Fundación epm	**POLÍTICA DE SEGURIDAD INFORMÁTICA**	Código **PL_019** Versión **03**
		Vigente desde 11/07/2018

	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.