MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

INTEGRA MULTISOLUTIONS S.A.S.

INTRODUCCIÓN

Con los avances en Internet y los desarrollos de la informática y las telecomunicaciones, la Seguridad Informática, se ha convertido en figura necesaria para la protección, mantenimiento, control de acceso, confidencialidad, integridad y disponibilidad de la información, tanto para su seguridad como para la seguridad en el soporte de las operaciones de las organizaciones.

Las Políticas de Seguridad Informática son las directrices de índole técnica y de organización que se llevan adelante respecto de un determinado sistema de computación a fin de proteger y resguardar su funcionamiento y la información en él contenida. El principio y final de toda red es el usuario, esto hace que las políticas de seguridad deban, principalmente, enfocarse a los usuarios, indican a las personas cómo actuar frente a los recursos informáticos de la Entidad.

Actualmente la Empresa INTEGRA MULTISOLUTIONS S.A.S cuenta con una plataforma tecnológica que almacena, procesa y transmite la información, incluye equipos de cómputo de usuario servidores, equipos de conectividad que se interconectan por medio de una red de datos interconectado a internet. Siendo la información un activo valioso para la empresa, se hace necesario no solo la implementación de herramientas de hardware y software de seguridad, sino involucrar al personal para proteger su integridad y confidencialidad.

Este compendio tiene como finalidad dar a conocer las PSI - Políticas de Seguridad Informática, que deben aplicar y acatar los empleados, contratistas y terceros de la Empresa INTEGRA MULTISOLUTIONS S.A.S, entendiendo como premisa que la responsabilidad por la seguridad de la información es de todos y cada uno.

1. OBJETIVO

Definir e implementar las políticas de seguridad informática que dan las pautas y rigen para la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general, sobre el ambiente tecnológico de la Empresa INTEGRA MULTISOLUTIONS S.A.S, para su interiorización, aplicación y verificación permanente.

2. ALCANCE

Las políticas de seguridad informática están orientadas a toda la información almacenada, procesada y transmitida en medios electrónicos, estas políticas deben ser conocidas y cumplidas tanto por funcionarios de planta como por los contratistas que apoyan la gestión y por los terceros o grupos de interés que utilicen la información generada y custodiada por la Empresa INTEGRA MULTISOLUTIONS S.A.S, y por quienes hagan uso de los servicios tecnológicos de la Entidad.

3. DEFINICIONES

Para los efectos del presente manual, se adoptarán las siguientes definiciones:

Acceso físico: La posibilidad de acceder físicamente a un computador o dispositivos, manipularlo tanto interna como externamente.

Acceso lógico: Ingresar al sistema operativo o aplicaciones de los equipos y operarlos, ya sea directamente, a través de la red de datos interna o de Internet.

Activos de Información: Toda aquella información que la Entidad considera importante o fundamental para sus procesos, puede ser ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, aplicaciones, software del sistema, etc.

Aplicaciones o aplicativos: Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares.

Cableado estructurado: Cableado de un edificio o una serie de edificios que permite interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes servicios que dependen del tendido de cables como datos, telefonía, control, etc.

Cifrado de datos: Proceso por el que una información legible se transforma mediante un algoritmo (llamado cifra) en información ilegible, llamada criptograma o secreto. Esta información ilegible se puede enviar a un destinatario con muchos menos riesgos de ser leída por terceras partes.

Configuración Lógica: conjunto de datos que determina el valor de algunas variables de un programa o de un sistema operativo, elegir entre distintas opciones con el fin de obtener un programa o sistema informático personalizado o para poder ejecutar dicho programa correctamente.

Copia de respaldo o backup: Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

Contenido: Todos los tipos de información o datos que se divulguen a través de los diferentes servicios informáticos, entre los que se encuentran: textos, imágenes, video, diseños, software, animaciones, etc.

Contraseñas: Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

Cuenta de acceso: Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para que pueda obtener seguridad, acceso al sistema, administración de recursos, etc.

Dispositivos/Periféricos: Aparatos auxiliares e independientes conectados al computador o la red.

Dominio: Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

Información confidencial: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.

Información/Documento electrónico: Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se pueden clasificar por su forma y formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, entre otros.

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos.

Mantenimiento lógico preventivo: Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.

Mantenimiento físico preventivo: Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas que debe realizarse sobre el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.

