la confiabilidad, disponibilidad e integridad de la información y el aprovechamiento de los recursos informáticos que sean de propiedad de la Fundación EPM o no, siempre que se encuentren al servicio de la Entidad, a través de:

- Establecer las bases del debido uso de los recursos informáticos.
- Orientar las actuaciones de los usuarios a través de instructivos y/o procedimientos a adoptar en distintas situaciones de ocurrencia repetidas.

2. Alcance

Las políticas informáticas aquí plasmadas deberán ser aplicadas y cumplidas por parte de todos los empleados, contratistas y Aliados de la Fundación EPM y sobre todos los recursos informáticos que sean o no propiedad de la Fundación EPM, siempre que se encuentren al servicio de la Entidad.

3. Glosario de términos

ACL (Access Control List - Lista de Control de Acceso): Es una lista de permisos de usuario para un archivo, carpeta u otro objeto. Define qué usuarios y grupos pueden acceder al objeto y qué operaciones pueden realizar.

Administrador: Toda persona responsable por la operación día a día de un sistema de cómputo o red de computo.

Adware: Es el nombre que se le da a los programas diseñados para mostrar anuncios en el computador, redirigir solicitudes de búsqueda a sitios web publicitarios y recopilar datos de tipo de comercial sobre las personas.

Antivirus: El software antivirus es un programa o conjunto de programas diseñados para prevenir, buscar, detectar y eliminar virus de software y otros programas maliciosos como gusanos, troyanos, adware y más.

Aplicación: Una aplicación es cualquier programa, o grupo de programas, que está diseñado para el usuario final. El software de aplicaciones (también llamado programas de usuario final) incluye elementos como programas de bases de datos, procesadores de texto, navegadores web y hojas de cálculo.

Autenticidad: Proceso mediante el cual se tiene un alto grado de certeza de la correcta identificación de personas, equipos, interfaces, datos y procesos.

Automatización: Ejecución automática de ciertas tareas con el fin de agilizar el desarrollo de los procesos

Autorización: Proceso de dar privilegios a los usuarios.

Backdoor: Es un programa informático malicioso que se utiliza para proporcionar al atacante acceso remoto no autorizado a un computador comprometido mediante la explotación de vulnerabilidades de seguridad. Un Backdoor funciona en segundo plano y se oculta del usuario. Es muy similar a otros virus de malware y, por lo tanto, es bastante difícil de detectar. Es uno de los tipos de parásitos más peligrosos, ya que le da a una persona maliciosa la capacidad de realizar cualquier acción posible en un computador remoto.

Botnet: Es un grupo de computadoras conectadas de manera coordinada con fines maliciosos. Cada computadora en una botnet se llama bot. Estos bots forman una red de datos que es maliciosamente controlada por un tercero y utilizada para transmitir malware o correo no deseado, o para lanzar ataques.

Un botnet también puede ser conocido como un ejército zombie.**BYOD:** Se refiere a los empleados que llevan sus propios dispositivos informáticos, como teléfonos inteligentes, computadores portátiles o tabletas, al lugar de trabajo para su uso y conectividad en la red corporativa segura.

CAL (Client Access Licenses – Licencias de Acceso de Cliente): Es una licencia que otorga a un usuario o dispositivo el derecho a acceder a los servicios de un servidor. El licenciamiento por Servidor está orientado a servidores físicos de uno o dos procesadores. El licenciamiento por Procesador está orientado a instancias físicas y/o virtuales y considera el número de procesadores físicos de cada servidor para licenciar.

Carácter especial de contraseña: Son aquellos símbolos que se pueden usar al momento de crear un password. Por ejemplo, @ % + \ / ' ! # $ ^ ? : . ( ) { } [ ] ~ ` - _

CMDB (Configuration Management Database – Base de Datos de Gestión de Configuración): En una base de datos que contiene toda la información relevante sobre los componentes de hardware y software utilizados en los servicios de TI de la organización y las relaciones entre esos componentes. Proporciona una vista

organizada de los datos de configuración y un medio para examinarlos desde cualquier perspectiva deseada.

Computación en la nube (Cloud Computing): Es un término utilizado para describir servicios proporcionados a través de una red por una colección de servidores remotos. Esta "nube" abstracta de computadoras proporciona una gran capacidad de almacenamiento distribuido y de procesamiento a la que se puede acceder desde cualquier dispositivo conectado a Internet que ejecute un navegador web.

Los tipos de sistema en la nube que existen hasta ahora son: nube pública, nube privada y nube híbrida y sus modalidades, software como servicio (SaaS), infraestructura como servicio (IAAS), plataforma como servicio (PaaS).

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006].

Continuidad del servicio TI: Procedimientos de continuidad adecuados y justificables en términos de costos para cumplir con los objetivos propuestos en el renglón de continuidad en la organización. Esto incluye el diseño de planes de recuperación y medidas de reducción de riesgo.

Contraseña o password: Conjunto de caracteres que forman una palabra secreta y que sirve a un usuario para identificarse de manera única ante un sistema.

Control de Acceso: Es el que se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que le sea permitido el acceso al sistema.

Copia de seguridad (Backup): Es el proceso de respaldo de archivos o bases de datos físicos o virtuales a un sitio secundario para la preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de datos es fundamental para un plan de recuperación de desastres (DR) exitoso.

Correo Basura: Correos no deseados

Correo electrónico: Redacción, envío o recepción de mensajes sobre sistemas de comunicación.

Correo Spam: Correo electrónico no deseado que se envía a un destinatario especifico, sin su consentimiento u aprobación, generalmente en forma masiva y con fines comerciales

Cuenta de usuario: Es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.

Datos: Representación de hechos, conceptos en una manera formal, apropiada para comunicación, interpretación o procesamiento manual o automático.

DDOS (Distributed Denial of Service – Ataque Distribuido de Denegación de Servicio): Un tipo de ataque en el que un número de computadores u otros dispositivos inundan con paquetes de datos un sitio web hasta que se queda sin posibilidad de aceptar más solicitudes y, para los clientes habituales, parece estar fuera de línea. Este es uno de los usos que se les da a los botnets.

Día Cero: Vulnerabilidad de software que el fabricante desconoce y para la que, por lo tanto, no existen parches o actualizaciones de seguridad. Si los cibercriminales descubren un Día Cero, ejecutan un exploit para atacar los sistemas afectados.

Dirección IP: Cada nodo en una red TCP/IP requiere de una dirección numérica que identifica una red y un anfitrión local o nodo de la red, esta dirección se compone de cuatro números separados por puntos, por ejemplo, 10.2.1.250

Disco duro: Es parte de una unidad a menudo llamada "unidad de disco" o "unidad de disco duro", que almacena y proporciona un acceso relativamente rápido a grandes cantidades de datos en una superficie o conjunto de superficies cargadas electromagnéticamente.

Disponibilidad: Es un servicio que permite que los usuarios autorizados tengan acceso a los activos de información en el lugar, momento y forma requeridos.

Exploit: Un exploit es el uso de software, datos o comandos para "explotar" alguna debilidad en un sistema o programa informático para llevar a cabo acciones dañinas, como un ataque de denegación de servicio, caballos de Troya, gusanos o virus. La debilidad en el sistema puede ser un error, un fallo o simplemente una vulnerabilidad de diseño. Un exploit remoto explota la vulnerabilidad de seguridad sin tener acceso previo al sistema. Un exploit local necesita acceso previo al

sistema vulnerable y generalmente implica aumentar los privilegios de la cuenta de usuario que ejecuta el exploit. Aquellos que utilizan este tipo de ataques a menudo usan ingeniería social para obtener información crítica necesaria para acceder al sistema.

Firewall: Es un sistema de seguridad de red diseñado para evitar el acceso no autorizado a o desde una red privada. Los firewalls se pueden implementar como hardware y software, o como una combinación de ambos. Los de red se utilizan con frecuencia para evitar que usuarios de Internet no autorizados accedan a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que ingresan o salen de la intranet pasan por el firewall, que examina cada mensaje y bloquea aquellos que no cumplen con los criterios de seguridad especificados.

Freeware: Software de libre distribución.

FTP. File transfer Protocol: Es un programa de transferencia de archivos en entornos TCP/IP como internet FTP, se utiliza para conectarse con otro sistema y ejecutar varias órdenes de generación de listas y transferencia de archivos entre ambos sistemas.

Hardware: Se refiere a las partes físicas de un computador y dispositivos relacionados. Los dispositivos de hardware interno incluyen motherboards, discos duros y memoria RAM. Los dispositivos de hardware externos incluyen monitores, teclados, mouse, impresoras y escáneres.

ICQ: Programa de mensajería instantánea en línea desarrollado por Mirabilis LTD. Es usado como una herramienta de conferencia en la red para pláticas electrónicas vía teclado (“chatear”), mandar correos electrónicos y ejecutar transferencias de archivos, jugar juegos de computadoras, etc.

Ingeniería social: Es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para la obtención de una contraseña o acceso a un sistema de información.

Integridad: Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.

Internet: A veces llamada simplemente "la red", es un sistema mundial de redes informáticas que proporciona una variedad de instalaciones de información y

comunicación y que consta de redes interconectadas que utilizan protocolos de comunicación estandarizados.

Intranet: Es un servidor Web seguro, interno y exclusivo, que le da a los empleados y al personal de una institución o compañía la posibilidad de compartir información sin que se exponga a la comunidad Web en general.

Inyección SQL: (SQLi) se refiere a un ataque de inyección en el que un atacante puede ejecutar sentencias SQL maliciosas (también comúnmente denominadas carga maliciosa) que controlan el servidor de bases de datos de una aplicación web. Dado que una vulnerabilidad de Inyección SQL podría afectar a cualquier sitio web o aplicación web que utilice una base de datos basada en SQL, la vulnerabilidad es una de las más antiguas, más prevalentes y más peligrosas de las vulnerabilidades de las aplicaciones web.

Jailbreak: En el contexto de un dispositivo móvil, es el uso de un exploit para eliminar las restricciones del fabricante o del operador de un dispositivo como un iPhone o iPad. El exploit generalmente implica ejecutar un ataque a escala de privilegios en el dispositivo de un usuario para reemplazar el sistema operativo instalado por el fabricante con un kernel personalizado.

Kernel: Es el componente central de un sistema operativo. Mediante la comunicación entre procesos y las llamadas al sistema, actúa como un puente entre las aplicaciones y el procesamiento de datos realizado a nivel de hardware. Cuando un sistema operativo se carga en la memoria, el kernel se carga primero y permanece en la memoria hasta que el sistema operativo se apaga nuevamente. Es responsable de procesos de bajo nivel como la gestión de discos, la gestión de tareas y la gestión de memoria.

Keylogger: Es un spyware malicioso que se utiliza para capturar información confidencial mediante el registro de teclas. Éste captura información de contraseñas o información financiera, que luego se envía a terceros para su explotación criminal.

Malvertising: Es una forma maliciosa de publicidad en Internet utilizada para propagar malware. Generalmente se ejecuta ocultando código malicioso en anuncios en línea relativamente seguros. Estos anuncios pueden llevar a la víctima a contenido no confiable o infectar directamente el computador de la víctima con malware, que puede dañar un sistema, acceder a información confidencial o incluso controlar el computador a través del acceso remoto.

Malware (malicious software): Es cualquier programa o archivo que es dañino para un usuario de computador. El malware incluye virus informáticos, gusanos, caballos de Troya y spyware. Estos programas maliciosos pueden realizar una variedad de funciones, que incluyen robar, cifrar o eliminar datos confidenciales, alterar o secuestrar funciones de cómputo central y supervisar la actividad del computador de los usuarios sin su permiso.

Navegar por la red: Es la acción de visitar páginas en la World Wide Web por medio de una aplicación llamada explorador y que contiene documentos de hipertexto interconectados y accesibles vía Internet.

No repudio: No repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío. No repudio en destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción del mismo.

OEM: Un fabricante de equipos originales (OEM) fabrica piezas o componentes que se utilizan en los productos de otra empresa. Un componente de OEM puede ser una pieza, un subsistema o software. Algunos ejemplos son los sistemas operativos y los microprocesadores en equipos. Por lo general, el fabricante de equipos no fabrica ni el microprocesador ni el SO. En su lugar, el fabricante de equipos compra estas piezas de otras empresas como OEM. En este sentido, OEM también puede ser un verbo: "comprar como OEM una pieza" de otra empresa.

Proceso: Conjunto de instrucciones para el cumplimiento de una etapa especifica señalada

Ransomware: Es un subconjunto de malware en el que los datos del computador de la víctima están bloqueados, generalmente mediante cifrado, y se exige el pago antes de que los datos rescatados se descifren y se devuelva el acceso a la víctima. El motivo de los ataques de ransomware es casi siempre monetario, y a diferencia de otros tipos de ataques, generalmente se notifica a la víctima que ha ocurrido un ataque y se le dan instrucciones sobre cómo recuperarse del ataque. El pago a menudo se exige en una moneda virtual, como Bitcoin, por lo que no se conoce la identidad del ciberdelincuente.

Recuperación de desastres: Consiste en las precauciones que se adoptan para minimizar los efectos de un desastre y que la organización pueda continuar operando o reanudar rápidamente las funciones de misión crítica.

Recursos informáticos / Activos informáticos: Hardware, software, equipos de cómputo y telecomunicaciones

Red: Es un sistema de comunicación que se da entre diversos recursos informáticos por medio de protocolos para permitir el intercambio de información.

Regla de negocio: Describe las políticas, normas, operaciones, definiciones y restricciones presentes en una organización y que son de vital importancia para alcanzar los objetivos misionales.

RFC: Los documentos RFC (Request for Comments) han sido utilizados por la comunidad de Internet como una forma de definir nuevos estándares y compartir información técnica. Investigadores de universidades y corporaciones publican estos documentos para ofrecer mejores prácticas y solicitar comentarios sobre las tecnologías de Internet. Las RFC son administradas hoy por una organización mundial llamada Internet Engineering Task Force (IETF).

Riesgo: Es una pérdida o daño futuro potencial que puede surgir por un actuar presente

Rooting: Es el término utilizado para describir el proceso de obtener acceso a la raíz o control privilegiado sobre dispositivos, más comúnmente teléfonos inteligentes y tabletas con sistema operativo Android. También se puede hacer rooting en dispositivos basados en entornos Linux. El rooting permite que un usuario normal tenga permisos de administrador en el entorno del sistema operativo. En el caso de los dispositivos Android, ayuda a eludir la arquitectura de seguridad, pero si no se hace correctamente, podría causar problemas.

Rootkit: Un grupo de programas que sirven para ganar privilegios en un computador de forma subrepticia, así como para ocultar información tanto del administrador legítimo como del sistema operativo. Se lo usa, típicamente, para acceder a un sistema con credenciales de administrador.

SAI - Sistemas de Alimentación Ininterrumpida: Es un dispositivo de hardware que proporciona una fuente de alimentación de respaldo en caso de un corte de energía (apagón), baja de voltaje o un aumento en la potencia. Un SAI proporciona energía suficiente para que un computador se cierre correctamente o permanezca funcional durante la interrupción. Hay tres versiones del SAI: en espera, en línea y en línea interactiva.

Scareware: Es un tipo de software que aparece como una ventana emergente en un computador. Este software se disfraza como un mensaje de advertencia, pero no es más que un truco destinado a asustar (scare) al propietario del equipo para que revele su información personal.

Una vez que el usuario accedió a dar acceso al software de su computador, comienza el escáner malicioso.

Seguridad: Medida tomada para reducir el riesgo

Servidor Proxy: Es un computador que funciona como intermediario entre una estación de trabajo de un usuario y el internet. Se instala por seguridad, control administrativo y servicio de caché, disminuyendo el tráfico de internet e incrementando la velocidad de acceso.

Servidor: Es una instancia de un programa de computador que acepta y responde a solicitudes hechas por otro programa, conocido como cliente. De forma menos formal, cualquier dispositivo que ejecute software de servidor también podría considerarse un servidor. Los servidores se usan para administrar recursos de red. Por ejemplo, un usuario puede configurar un servidor para controlar el acceso a una red, enviar o recibir correo electrónico, administrar trabajos de impresión o alojar un sitio web.

Shareware: Software de libre distribución que cuenta con un periodo de pruebas que puede variar entre 30 y 60 días.

Software de aplicación: maneja multitud de tareas comunes y especializadas que un usuario desea realizar, como contabilidad, comunicación, procesamiento de datos y procesamiento de textos.

Software: Información organizada en forma de sistemas operativos, utilidades, programas y aplicaciones que permiten que los computadores funcionen. Consiste en instrucciones y códigos cuidadosamente organizados escritos por programadores en cualquiera de los diferentes lenguajes de programación especiales. El software se divide comúnmente en dos categorías principales: Software del sistema: controla las funciones básicas (e invisibles para el usuario) de un computador y generalmente viene preinstalado con la máquina.