Medios de almacenamiento extraíble: Son aquellos soportes de almacenamiento diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, CompactFlash, Memory Stick).

Plataforma web: Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de Internet.

Recurso informático: Todos aquellos componentes de Hardware y programas (Software) que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Los recursos informáticos incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Red de datos: Es un conjunto de ordenadores que están conectados entre sí, y comparten recursos, información, y servicios.

Riesgo: Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.

Servicio informático: Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.

Servidor: Se entiende como el software que configura un PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red, pero también pueden acceder a él a través de la computadora donde está funcionando.

Sistema de información: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

Software antivirus: Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión de Internet, los nuevos navegadores y el uso de ingeniería social, los antivirus han evolucionado para detectar varios tipos de software fraudulento, también conocidos como malware.

Software de gestión: Son todos aquellos programas utilizados a nivel empresarial, que por su definición genera acción de emprender algo y por su aplicación persigue fines lucrativo y no lucrativo. También es un software que permite gestionar todos los procesos de un negocio o de una empresa en forma integrada. Por lo general está compuesto por modulo cruzado de los procesos del negocio.

Software malicioso: Es aquel que se ha diseñado específicamente para dañar un computador, este tipo de software realiza acciones maliciosas como instalar software sin el consentimiento del usuario o virus.

Tráfico de red: Es la cantidad de datos enviados y recibidos por los usuarios de la red.

UPS: Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

4. POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

4.1. Se destinará un área en la Enditad que servirá como centro de telecomunicaciones en el cual se ubicarán los sistemas de telecomunicaciones y servidores, debidamente protegidos con la infraestructura apropiada, de manera que se restrinja el acceso directo a usuarios no autorizados.

4.2. El centro de Telecomunicaciones deberá contar con sistema de protección contra incendios, control de temperatura (aire acondicionado) permanente a una temperatura no superior a 22 grados centígrados, así como sistema eléctrico de respaldo (UPS).

4.3. Seguir los estándares de protección eléctrica vigentes para minimizar el riesgo de daños físicos de los equipos de telecomunicaciones y servidores.

4.4. Las instalaciones eléctricas y de comunicaciones, estarán preferiblemente fijas o en su defecto resguardadas del paso de personas o materiales, y libres de cualquier interferencia eléctrica o magnética.

4.5. Contar por lo menos con dos extintores de incendio adecuado y cercano al centro de telecomunicaciones.

4.6. Los equipos que hacen parte de la infraestructura tecnológica de la Empresa INTEGRA MULTISOLUTIONS S.A.S, tales como servidores, estaciones de trabajo, centro de cableado, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

5. POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS

5.1. Gestión de la Información

5.1.1. Todo funcionario de planta o contratista que inicie labores en la Empresa INTEGRA MULTISOLUTIONS S.A.S, relacionadas con el uso de equipos de cómputo, software de gestión, aplicativos, plataformas web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir y respetar las directrices impartidas en el Manual de

Políticas de Seguridad Informática.

5.1.2. Los funcionarios que se desvinculen y los contratistas que culminen su vínculo contractual con la Empresa INTEGRA MULTISOLUTIONS S.A.S, deberán hacer: entrega formal de los equipos asignados, así como de la totalidad de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para expedición de paz y salvo y/o liquidación de contrato.

5.1.3. Toda la información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo, pertenece a la Empresa INTEGRA MULTISOLUTIONS S.A.S, por lo tanto, no se hará divulgación ni extracción de la misma sin previa autorización de las directivas de la Entidad.

5.1.4. No se realizará por parte de los funcionarios o contratistas copia no autorizada de información INTEGRA MULTISOLUTIONS S.A.S. El retiro de información electrónica perteneciente a la Empresa INTEGRA MULTISOLUTIONS S.A.S y clasificada como confidencial, se hará única y exclusivamente con la autorización del Directivo competente.

5.1.5. Ningún funcionario o contratista podrá visualizar, copiar, alterar o destruir información que no se encuentre bajo su custodia.

5.1.6. Todo contrato o convenio relacionado con servicios de tecnología y/o acceso a información, debe contener una obligación o cláusula donde el contratista o tercero acepte el conocimiento de las políticas de seguridad y acuerde mantener confidencialidad de la información con la suscripción de un acuerdo o compromiso de confidencialidad de la información, el cual se hará extensivo a todos sus colaboradores.

5.2. Hardware y Software:

5.2.1. La instalación y desinstalación de software, la configuración lógica, conexión a red, instalación y desinstalación de dispositivos, la manipulación interna y reubicación de equipos de cómputo y periféricos, será realizada únicamente por personal del área de TIC´S.

5.2.2. El espacio en disco duro de los equipos de cómputo pertenecientes a la Empresa INTEGRA MULTISOLUTIONS S.A.S será ocupado únicamente con información institucional, no se hará uso de ellos para almacenar información de tipo personal (documentos, imágenes, música, video).

5.2.3. Ningún funcionario o contratista podrá acceder a equipos de cómputo diferentes al suyo sin el consentimiento explícito de la persona responsable.

5.2.4. Ningún funcionario o contratista podrá interceptar datos informáticos en su origen, destino o en el interior de un sistema informático protegido o no con una medida de seguridad, sin autorización.

5.2.5. Ningún funcionario o contratista podrá impedir u obstaculizar el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, salvo el personal autorizado del área de TIC´S en aplicación de las políticas o medidas de seguridad.

5.2.6. No se permite el uso de la plataforma y servicios informáticos (equipos de cómputo, periféricos, dispositivos, internet, red de datos, correo electrónico institucional) de la Empresa INTEGRA MULTISOLUTIONS S.A.S, para actividades que no estén relacionadas con las labores propias de La Entidad.

5.2.7. Los funcionarios y contratistas serán responsables de contar con conocimientos actualizados en informática básica y el uso de herramientas ofimáticas.

5.3. Correo Electrónico:

5.3.1. El correo electrónico institucional es exclusivo para envío y recepción de mensajes de datos relacionados con las actividades de la Empresa información INTEGRA MULTISOLUTIONS S.A.S, no se hará uso de él para fines personales como registros en redes sociales, registros en sitios web con actividades particulares o comerciales o en general entablar comunicaciones en asuntos no relacionados con las funciones y actividades en la Entidad.

5.3.2. La información transmitida a través de las cuentas de correo electrónico institucional no se considera correspondencia privada, ya que estas tienen como fin primordial la transmisión de información relacionada con las actividades ordinarias de la Empresa INTEGRA MULTISOLUTIONS S.A.S.

5.3.3. Es prohibido utilizar el correo electrónico institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares, reenviar contenido y anexos que atenten contra la propiedad intelectual.

5.3.4. Es responsabilidad del funcionario o contratista depurar su cuenta de correo periódicamente, en todo caso se debe hacer copia de seguridad completa de los correos tanto recibidos como enviados.

5.4. Internet:

5.4.1. No se harán descargas de archivos por internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades en la Entidad.

5.4.2. El Servicio de internet de la Empresa INTEGRA MULTISOLUTIONS S.A.S no podrá ser usado para fines diferentes a los requeridos en el desarrollo de las actividades propias de la Entidad. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

5.4.3. No es permitido el uso de Internet para actividades ilegales o que atenten contra la ética y el buen nombre de la Empresa INTEGRA MULTISOLUTIONS S.A.S o de las personas.

5.4.4. La Empresa INTEGRA MULTISOLUTIONS S.A.S se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

5.5. Cuentas de Acceso:

5.5.1. Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles, cada funcionario y contratista es responsable por las cuentas de acceso asignadas y las transacciones que con ellas se realicen. Se permite su uso única y exclusivamente durante el tiempo que tenga vínculo laboral o contractual con la Empresa INTEGRA MULTISOLUTIONS S.A.S.

5.5.2. Las contraseñas de acceso deben poseer un mínimo de ocho (8) caracteres y debe contener al menos una letra mayúscula, una letra minúscula, un número y un carácter especial (+-*/@#$%&). No debe contener vocales tildadas, ni eñes, ni espacios.

5.5.3. La contraseña inicial de acceso a la red que le sea asignada debe ser cambiada la primera vez que acceda al sistema, además, debe ser cambiada mínimo cada 4 meses, o cuando se considere necesario debido a alguna vulnerabilidad en los criterios de seguridad.

5.5.4. Solamente puede solicitar cambio o restablecimiento de contraseña desde el servidor el funcionario o contratista al cual pertenece dicho usuario, o el jefe inmediato mediante solicitud motivada al correo electrónico del área de TIC´S.