Spam: Publicidad no solicitada que llega por correo electrónico u otros medios. Normalmente, no es más que una molestia que los filtros antispam de los principales proveedores de correo mantienen a raya. Pero pueden también

contener links maliciosos, en cuyo caso pasan a ser una forma de phishing que, en lugar de alertarnos sobre un problema, nos tienta con un supuesto aviso de publicidad.

Spyware: El software espía es un software que se instala en un dispositivo informático sin que el usuario final lo sepa. Dicho software es controvertido porque, a pesar de que a veces se instala por razones relativamente inocuas, puede violar la privacidad del usuario final y tiene el potencial de ser objeto de abuso.

TELNET: Es el programa de inicio de sesión y emulación de terminal para redes TCP/IP como internet. Su principal funciona es permitir a los usuarios iniciar la sesión en sistemas anfitriones remotos.

TI (Tecnología de la Información): Conjunto de herramientas, procesos y metodologías (como codificación o programación, comunicaciones de datos, conversión de datos, almacenamiento y recuperación, análisis y diseño de sistemas, control de sistemas) y equipos asociados empleados para recopilar, procesar y presentar información. En términos generales, TI también incluye automatización de oficinas, multimedia y telecomunicaciones.

Unidades de almacenamiento: Dispositivos que se usan para guardar y localizar la información de forma ordenada para acceder a ella cuando se necesario. Pueden ser internos como el disco duro o externos como memorias USB, unidades de CD, unidades de DVD, unidades de Blu-ray (BD), tarjetas de memoria SD.

Usuario informático: Puede ser un humano o una computadora que tiene permisos de acceso a un sistema de información en el cual fue previamente agregado con algunos privilegios y ciertas restricciones.

Virus: Un virus informático es un código malicioso que se replica copiándose en otro programa, documento o sector de arranque del computador y cambia el funcionamiento de este. El virus requiere que alguien, consciente o inconscientemente, disemine la infección sin el conocimiento o permiso del usuario o administrador del sistema.

Vulnerabilidad Crítica: Una vulnerabilidad crítica es una característica o una falla de un software que permite ejecutar código de forma remota, obtener privilegios de administrador o filtrar datos sensibles de ese sistema.

Wi-Fi: Es un protocolo de red inalámbrica que permite a los dispositivos comunicarse sin cables de Internet. Es técnicamente un término de la industria que representa un tipo de protocolo de red de área local (LAN) inalámbrica basado en el estándar de red IEEE 802.11. Este es el medio más popular para comunicar datos de forma inalámbrica, dentro de una ubicación fija. Es una marca registrada de Wi-Fi Alliance, una asociación internacional de compañías involucradas con tecnologías y productos LAN inalámbricos.

3. Condiciones Generales

3.1. Clasificación de la Información:

- **Altamente confidencial:** Es la información con el más alto grado de sensibilidad. Si se divulga sin la debida autorización, puede causar pérdidas económicas o de imagen y poner en riesgo la supervivencia de la Entidad. Su utilización por parte de la competencia o personal externo va en detrimento de los intereses de la Fundación EPM.
- **Confidencial:** Es la información sensible. Su utilización inadecuada puede traer efectos adversos para la empresa.
- **Restringida:** Es la información de uso interno para el personal autorizado, en función de los diferentes perfiles que cada uno tenga. También se encuentra establecida dentro de esta clasificación la información que es exclusiva del cliente y que sólo debe ser conocida por él.
- **Pública:** Es la información a la que cualquier persona puede tener acceso.

3.2. Propiedad de los Recursos y de la Información.

- Los recursos que la Fundación EPM pone a disposición de los empleados deben utilizarse para fines relacionados con las actividades y obligaciones de la organización.
- Se debe hacer un buen uso y ser cuidadoso con los equipos puestos a su disposición: impresoras, computadoras, software, teléfonos,

faxes, archivos de documentos e información. Recuerde que USTED es el RESPONSABLE de los mismos.

- La administración de la información almacenada en los recursos informáticos es responsabilidad del empleado y propiedad de la Fundación EPM.
- Todos los Contratistas del grupo EPM, que tienen acceso a la red corporativa de datos son responsables por el cumplimiento de las políticas de seguridad y contingencia informática.

3.2. Divulgación de la Información.

"Uno de los principales riesgos y factores de fuga de información es la "Ingeniería Social", con la cual se manipula la confianza de las personas para lograr tener acceso a la información. Por esta razón debemos velar por el cumplimiento de las políticas para minimizar el riesgo."

Aspectos Claves:

- No discuta información confidencial de la empresa en sitios públicos o en vehículos y medios de transporte masivo.
- No facilite los equipos y sistemas de información de la empresa a personas no autorizadas.
- No utilice los recursos informáticos y de telecomunicaciones para otras actividades que no estén directamente relacionadas con su trabajo.
- No extraiga datos fuera de la sede de la empresa sin la debida autorización.
- No revele información telefónicamente a menos que esté seguro de la identidad del interlocutor que la está solicitando.
- No envíe a través de internet mensajes con información confidencial a no ser que esté cifrada (protegida/encriptada).
- No divulgue su contraseña a nadie. Con ella pueden realizarse actos indebidos en su nombre.
- No suministre su login a terceros.

- Siempre adopte una actitud reservada con personas que intenten obtener información personal suya o de sus compañeros.

3.4 Manejo de Documentos

- Guarde la información sensible bajo llave cuando no la esté usando y, especialmente, cuando usted se vaya a retirar de su puesto de trabajo.
- Bloquee manualmente su pantalla cuando se vaya a alejar de su puesto de trabajo. Su equipo se demora unos segundos en bloquearse automáticamente y en ese tiempo se corre riesgo.
- Cuando imprima información sensible o confidencial, retírela rápidamente de la impresora y preferiblemente esté presente al momento de imprimir.
- Cuando no vaya a hacer uso adicional de los documentos, destruya los que contengan información confidencial. Para ello utilice preferiblemente máquinas destructoras de papel.
- Mantenga una conducta de “escritorios limpios”.
- No deje documentos confidenciales con su contenido visible.
- Cerciórese de que los datos e información confidencial que aparecen en la pantalla de su computador no sean vistos por personas no autorizadas. Haga uso adecuado del protector de pantalla y de su contraseña.
- Asegúrese de no reutilizar como papel borrador hojas de documentos que contengan información confidencial.
- No utilice recordatorios escritos que expongan información confidencial.
- Verifique cuidadosamente los destinatarios de la correspondencia para evitar el desvío de información y los errores en la entrega de la misma.
- Destruya adecuadamente la correspondencia y documentos que desecha, ya que pueden contener información confidencial.

- De conformidad con el Reglamento Interno de Trabajo de la Fundación EPM **,** en su Título de Prohibiciones al Empleador y sus Trabajadores se **PROHIBE** expresamente a los trabajadores:

  - Sustraer o ayudar a sustraer de las dependencias de la Fundación EPM , los útiles o elementos de trabajo, las materias primas, sistemas elaborados, mercancía almacenada, información o documentos de la entidad o de los empleados, sin permiso escrito de la Fundación EPM .
  - Suministrar a extraños, sin autorización expresa de la Fundación EPM , datos relacionados con la organización interna de la misma o respecto de sus sistemas, servicios o procedimientos.
  - Ingresar CD u otros dispositivos para compartir o gravar información de carácter confidencial, para fines personales y beneficio de terceros.

4. Políticas de control y gestión de accesos y privilegios

- La creación de cuenta de usuario deberá ser solicitada por el jefe inmediato del empleado a través del formato FR-019 Requisición y Alistamiento puesto de trabajo y enviada a la Coordinación de servicios administrativos. Esta cuenta será solicitada a través del catálogo de servicios de EPM por parte de servicios TI y deberá ser aprobada por el profesional de servicios TI. Las políticas de creación de cuentas de usuario están definidas según los lineamientos de EPM.
- El Directorio activo solicitará el cambio de contraseña cuando el usuario de red inicie sesión por primera vez.
- Una persona deberá tener asignada solo una cuenta de usuario de acceso a los servicios informáticos de la Fundación EPM.
- Las cuentas de usuario estarán vigentes solo mientras exista un vínculo contractual entre el empleado y la Fundación EPM.