5.5.5. Todo funcionario o contratista que se retire de la Entidad de forma definitiva o temporal (superior a 1 semana), deberá hacer entrega formal a quien lo reemplace en sus funciones o a su superior inmediato de las claves de acceso de las cuentas asignadas, con el fin de garantizar la continuidad de las operaciones a su cargo.

5.6. Seguridad Física:

5.6.1. Es responsabilidad de los funcionarios y contratistas velar por la conservación física de los equipos a ellos asignados, haciendo uso adecuado de ellos y en el caso de los equipos portátiles, estos podrán ser retirados de las instalaciones de la Entidad única y exclusivamente por el usuario a cargo y estrictamente para ejercer labores que estén relacionadas con la Empresa INTEGRA MULTISOLUTIONS S.A.S. En caso de daño, pérdida o robo, se establecerá su responsabilidad a través de los procedimientos definidos por la normatividad para tal fin.

5.6.2. Los funcionarios y contratistas deberán reportar de forma inmediata a los directivos la detección de riesgos reales o potenciales sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes, peligro de incendio, peligro de robo, entre otros. Así como reportar de algún problema o violación de la seguridad de la información, del cual fueren testigos.

5.6.3. Mientras se operan equipos de cómputo, no se deberá consumir alimentos ni ingerir bebidas.

5.6.4. Se debe evitar colocar objetos encima de los equipos de cómputo que obstruyan las salidas de ventilación del monitor o de la CPU.

5.7. Derechos de Autor:

5.7.1. Ningún usuario, debe descargar y/o utilizar información, archivos, imagen,

sonido, software u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos.

5.8. Uso de Unidades de Almacenamiento Extraíbles:

5.8.1. Los funcionarios y contratistas que tengan información de propiedad de la Empresa INTEGRA MULTISOLUTIONS S.A.S en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

5.8.2. Toda información que provenga de un archivo externo de la Entidad o que deba ser restaurado tiene que ser analizado con el antivirus institucional vigente.

5.9. Clasificación de la información:

5.9.1. Los documentos electrónicos resultantes de los procesos misionales y de apoyo de la Empresa INTEGRA MULTISOLUTIONS S.A.S, se tratarán conforme a los lineamientos y parámetros establecidos en el Sistema de Gestión Documental de la entidad. Los activos de información asociados a cada sistema de información serán identificados y clasificados por su tipo y uso siguiendo lo establecido en las tablas de retención documental vigentes.

5.10. Personal de Sistemas:

5.10.1. El control de los equipos tecnológicos deberá estar bajo la responsabilidad del área de TIC´S, así como la asignación de usuarios y la ubicación física.

5.10.2. En el área de TIC´S se deberá llevar un control total y sistematizado de los recursos tecnológicos tanto de hardware como de software.

5.10.3. El área de TIC´S será la encargada de velar por que se cumpla con la normatividad vigente sobre propiedad intelectual de soporte lógico (software).5.10.4. Las licencias de uso de software estarán bajo custodia del área de TIC´S. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas u otros medios) que acompañen a las versiones originales de software.

5.10.5. El área de TIC´S es la única dependencia autorizada para realizar copia de seguridad del software original, aplicando los respectivos controles. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.

5.10.6. Todas las publicaciones que se realicen en el sitio WEB de la entidad deberán atender el cumplimiento de las normas en materia de propiedad intelectual.

5.10.7. El acceso a los sistemas de información y red de datos será controlado por medio de nombres de usuario personales y contraseña. El área de TIC´S será la encargada de crear y asignar las cuentas de acceso y sus permisos a dominio de red, sistemas de información y correo electrónico, previo cumplimiento del procedimiento establecido para tal fin.

5.10.8. Se deben asignar usuarios unificados para todos y cada uno de los sistemas, servicios y aplicaciones, garantizando la estandarización por cada usuario; es decir, que cada usuario debe tener el mismo nombre de usuario para todos los sistemas y aplicaciones de la Entidad. La estandarización de los nombres de usuario estará compuesta de la siguiente forma: (Primer letra del primer nombre + punto (.) + primer apellido, en caso de existir duplicidad, Primeras dos letras del primer nombre + punto (.) + primer apellido).

5.10.9. Las cuentas de acceso a sistemas, servicios y aplicaciones no podrán ser eliminadas al retiro de los funcionarios o contratistas, debe aplicarse la inactivación del usuario.

5.10.10. Se realizará backup a la información institucional y bases de datos, conforme a lo establecido en la política de backup y cronograma, así como en los casos extraordinarios: desvinculación de funcionario o contratista, envío de equipo para garantía, mantenimiento correctivo de equipo.

5.10.11. Las contraseñas de los usuarios administradores de las plataformas tecnológicas y sistemas de información de la Entidad deberán ser salvaguardadas por el área de TIC´S en un archivo protegido a través de técnicas de cifrado de datos u otro mecanismo seguro.

5.10.12. La red interna de la Empresa INTEGRA MULTISOLUTIONS S.A.S deberá estar protegida de amenazas externas, a través de sistemas que permitan implementar reglas de control de tráfico desde y hacia la red.

5.10.13. Todos los equipos de la entidad deben tener instalado un antivirus, en funcionamiento, actualizado y debidamente licenciado.

5.10.14. Se realizará mantenimiento lógico preventivo a los equipos de cómputo mínimo cada 6 meses y mantenimiento físico preventivo mínimo una vez por año, que incluya el cableado estructurado. El área de TIC´S deberá elaborar el plan y

cronograma de mantenimientos, el cual será notificado a los usuarios, adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos e información.

5.11. Directivos:

5.11.1. La Entidad debe garantizar capacitación a los funcionarios en el manejo del software de gestión, plataformas y aplicativos implementados en la Empresa INTEGRA MULTISOLUTIONS S.A.S.

5.11.2. Deberá notificarse al área de TIC´S las novedades de vinculación y desvinculación de personal de la Empresa INTEGRA MULTISOLUTIONS S.A.S, con el fin de crear o cancelar, según sea el caso, los accesos a los sistemas de información, correo electrónico y red de datos.

6. POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

6.1. La seguridad en Internet comprende el conjunto de medidas destinadas a proteger la infraestructura tecnológica y la información que circula por la red, la cual suele ser el principal objetivo de actores maliciosos.
La seguridad informática, por su parte, desarrolla procedimientos, normas y mecanismos que permiten identificar y mitigar vulnerabilidades tanto en los datos como en los equipos —por ejemplo, computadores o servidores—.

El uso de soluciones antivirus confiables continúa siendo uno de los mecanismos más eficaces para prevenir incidentes.

- Principales riesgos en Internet
- Sustracción de información
- Alteración o pérdida de datos
- Ataques a sistemas o equipos
- Suplantación de identidad
- Comercialización indebida de datos personales
- Fraudes y robo de dinero

Como usuarios, es posible reducir la exposición a estos riesgos adoptando prácticas preventivas: mantener actualizados los antivirus en los dispositivos conectados a Internet, evitar operaciones financieras desde redes públicas o computadores compartidos, y revisar cuidadosamente los archivos adjuntos asociados a correos de origen desconocido antes de abrirlos o descargarlos. Recomendaciones para fortalecer la seguridad en Windows

Para incrementar la protección en equipos con Windows, es esencial conservar el sistema operativo y los programas actualizados, contar con un antivirus confiable y tener el firewall configurado de manera adecuada. A esto se suman medidas básicas como emplear contraseñas robustas y evitar abrir enlaces o archivos adjuntos sospechosos.

Recomendaciones puntuales:

- Mantener vigente el sistema operativo y las aplicaciones, pues las actualizaciones incluyen parches que corrigen fallos de seguridad.
- Usar un antivirus reconocido, con protección en tiempo real y actualizaciones frecuentes.
- Configurar el firewall para bloquear accesos no autorizados.
- Implementar contraseñas extensas, únicas y difíciles de predecir.
- Evitar abrir adjuntos o enlaces dudosos.
- Deshabilitar el acceso remoto si no es necesario.
- Minimizar efectos visuales que puedan afectar rendimiento y seguridad.
- Descargar únicamente software proveniente de fuentes verificadas.
- Realizar análisis periódicos de malware.
- Consultar las recomendaciones de “Protección de Windows”.

Recomendaciones para mejorar la seguridad en Mac

En los equipos macOS, la seguridad se refuerza mediante contraseñas sólidas, autenticación biométrica, actualizaciones constantes y el uso adecuado de las configuraciones de privacidad. El cifrado con FileVault, los respaldos regulares y la gestión responsable de accesos y permisos también son claves para reducir riesgos.