- Cuando se presenten novedades laborales que impliquen la ausencia del empleado, la cuenta de usuario de red se deshabilitará hasta que finalice la novedad. Estas serán reportadas por el área de Gestión humana.
- Los permisos de acceso a los recursos informáticos y servicios de la red de datos deben ser solicitados e implementados por el personal responsable del servicio de TI y aprobados por los niveles jerárquicos de la Fundación EPM.
- Se debe poder identificar de manera inequívoca cada usuario y hacer seguimiento de las actividades que éste realiza. Para el caso de Empleados en Misión contratados a través de empresa temporal se le creara un usuario cumpliendo las mismas políticas de creación de usuarios de EPM, y catalogados como contratistas de la Fundación EPM.

- Para que a un colaborador se le pueda autorizar y solicitar el acceso a programas y/o aplicativos de software, es requisito indispensable que tenga ya aprobada una cuenta de usuario de red de la Fundación EPM. Salvo los casos en que los equipos no se encuentren en el dominio.

- Cada área de la Fundación EPM es responsable de reportar cada que aplique y solicitar la depuración de los usuarios de los sistemas de información y sus derechos de acceso y privilegios. Así mismo, la dependencia de Servicios TI deberá comparar y depurar ese listado con el de empleados activos generado por el área de Gestión Humana.

- Los usuarios son responsables de realizar un adecuado uso de los recursos tecnológicos y servicios de la red que se ponen a su disposición.

- Todas las personas que laboran en la Fundación EPM y que estén conectadas a la red de datos son responsables por el cumplimiento de los lineamientos reglas de negocio y procedimientos con respecto a la seguridad de TI.

- La información que sea considerada confidencial y sensible deberá ser transmitida de manera segura a través de una ruta o medio confiable

(equipos de comunicaciones) con controles para brindar autenticidad de contenido, prueba de envío, y no repudio de origen o destino.

- La cuenta de usuario y la contraseña de acceso a la red corporativa de la Fundación EPM es personal e intransferible. El usuario es responsable por el uso de los privilegios que le sean asignados.

- El número máximo de intentos fallidos de inicio de sesión es de diez (10); después de ello, la cuenta se bloqueará.
    - Nota: Esta política es la establecida por el Grupo EPM. Sin embargo, lo recomendado es: por encima de 4 intentos para permitir el error del usuario, y por debajo de 10 para evitar ataques de fuerza bruta.
- Cuando no estén en uso, las estaciones de trabajo y los portátiles y deben estar bloqueados a fin de impedir la extracción de la información de los equipos utilizando herramientas externas al equipo.
- Cuando un colaborador cesa sus actividades en la Fundación EPM se solicitará la desactivación de su cuenta del directorio activo y todas las aplicaciones a las que tenga acceso

- El usuario debe elegir una contraseña que no pueda ser adivinada fácilmente.

- Para crear o cambiar una contraseña se deben tener en cuenta las siguientes características: tener mínimo 8 caracteres, contener por lo menos una mayúscula, una minúscula, un número y un carácter especial soportado por contraseñas.

- No debe haber conexión lógica entre la contraseña y el usuario, como por ejemplo: el nombre, la fecha de nacimiento y similares.

- La contraseña de acceso a la red corporativa de datos debe ser cambiada cada 25 días con el fin de minimizar los riesgos de pérdida o filtración de la información. El cambio es obligado por el sistema, el cual notifica al usuario sobre su vencimiento

- Cada usuario será responsable por las modificaciones hechas a las bases de datos, los envíos de correo electrónico, cualquier posible infección de virus y por consiguiente cualquier pérdida o daño de información hechos con su cuenta personal.

- La persona que sea sorprendida haciendo uso indebido del correo electrónico para emprender ataques a sitios externos será sancionada de acuerdo a las normas y leyes vigentes.

- La seguridad de la red estará a cargo de EPM, que utilizará los dispositivos necesarios para autorizar el acceso a la red, así como de los permisos a los servicios por cuenta (Web, Correo Electrónico, FTP, Firewall, telefonía IP), si hubiera lugar a ellos. Todo esto según los requerimientos de la Fundación EPM

5. Política para la realización de copias de respaldo (backups) de la información de la Fundación EPM.

- Cada empleado de la fundación EPM es responsable de mantener una copia de respaldo de su información sensible.

- La Fundación EPM proporcionará espacio de almacenamiento en un servidor para que cada área o proceso gestione sus propios respaldos. Dependiendo de la criticidad del proceso, se realizará diario, semanal o quincenalmente.

- La información de las bases de datos, aplicaciones y demás procesos locales que requieran copias de respaldo periódicas y sean administrados por el personal de la Fundación EPM, serán llevadas a cabo por el profesional o tecnólogo de servicios TI.

Las copias de respaldo de los aplicativos de computación alojados en la nube serán responsabilidad del proveedor del servicio Cloud Computing y realizados regularmente por éste, según las condiciones contractuales.

- Para efectos de una fácil ubicación y recuperación de la información, cada usuario debe crear una carpeta con su nombre en la partición “D” del equipo y será allí y sólo allí donde debe almacenar sus archivos (laborales y personales). El área de Servicios TI no se hace responsable por la pérdida de información que no se encuentre en esta ruta.

6. Políticas de seguridad en la nube (cloud) de la Fundación EPM.

- Para los servicios de software en la nube (SaaS, Software as a Service), el proveedor (CSP, Cloud Solutions Provider) será el responsable de actualizar y mejorar su software permitiendo a la Fundación EPM acceder a la última tecnología, según las condiciones contractuales

- También es deber del proveedor, la implementación de medidas de protección de datos y de seguridad de la información contenida en sus sistemas.

- El proveedor de servicios en la nube debe proporcionar información a la Fundación EPM sobre la arquitectura, la tecnología utilizada, las medidas de seguridad adoptadas y las funcionalidades disponibles.

- El proveedor de servicios en la nube debe garantizar que los controles de acceso y la autenticación de los usuarios se implementen teniendo en cuenta el cifrado de datos, según las condiciones contractuales.

- Se debe firmar entre las partes un Acuerdo de Nivel de Servicio (ANS) preciso que garantice la continuidad del servicio en mínimo un 99.5% y gestione oportuna y adecuadamente los incidentes que se presenten en la Fundación EPM. Además, considerar el recurso o compensación a los que tiene derecho la Fundación si el proveedor no proporciona el servicio como se pactó.

- La Fundación EPM podrá tener acceso a los *logs* (registro de eventos) del sistema *cloud* en el caso que lo requiera.

- Así los datos se encuentren fuera de las instalaciones de la Fundación EPM, y gestionados por el proveedor de servicios *cloud*, sigue siendo ésta responsable de la seguridad, integridad, disponibilidad y confidencialidad de la información.

- El proveedor de servicios en la nube debe tener una política de recuperación de datos en caso de desastres.

- La Fundación EPM debe asegurarse de poder recuperar la información almacenada en la nube en el caso de que cambie de proveedor de servicio para lo cual debe incluir cláusulas contractuales que permitan esto.

7. Política para definir qué tipo de información puede extraer el empleado cuando cesa actividades en la Fundación EPM.

- Como la información es el activo más importante de la Fundación EPM, ésta debe cumplir con los principios de disponibilidad, integridad y confidencialidad.

- Al ser confidencial significa que solo puede ser gestionada por quienes tengan la potestad para su administración.

- De acuerdo a ello, solo será permitido copiar de la Fundación aquella información que sirva de soporte a la persona para su defensa en caso de que sea abierta una investigación por algún ente del Estado.

8. Política para la administración de software.

- Solo está permitido instalar software de uso libre, después de que se validen las condiciones de acuerdo de licencia del mismo y autorización por parte de seguridad informática de EPM o software licenciado que haya pasado por la misma validación.

- Cuando un usuario en razón de sus actividades requiere la instalación de un software, diligencia el formato **FR_057_Solicitud instalación software** y envía al Área de Servicios TI, quienes evalúan su pertinencia y aprobación, siendo los únicos autorizados para su posterior instalación.
- Para ambos casos es necesario solicitar la instalación por medio de la aplicación Catálogo EPM por parte de servicios TI.

- El motivo de este procedimiento es que la mesa de servicios de TI de EPM valide la aplicación, haciendo un diagnóstico de seguridad para impedir instalar software malicioso o alguna otra amenaza que pueda poner en peligro la integridad de la red informática corporativa.

- Si el software es libre, la Fundación EPM debe facilitar para su validación el nombre del usuario que requiere la instalación, el nombre de las maquinas dónde se requiere, las fechas de uso del programa, el nombre del programa, así como la ruta de descarga.

- Si el software es licenciado, la Fundación EPM debe adjuntar, para su validación, el comprobante de licenciamiento y/o cesión de derechos de uso, nombre del usuario que requiere la instalación, el nombre de las maquinas dónde se requiere, las fechas de uso del programa, el nombre del programa, así como la ruta de descarga.

- Toda falla detectada o mensaje de error recibido por parte de los usuarios, debe ser reportada de inmediato al Área de Servicios TI para su atención y solución oportuna.

- Queda prohibido borrar o alterar archivos pertenecientes a los programas y sistema operativo, así como archivos de configuración del equipo.

- Para el caso de los sistemas de información, no administrados directamente por el Área de Servicios TI, el administrador titular debe informar por escrito los niveles de seguridad del aplicativo, al Área de Servicios TI con el fin de monitorear y garantizar dichos niveles., además será quien se encargue de velar por el correcto funcionamiento de la

aplicación, creación de usuarios responsables, gestión de las bases de datos, copias de respaldo, interacción con el proveedor del aplicativo, continuidad del servicio, correcta interoperabilidad entre módulos. Según las condiciones contractuales

- Las herramientas de software son suministradas exclusivamente por Servicios TI, el cual lleva el control del inventario de licencias de software por equipo.

9. Políticas de protección contra software malicioso (*malware*).

Entre los factores que mayor influencia tienen en la pérdida o daño de información, están los virus informáticos. A continuación se enuncian algunas recomendaciones básicas que pueden ayudar a minimizar su ocurrencia:

- Todos los sistemas sin las actualizaciones de seguridad requeridas o los sistemas infectados con cualquier tipo de malware deben ser desconectados de la red de la Fundación EPM.
- Cualquier usuario que sospeche de una infección por código malicioso, debe apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, llamar al soporte de servicios TI y evitar hacer intentos de eliminarlo.
- Solamente los administradores de sistemas deben enfrentar una infección por código malicioso del computador.
- Los usuarios no deben intentar eliminar el código malicioso, a menos que sigan instrucciones precisas de los administradores de la infraestructura de control de malware.
- Los usuarios seguirán las recomendaciones del área de TI sobre la prevención y manejo de virus u otras amenazas a los recursos informáticos.
- Los usuarios no deben transferir (subir y bajar) software desde y hacia sistemas que no se encuentran autorizados.

- Los usuarios no deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos de que el software haya sido examinado en busca de código malicioso y que haya sido aprobado por el Especialista en Seguridad Informática. Aunque su distribución sea gratuita, absténgase de instalar software no autorizado “bajado” de Internet.

- Antes de efectuar la operación de descompresión, todo software transferido desde sistemas externos a la Fundación EPM, debe ser analizado con un software de detección, eliminación y reparación de código malicioso aprobado. No abra correos electrónicos de remitentes desconocidos. No ejecute archivos adjuntos directamente desde su correo electrónico.

- Para reducir el riesgo de infección por virus todos los usuarios se abstendrán de abrir o enviar archivos extraños y posiblemente dañinos que sean recibidos en su buzón de correo electrónico (personal y corporativo), deberán notificar al personal de Servicios TI para su atención, prevención, corrección y registro.

- No ingrese en la WEB a sitios inapropiados relacionados con pornografía, juegos, drogas o hacking.

- Debe certificarse que todo el software, archivos o ejecutables, se encuentran libres de virus antes de ser enviados a una entidad externa a la Fundación EPM.

- Debe instalarse software de detección, eliminación y reparación de código malicioso a nivel de , servidores de la Intranet y en las estaciones de trabajo de los usuarios, que sean administrados por la Fundación EPM

- Antes de que cualquier archivo sea restaurado en un sistema de la Fundación EPM desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema de detección, eliminación y reparación de código malicioso actualizado.

- Los usuarios no deben intencionalmente escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar u obstaculizar el desempeño de cualquier sistema de la Fundación EPM o de cualquier entidad externa a ella.

- Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, sin la autorización previa del profesional de servicios TI de la Fundación EPM.

10. Política para la confidencialidad de la información institucional y trato con terceros.

- Se deben revisar con regularidad por parte del área jurídica los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la Fundación para la protección de la información.

- Todo contrato, convenio, pacto, alianza que se realice entre la Fundación EPM y un tercero, y que implique divulgar información exclusiva de la organización, debe contener un acuerdo de confidencialidad por parte del receptor.

- Los acuerdos con terceras partes que implican acceso, procesamiento, comunicación, servicios y gestión de la información o adición de productos, deben considerar todos los requisitos de confidencialidad.

11. Política para la navegación en Internet.

- Los privilegios del uso de Internet estarán limitados por la necesidad de acceso que tenga cada empleado de la Fundación EPM de acuerdo a los requerimientos del ejercicio de su labor.

- Es competencia del Proceso de Servicios TI restringir el acceso a sitios nocivos y servicios que no sean de utilidad para la Entidad y que demeriten la calidad y agilidad de la red.

- El acceso a Internet a través de la Fundación es un privilegio y todos los colaboradores deben cumplir las políticas de buen uso. La violación a estas políticas podría suponer acciones disciplinarias o legales.

- Los empleados también serán responsables de los daños causados por cualquier violación o infracción a estas políticas. Se requiere que todos los empleados reconozcan su confirmación y comprensión, y que aceptan cumplir las reglas.

- Se prohíbe utilizar Internet para realizar consultas a páginas con contenido pornográfico, violentas, ofensiva racial.

- Se prohíbe utilizar Internet para acceder a sitios que sintonizan estaciones de radio a excepción de aquellos procesos que por su labor requieren de dicho acceso. Estos son los encargados de consumir el mayor ancho de banda.

- No ingrese a páginas de dudosa procedencia. Verifique que las páginas que está consultando cuenten con mínimas medidas de seguridad (candado, certificados digitales, etc.)

- Evite descargar archivos de música o de video “bajados” de Internet o de dispositivos móviles como USB, CD y DVD, entre otros, cuando sean de dudosa procedencia o no tengan relación con el trabajo asignado

12. Políticas para el uso de correo electrónico institucional.

Recuerde que la comunicación por correo electrónico entre la Fundación EPM y sus usuarios internos o externos debe efectuarse mediante el uso del sistema homologado por la entidad. Toda información transmitida por este medio es considerada como propiedad de la Entidad.

- Las cuentas de usuario que se asignan a los empleados de la Fundación EPM, son únicamente para uso institucional.

- Es responsabilidad del proceso de servicios TI, la configuración de las cuentas de correo corporativo de cada usuario, en el respectivo cliente de administración de correo que se esté implementando.

- Todos los empleados serán responsables de la administración, seguridad, confidencialidad y respaldo de la información enviada y recibida, a través del correo electrónico. El proceso de servicios TI, es el responsable de dar a conocer los manuales y procedimientos, al igual que la capacitación a los empleados sobre el uso de los clientes de correo utilizados y como efectuar sus copias de respaldo periódicamente.

- El Oficial de Protección de Datos debe garantizar que todo el personal vinculado a la Fundación EPM conozca y aplique la **PR_033_Política Administrativa de Protección de Datos Personales**, pero son los empleados quienes son responsables de cuidar la información personal que se comparte por el correo electrónico a usuarios internos o externos de la Institución.

- La información de carácter personal contenida en las bases de datos es considerada como propiedad de la entidad; por este motivo está totalmente prohibido la transferencia o cesión de bases de datos que contenga información personal ya sea de los empleados o de la comunidad en general. Solo se podrá enviar información si se tienen las previsiones establecidas por la Institución como acuerdos de confidencialidad o autorizaciones.
- El contenido de los mensajes de correo se considera confidencial y solo perderá este carácter en casos de investigaciones administrativas, judiciales o incidentes relacionados con seguridad informática. (Con el debido tratamiento y cumplimiento en el marco de las leyes colombianas).