Guía detallada:

- Establecer contraseñas complejas y distintas para cada cuenta; un gestor de contraseñas puede ser útil.
- Activar Face ID o Touch ID para una autenticación más segura.
- Mantener el sistema y las aplicaciones al día.
- Configurar el firewall y emplear navegación privada cuando sea necesario.
- Proteger la información con FileVault.
- Realizar copias de seguridad frecuentes con Time Machine.
- Ser precavido frente a enlaces o adjuntos no verificados; utilizar antivirus si se considera pertinente.
- Administrar permisos de acceso a cámara, micrófono y localización.
- Activar la función “Buscar mi Mac”.
- Aplicar buenas prácticas en el uso del correo electrónico.
- Controlar el uso del dispositivo por parte de menores con las opciones de tiempo en pantalla.
- Evitar inicios de sesión automáticos.
- Limitar la instalación de aplicaciones a la App Store o a desarrolladores autorizados.
- Confirmar la legitimidad de las fuentes antes de instalar actualizaciones.
- Adoptar medidas de seguridad para servicios en la nube, incluidas contraseñas fuertes y controles adicionales de acceso.

7. POLÍTICA DE ADMINISTRACIÓN DE BACKUP

7.1. Objetivo:

Establecer las directrices para la ejecución y control de las copias de seguridad de la información digital perteneciente a la Empresa INTEGRA MULTISOLUTIONS S.A.S.

7.2. Alcance:

Estas directrices son aplicables a la información institucional, bases de datos y archivos de restauración de los equipos pertenecientes a la Empresa INTEGRA MULTISOLUTIONS S.A.S.

7.3. Clasificación de la Información:

Información Institucional:

Entiéndase como información institucional aquella relativa a las operaciones realizadas por cada una de las dependencias de la Empresa INTEGRA MULTISOLUTIONS S.A.S., su producción, almacenamiento y gestión está a cargo de cada uno de los funcionarios y contratistas. Información que se encuentra alojada en los equipos de cómputo.

Bases de Datos:

Las bases de datos son el conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso, la Empresa INTEGRA MULTISOLUTIONS S.A.S cuenta con la base de datos del software de gestión de usuarios RED GERENCIADA

Archivos de Restauración del Sistema:

Los archivos de restauración son la copia de las unidades necesarias para que se ejecute el Sistema Operativo, son la herramienta para recuperar el Sistema Operativo de un error grave o restaurar el equipo si la unidad de disco duro o el equipo dejan de funcionar.

7.4. Periodicidad del Backup

TIPO DE INFORMACIÓN	FRECUENCIA DE COPIA
Información Usuarios	Diaria
Bases de Datos	Diaria
Backup firmware Equipos Conectividad	Diaria

7.5. Medios de Almacenamiento

Las copias de seguridad son almacenadas en un Cloud en la nube asegurado por un correo exclusivo para tal fin y copia en un Disco Duro Extraíble dispuesto exclusivamente para este fin. Este debe ser resguardado por el responsable del área de TIC´S.

7.6. Tipos de Backup

Las copias de seguridad se realizarán bajo el método de backup completo y backup incremental.

Backup completo: se hace un respaldo completo de todos archivos del equipo. El backup abarca el 100% de los datos.

Backup incremental: se hace una copia de todos los archivos que han sido modificados desde que fue ejecutado el último backup completo.

8. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

El sitio web de la Empresa INTEGRA MULTISOLUTIONS S.A.S tiene como función principal proveer información y servicios, así como divulgar y promover normas y directrices que exige el Ministerio de Tecnologías de la Información y Comunicaciones a los Usuarios y público en general.

NTEGRA MULTISOLUTIONS S.A.S solicita al visitante y a usuarios de esta página que lea detalladamente la política de privacidad, tratamiento de datos y leyes a las que la empresa se compromete a cumplir tal cual lo exige el gobierno nacional.

El sitio Web de la empresa se publica bajo el dominio http://mastvproducciones.net.co/

La Empresa INTEGRA MULTISOLUTIONS S.A.S, los Jefes de Oficina, el área de TIC´S, Técnicos internos y de campo y todo el personal que se relacione de algún modo con la empresa, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas por parte de su equipo de trabajo.