- Los empleados de la Fundación EPM no pueden emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Institución.
- Todos los mensajes de correo electrónico que envíen los empleados de la Fundación EPM deben contener los datos de firma que indique el área de comunicaciones de la Fundación EPM.
- Siempre que se envíen correos electrónicos que contengan cualquier tipo de información, en la firma institucional de cada empleado debe ir incluido el AVISO DE PRIVACIDAD, que se adopta como buena práctica en manejo de datos personales y bases de datos
- Los usuarios no pueden crear, enviar, o retransmitir mensajes de correo electrónico que puedan constituir acoso o que puedan contribuir a un ambiente de trabajo hostil.
- Toda información contenida en el correo electrónico es considerado información privada y debe ser manejado como una comunicación privada y directa y es por lo tanto es de uso exclusivo del entre el remitente y los destinatarios intencionales.
- La Fundación EPM debe notificar a todos los usuarios que los sistemas de correo electrónico solamente deben ser utilizados para propósitos de la entidad. Todos los mensajes enviados por este correo electrónico constituyen registros de la Fundación, quien se reserva el derecho de acceder y revelar cualquier mensaje para cualquier propósito sin previo aviso. Los Directores, previa autorización de la Dirección Ejecutiva, pueden solicitar revisar el correo electrónico institucional de los empleados para determinar si han roto la seguridad, violado los lineamientos de seguridad de la Fundación EPM o han realizado actividades no autorizadas.
- Los empleados de la Fundación EPM no pueden modificar, falsificar o eliminar cualquier información contenida en los mensajes de correo electrónico, incluyendo el cuerpo y los encabezados.

- Ningún empleado de la Fundación EPM puede utilizar comentarios obscenos, despectivos u ofensivos en contra de cualquier persona o entidad en mensajes de correo electrónico institucional.
- Los empleados de la Fundación EPM no pueden enviar o distribuir cualquier mensaje a través de los sistemas de las empresas del Grupo Empresarial EPM, el cual pueda ser considerado difamatorio, acosador o explícitamente sexual o que pueda ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religión, política o situación de discapacidad.
- Los empleados no deben utilizar los recursos informáticos de la Fundación EPM para la transmisión de cualquier correo masivo no autorizado.
- Los servidores de correo de la Fundación EPM deben estar atentos a todos los mensajes de correo electrónico entrantes, que puedan contener software malicioso y contenido ajeno a la entidad.
- En todos los mensajes de correo electrónico salientes, debe agregarse un pie de página preparado por el departamento jurídico que indique que “El contenido de este documento y/o sus anexos son para uso exclusivo de su destinatario intencional y puede contener Información legalmente protegida por ser privilegiada o confidencial. Si usted no es el destinatario intencional de este documento por favor Infórmenos de inmediato y elimine el documento y sus anexos. Igualmente, el uso indebido, revisión no autorizada, retención, distribución, divulgación, reenvío, copia, impresión o reproducción de este documento y/o sus anexos está estrictamente prohibido y sancionado legalmente”.
- Los empleados de la Fundación EPM no deben emplear versiones digitalizadas de sus firmas manuscritas en los mensajes de correo electrónico institucional.
- Los empleados no deben abrir archivos adjuntos a los correos electrónicos de remitentes desconocidos o de los que no se tenga confianza, a menos que hayan sido analizados por el software de detección, eliminación y reparación de código malicioso aprobado.

- Los empleados de la Fundación EPM no deben utilizar las cuentas de correo electrónico oficiales para participar en grupos de discusión en Internet, listas de correo o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada por el Jefe inmediato y/o el jefe de la oficina de comunicaciones.

- Se prohíbe leer la correspondencia de los demás empleados, en atención al derecho de privacidad e intimidad de las personas.

- La distribución de correos electrónicos se hará a máximo 50 destinatarios para evitar posibles congestiones en la red y que seamos marcados como generadores de SPAM.

  Cada empleado tendrá asignado un espacio para almacenamiento definido por el proceso de servicios TI.

13. Políticas de mensajería instantánea de la Fundación EPM.

- No está permitida la mensajería instantánea pública en la Fundación EPM, a menos que se cuente con la autorización respectiva.
- El uso de mensajería instantánea como medio de comunicación sólo podrá utilizarse entre colaboradores de la Fundación, previa autorización.

- No se debe utilizar la mensajería instantánea en conversaciones confidenciales o para transmitir información crítica o sensible de la Fundación EPM.
- El sistema de mensajería instantánea, así como el correo electrónico del trabajo, son propiedad de la Fundación EPM, por lo tanto la Fundación EPM se reserva el derecho de monitorear, hacer seguimiento o examinar archivos y comunicaciones electrónicas.

14. Políticas de atención de incidentes de seguridad de TI.

- Aquellos empleados que manejen activos de información, deben reportar todo incidente de seguridad, cualquier anomalía o mal uso de los recursos de la Fundación EPM.

- Todos los incidentes de seguridad de TI deben ser registrados, gestionados y documentados en sus diferentes etapas para mantener los ANS (Acuerdos de Nivel se Servicio) negociados con los clientes y mejorar la seguridad de TI.
- Todos los problemas de seguridad de TI se deben gestionar buscando su causa raíz, con el fin de minimizar la ocurrencia de incidentes.
- En caso de un proceso de investigación solo se suministrarán pruebas técnicas; la valoración de las mismas estará a cargo de la entidad competente responsable de la investigación y serán canalizadas a través de Auditoria Interna o el área competente.

15. Política para el uso adecuado de los dispositivos móviles conectados a la red Wi-Fi Móviles Grupo EPM.

- La decisión de permitir el uso de dispositivos móviles de propiedad de un empleado de la Fundación EPM para consumir servicios de TI será basada en una necesidad de negocio documentada y aprobada por el jefe del empleado.

- El número máximo de dispositivos que un empleado de la Fundación EPM puede tener con posibilidad de conectarse a la red Wi-Fi es de dos, por ejemplo: un teléfono inteligente y una tableta.

- El pago por servicios complementarios, tales como el costo de las aplicaciones móviles de terceros para su uso personal o laboral serán asumidos por el empleado. En caso de que se requiera algún tipo de aplicación que tenga costo, esta debe pasar por su respectivo proceso de compras y contratación.

- El dispositivo personal estará bajo administración y monitoreo de la Fundación EPM cuando el dispositivo sea conectado a la red corporativa.

- El empleado de la Fundación EPM entiende que es el único responsable de cualquier copia de respaldo de la información almacenada en el dispositivo.

- El empleado de la Fundación EPM acuerda instalar y mantener actualizado un antivirus personal, y en buenas condiciones de funcionamiento su dispositivo, mediante la protección contra amenazas que puedan ponerlo en peligro.

- El empleado es consciente de que la Fundación EPM no será responsable en ningún caso por daño, pérdida o robo de dispositivos personales mientras el colaborador esté realizando actividades laborales.

- El empleado acuerda que la Fundación EPM instale software de administración licenciado por EPM sobre su dispositivo.

- La Fundación EPM podrá restringir el uso de aplicaciones en el dispositivo del empleado que no cumpla con los requisitos de seguridad.

- Descargar aplicaciones de las tiendas Apple Store, Play Store en general, es aceptable, siempre y cuando esas aplicaciones no produzcan vulnerabilidades que vayan en contra de la confidencialidad, integridad, disponibilidad y autenticidad de la información.

- Los empleados de la Fundación EPM no pueden utilizar cuentas externas de correo electrónico para sincronizar información de la Fundación en su dispositivo móvil.

- Todos los datos de la Fundación EPM almacenados en los dispositivos móviles deben ser asegurados en todo momento usando los métodos físicos y electrónicos definidos por Fundación.

- La funcionalidad de fábrica del dispositivo no debe ser modificada a menos que sea requerido o recomendado por la Fundación EPM. El uso de dispositivos que son “jailbreak”, "rooting" o han sido sometidos a cualquier otro método de cambio de protección incorporada de fábrica en el dispositivo, no están permitidas y constituyen una violación a estas políticas.

- El empleado debe prevenir que otros obtengan acceso a su dispositivo móvil.

- Los colaboradores serán responsables de todas las transacciones realizadas con sus credenciales, es por ello que no deben compartir sus contraseñas.

- Un dispositivo móvil que presenta visualmente información sensible y es usado en un lugar público (por ejemplo, aeropuerto, avión o cafetería) debe ubicarse de manera tal que la pantalla no pueda ser vista por los demás.

16. Política para el uso de dispositivos de almacenamiento extraíbles.

Los empleados de la Fundación EPM no tienen habilitadas las funcionalidades para los puertos, dispositivos o unidades lectoras que permitan el almacenamiento de información en medios extraíbles.

17. Política para la adquisición y reposición de activos informáticos.

ADQUISICION DE ACTIVOS INFORMATICOS

- Las decisiones de inversión de capital en activos informáticos deben responder a análisis financieros y económicos que contemplen las diferentes alternativas de inversión, con el fin de garantizar que dichas decisiones contribuyan a optimizar los procesos para cuyo fin se adquieren.

- La obtención de nuevos activos informáticos debe orientarse al mejoramiento de los procesos de la Fundación y a la búsqueda del

bienestar social en las poblaciones con influencia de los programas y/o proyectos de la Fundación EPM.

- La adquisición de bienes y servicios informáticos se llevará a cabo a través del proceso de compras y contrataciones, para lo cual deberá cumplir con las disposiciones que rigen la materia , a saber:

- El cumplimiento de la Política de Adquisición de bienes y servicios.

  - El cumplimiento de las disposiciones señaladas por la Dirección Administrativa y financiera para pagos a proveedores.

  - Cumplir totalmente el trámite de adquisición de bienes que comprende: recibir, almacenar y entregar a los empleados los bienes informáticos.

  - En la adquisición de computadores, impresoras, servidores y dispositivos de comunicación, etc. Con el objetivo de maximizar la utilidad de la inversión, el proceso de servicios TI emitirá anualmente estándares de las especificaciones técnicas mínimas aceptables.

  - En la adquisición de computadores y servidores se deberá incluir el software necesario instalado con su licencia correspondiente debiéndose además solicitar los medios de instalación y configuración.

  - En la adquisición de impresoras deberán corroborarse la disponibilidad en el mercado local de sus suministros (cartuchos, tóner, cables, etc) y que su relación precio/rendimiento sea mayor, salvo casos excepcionales que se requiere calidad de impresión.

  - En la adquisición de equipos de cómputo, servidores y dispositivos de comunicación, el proceso de servicios TI, determinará los requerimientos mínimos y máximos necesarios para el cumplimiento de las funciones y labores para los que se necesita el equipo.

- Para la adquisición de otros elementos tecnológicos especializados, quien deberá dar la autorización es el responsable del programa o proyecto, servicios TI solo podrá asesorar en la compra, en los casos que le competa.

ACTUALIZACION Y/O REPOSICION DE ACTIVOS INFORMATICOS

Se realizará teniendo en cuenta el tiempo de funcionalidad el cual varía de acuerdo a las características del equipo, el tiempo de uso, las actividades para las cuales se hayan adquirido y las condiciones ambientales y de utilización donde estén o hayan operado o en los casos en que la reparación del equipo sea más costoso en términos del beneficio que la adquisición de uno nuevo. Es conocido que toda tecnología tiende a ser obsoleta a medida que pasa el tiempo, en la mayoría de los casos esta obsolescencia se da generalmente por la renovación tecnológica, la dificultad para conseguir repuestos y por los requerimientos y exigencias de las necesidades de los usuarios, se han establecido los siguientes parámetros para la actualización y/o reposición de activos informáticos

- **Obsolescencia en el hardware de las estaciones de trabajo (equipos de escritorio, portátiles e impresoras)**: Los equipos adquiridos por la Fundación EPM tendrán un período de obsolescencia no mayor a 5 años (60 periodos de depreciación), servicios TI apoyará con el concepto técnico para el reemplazo de estos equipos, los cuales serán remitidos al personal de activos para ser dados de baja del inventario de la Fundación EPM. Sin embargo, muchos elementos de hardware pueden seguir prestando servicio en aplicaciones complementarias, secundarias o como pruebas para nuevos proyectos y/o servicios; lo cual en este caso será detallado en dicho concepto.

- **Daño irreparable o que su reparación supere el costo del activo informático:** En los casos en que un activo informático tenga daños en el hardware, donde varios componentes del equipo estén afectados y/o el costo del arreglo supere el valor actual del activo, se podrá hacer reposición del mismo.

- **Pérdida o Hurto de los activos informáticos:** La reposición de un activo informático procederá en este caso después de agotarse la investigación pertinente y ser autorizada por el area pertinente de acuerdo con las directrices dadas en el Procedimiento de Administración de activos, además de contar con el respectivo presupuesto para proceder con el trámite de compra respectivo de acuerdo con la política de Adquisición de bienes y servicios
- **Renovación tecnológica propiedad de terceros**: De acuerdo con las políticas de renovación del tercero, se notificara del cumplimiento de la vida útil de los equipos para solicitar su actualización y/o reposición.

18. Políticas para el inventario de activos de software.

- Mantener un inventario preciso de software es esencial para optimizar los recursos de la Fundación EPM, así como minimizar los riesgos asociados con el incumplimiento del licenciamiento de las aplicaciones.

- El área de servicios TI será responsable de la ejecución del inventario de software de los equipos propios y de terceros, con una periodicidad semestral.

- El software instalado en cada equipo de cómputo propiedad de la Fundación EPM debe estar respaldado por la licencia correspondiente.

- El servicio CAL (Client Access License) que tiene la Fundación, si bien no es un software, es una licencia que le da al usuario el derecho a utilizar los servicios de un servidor, por lo tanto, debe estar registrada en el inventario.

- El área de TI es la responsable de asesorar en la adquisición, controlar y administrar de forma centralizada las licencias de software de la Fundación EPM.

- Siempre que se adquiera una licencia es responsabilidad de cada área, enviar la información correspondiente a la licencia al área de servicios TI para su control.

- Asimismo, es quien mantiene actualizada la CMDB (Configuration Management Database) del grupo EPM en la cual también reposa el inventario de software de la Fundación.

- Servicios de TI aprueban la instalación de software libre (*freeware*) cuando haya una justificación consistente, cumpla con los lineamientos de seguridad informática del Grupo EPM y éste se requiera para cumplir las labores o actividades propias del colaborador.

- Para los computadores que vienen con el sistema operativo licenciado por **OEM**, cómo éste solo es válido para ese equipo, el software será dado de baja cuando se dé de baja la máquina.

- Cuando se termina un contrato o se vencen las licencias de software, el número disponible de éstas debe actualizarse de manera oportuna para reflejar la información exacta de las existentes.

- Todo software que se encuentre en los computadores de la Fundación EPM y que no se haya autorizado su instalación, será retirado del equipo.

- Por ningún motivo se permitirá la instalación de software o licencias comerciales sin que éstas se encuentren debidamente legalizadas por la Fundación EPM.

- Al igual que los tangibles informáticos, la solución ERP proporciona a la Fundación EPM una visión centralizada del inventario de licencias de propiedad de la Fundación en un único escritorio.

- La baja de software se hará según lo estipulado en el procedimiento **PR-047 Procedimiento Para Dar De Baja Software.**

19. Política para el aseguramiento físico de activos informáticos.

- En la medida de lo posible, los activos informáticos se mantendrán a salvo utilizando guaya de seguridad de la que solo el responsable del activo conserva la clave.

- Aquellos activos que no se puedan asegurar con guayas, se propenderá para que cuando el responsable no pueda estar en su custodia, éste permanezca bajo llave para evitar su pérdida.

- De otra manera, se guardarán bajo llave en la bodega de la Fundación EPM, necesitando para su sustracción los debidos documentos diligenciados para su préstamo.

20. Política para el uso adecuado de los activos informáticos.

- El proceso de asignación de equipos de cómputo, periféricos, software y consumibles en materia informática deben llevar la aprobación del Área de servicios TI.

- Cada usuario recibirá de conformidad y con previa revisión; el equipo de cómputo y demás elementos que requiera para sus labores, los cuales se detallarán en el formato **FR-020 Cartera de Activos**, a partir de este momento asume la responsabilidad sobre los mismos.

- La persona a la que se le asigne el equipo de cómputo, también será la responsable del resguardo del software instalado en ese equipo. Cualquier modificación o instalación de software, que no se encuentre en dicho resguardo y que no sea autorizado previamente por el Área de Servicios TI, será responsabilidad de la persona firmante, y para ello el Área de Servicios TI ejerce el control del resguardo del software.

- Al firmar el resguardo del software, el usuario se hace responsable de respetar y hacer respetar los derechos de autor del software instalado en el equipo.

- El usuario deberá observar un uso adecuado del equipo de cómputo y los programas de software, queda prohibido abrir físicamente el equipo, así como golpearlos y, en general, causar daños por negligencia o de manera intencional, lo cual es sancionado según lo establecido por el Proceso Administrativo y disciplinario de la Fundación.

- Cada equipo contará con una identificación, diseñada por el Área de Servicios TI (un nombre de equipo y dirección IP).

- Cada usuario será responsable de apagar el equipo en que este trabajando (monitor, CPU, impresora) al terminar la jornada laboral.

- Cada usuario será responsable de revisar el correcto funcionamiento de sus equipos, si se detecta alguna falla o mal funcionamiento del equipo, debe reportarlo inmediatamente a Área de Servicios TI. La pérdida de información ocasionada por cualquier tipo de falla que llegara a presentarse en el equipo, no es responsabilidad del Área de Servicios TI.

- El usuario responsable del equipo de cómputo, deberá establecer una contraseña de acceso al equipo, con la finalidad de evitar el mal uso del mismo, así como de asegurar la confidencialidad de la información.

- Sólo está permitido retirar de los espacios de la Fundación EPM, los equipos portátiles y de comunicaciones que estén a cargo del empleado. Para los demás equipos tecnológicos, se debe solicitar al encargado de cada espacio la firma de la orden de salida respectiva.

- Está prohibido el uso de la sesión de la cuenta de usuario administrador de las maquinas por personal no autorizado. Esta será para uso exclusivo del área de Servicios TI.

- Toda adquisición de accesorios y refacciones de cómputo debe ser solicitada, validada y autorizada por el Área de Servicios TI.

- Toda donación y/o comodato de bienes y servicios informáticos debe ser notificada previamente vía oficio al Área de Servicios TI.

- En caso de que el equipo donado y/o en comodato cuente con las licencias tanto de paquetería como de sistema operativo, se deberá enviar una copia

de las mismas, así como de las facturas correspondientes, al Área de Servicios TI.

- Los bienes informáticos de la Fundación están destinados al desarrollo del objeto social de la entidad y a brindar un servicio a la comunidad.

- Su uso debe realizarse de forma concienzuda, velando por la preservación y conservación para que éstos puedan ser aprovechados por el mayor número de usuarios posibles.

- La custodia y correcto uso de los activos informáticos son responsabilidad de los empleados o contratistas de la Fundación EPM a quienes les fueron entregados para su custodia y uso en el desarrollo de sus funciones.

- En general, los computadores portátiles y de escritorio, solo deben tener un monitor de video.

  En los siguientes casos, se podrá tener más de un monitor de video: i) Usuarios diseñadores que requieran alta definición de imagen y monitores de gran tamaño, ii) Personas con disminución considerable de su agudeza visual, la cual deberá ser certificada por un médico de Salud Ocupacional; iii) Para monitoreo en salas de seguridad o centros de control.

- Los equipos de cómputo, sus accesorios, los dispositivos de impresión y los teléfonos no deben ser instalados ni trasladados (entre dependencias o sedes) por los usuarios; estas actividades sólo las puede hacer el personal autorizado por Servicios TI.

- Los usuarios no deberán tener más de un computador asignado a menos que sea autorizado explícitamente por TI, para lo cual debe darse una justificación adecuada.

  Los criterios para que un usuario sea autorizado para tener más de un computador son: i) Administra salas de capacitación; ii) Es interventor de contratistas y le cargan en cartera los equipos que éstos usan; iii) Administra una sede en donde hay equipos para uso de visitantes (Ej.

UVAS, Museo del Agua, Parque Deseos); iv) Es gestor técnico del contrato de Tecnología.

- Los equipos de las personas que se desvinculan de la Fundación EPM deben ser devueltos a TI; dichos equipos quedarán disponibles para atender otras necesidades.

21. Política para la devolución de activos informáticos por cese de actividades de los empleados.

- Los activos informáticos entregados a cada empleado deben ser devueltos a la Fundación una vez cese la actividad para la cual se destinaron o cuando se presente la desvinculación del colaborador.
- Cuando un empleado se desvincula de la Fundación debe hacer entrega a su jefe de la información que tiene en sus equipos.

- El área de servicios TI se debe ocupar de todos los servicios informáticos que el empleado tenga activos, entre ellos el bloqueo de la cuenta del usuario, desactivación de la cuenta de correo corporativo, archivos y carpetas corporativas, desactivación de Skype,

- El proceso de administración de activos se encarga de listar y recibir los activos que el empleado que se va a retirar tiene a su nombre.

- Una vez todo lo anterior se encuentre verificado, TI y Administración de activos expiden un paz y salvo el cual firman y trasladan al jefe del área donde laboraba el empleado El formato de paz y salvo expedido por la Fundación EPM para llevar a cabo este proceso es el **FR_086 Paz y salvo laboral**

22. Política para el borrado seguro de medios de almacenamiento de datos.

Para el borrado seguro de medios de almacenamiento de datos a dar de baja, recuperar o reintegrar, se procederá según el procedimiento **PR-048 Borrado**

seguro de medios de almacenamiento de datos y se dejará la respectiva constancia del procedimiento en acta de baja del activo.

23. Política de excepciones.

- Aquellos incidentes de seguridad que surjan y que no estén documentados en las políticas de seguridad generales se deberán incluir en esta política a modo de actualización

- De acuerdo a la naturaleza de su criticidad, se define con la Dirección Administrativa y Financiera si solamente se deja reporte del suceso o si se adiciona a las políticas permanentes de la Fundación EPM.

24. Manejo de vulnerabilidades críticas.

- Las actualizaciones de seguridad o parches que corrigen vulnerabilidades críticas en un sistema operativo, el navegador web, la suite de Office o cualquier otro programa, por insignificante que parezca, se deben instalar de forma inmediata.

25. Usos Inapropiados o inaceptables

- Dejar sesiones de trabajo abiertas.
- Utilizar los recursos de la Fundación EPM para llevar a cabo actividades diferentes a sus funciones.
- Utilizar los recursos de tal forma que se violen éstas u otras políticas o reglamentos institucionales. Distribuir datos e información confidencial de la Fundación sin autorización.
- Usar, alterar o acceder sin autorización a la información de los datos de otros usuarios.
- Leer la correspondencia electrónica ajena, a menos que este específicamente autorizado para hacerlo.

- Prestar o tener visibles en el puesto de trabajo las contraseñas de la cuenta de red, correo institucional y/o cualquier otra cuenta de acceso de los servicios informáticos de la Fundación EPM.
- Suplantar a otras personas, haciendo uso de una falsa identidad, utilizando cuentas de acceso ajenas a los servicios.
- Intentar violar los mecanismos de seguridad de la red, los controles, perjudicar el funcionamiento de la red, o saltarse las restricciones establecidas por el área de sistemas.
- Sacar o tomar prestados los equipos y recursos de la Fundación sin tener la debida autorización.
- Utilizar los recursos de la Fundación para llevar a cabo actividades fuera de la Ley.

SUPERVISIÓN DE LAS POLÍTICAS

La supervisión del cumplimiento de las políticas informáticas está a cargo del área de Servicios TI, éste a su vez está facultado para:

- Supervisar en cualquier momento el cumplimiento de estas políticas informáticas y de la normatividad vigente en materia de tecnologías de información y comunicaciones.

- Suspender el servicio de red a los usuarios que se les detecte uso inapropiado, hasta la aclaración del mismo, o de ser procedente la inhabilitación del servicio.

- Bloquear el servicio de red e Internet a los usuarios que se les detecte alguna infección por virus, que puedan afectar el funcionamiento e integridad de las redes de datos de la Fundación EPM, hasta que sean desinfectados totalmente.

- Emplear herramientas para monitorear la utilización de los recursos y detectar prácticas de uso inadecuadas de los mismos.

- Emplear el software necesario para evaluar y optimizar la seguridad de la red.

- Reportar a los procesos encargados el incumplimiento de las políticas.

- En el caso de las oficinas ubicadas por fuera de la oficina principal de la Fundación EPM y que cuenten con áreas de sistematización e informática, será responsabilidad del titular de la misma el cumplimiento de las normas vigentes en tecnologías de información y comunicaciones; además de las políticas establecidas en este documento y en su caso proponer las normas y/o políticas adicionales que se adecuen a las necesidades de la infraestructura contenida en la sede, en su efecto éstas deben ser documentadas y reportadas al Proceso de Servicios TI para su análisis, validación e inclusión en el presente documento. En caso de no haber un titular de sistematización o informática en dichas oficinas, será responsabilidad del Profesional del Proceso de Servicios TI, vigilar su cumplimiento. (Ej: Museo del Agua, Parque de los Deseos, UVAS).

VIOLACIÓN DE LAS POLÍTICAS

La infracción a las políticas informáticas de la Fundación EPM establecidas en este documento será notificado al Líder del Proceso al cual corresponda, con copia al Director (a) Administrativo (a) y Financiero (a), con el fin de que se tomen las medidas correctivas y apliquen las sanciones a que haya lugar.

Documentos Referenciados

FR_019_Requisición y Alistamiento puesto de trabajo
FR_20_Cartera de activos
FR_057_Solicitud instalación software
PR_047_Procedimiento para dar de baja Software
PR_048_Procedimiento para el borrado seguro de medios de almacenamiento de datos