TABLA DE CONTENIDO

2. OBJETIVO:

GENERAL

Determinar los lineamientos que permitan proteger la Información de la ESE Fabio Jaramillo Londoño a través de acciones de aseguramiento de la Información teniendo en cuenta los requisitos legales, operativos, tecnológicos, de seguridad y de la entidad alineados con el contexto de direccionamiento estratégico y de gestión del riesgo con el fin de asegurar el cumplimiento de la integridad, disponibilidad, legalidad y confidencialidad de la información.

3. ALCANCE:

El manual contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información en la ESE FJL. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por los funcionarios, contratistas y todos los terceros que tengan acceso, almacenen, procesen o trasmitan información de la institución o sus usuarios.

4. DEFINICIONES:

ACTIVOS DE INFORMACIÓN: Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Este tipo de activo representa los datos de la organización, información que tiene valor para los procesos, independientemente de su ubicación: puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil de la Institución.

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN: Instancia del nivel superior, que deben validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: Es toda actividad o procesos encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas que pueden ser de carácter administrativo, técnico o legal.

DISPONIBILIDAD: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un incidente de seguridad de la información se define como un acceso, uso, divulgación, modificación o destrucción no autorizada de la información y de sus usuarios; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política de Información.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado completo de los activos.

CLAVE: Contraseña, clave o password es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

CORREO ELECTRONICO INSTITUCIONAL: Es el servicio basado en el intercambio de información a través de la red y el cual es provisto por la ESE FJL, para los funcionarios, contratistas y practicantes autorizados para su acceso. El propósito principal es compartir información de forma rápida, sencilla y segura. El sistema de correo electrónico puede ser utilizado para el intercambio de información, administración de libreta de direcciones, manejo de contactos, administración de agenda y el envío y recepción de documentos, relacionados con las responsabilidades institucionales.

CUSTODIA DE LA INFORMACIÓN: es el encargado de la administración de seguridad de información. Dentro de sus responsabilidades se encuentra la gestión del Plan de Seguridad de Información así como la coordinación de esfuerzos entre el personal de sistemas y los responsables de las otras áreas de la Entidad, siendo estos últimos los responsables de la información que utilizan. Asimismo, es el responsable de promover la seguridad de información en todo el Instituto con el fin de incluirla en el planteamiento y ejecución de los objetivos institucionales.

DISPONIBILIDAD DE LA INFORMACIÓN: La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

INTERNET: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

INTRANET: Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.

MALWARE: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca

robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

MECANISMOS DE BLOQUEO: Son los mecanismos necesarios para impedir que los usuarios, tanto de los sistemas de información como de los servicios, tengan acceso a estos sin previa autorización, ya sea por razones de seguridad, falta de permisos, intentos malintencionados o solicitud de los propietarios de la información. Los bloqueos pueden ser temporales o definitivos dependiendo de tipo de situación presentada.

MEMORIA USB: La memoria USB (Universal Serial Bus) es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información.

MENSAJERÍA INSTANTÁNEA INSTITUCIONAL: Comúnmente conocido como "Chat", es un canal de comunicación provisto por La ESE FABIO JARAMILLO LONDOÑO para facilitar una forma de comunicación en tiempo real entre los funcionarios, contratistas y practicantes autorizados creando un espacio virtual de encuentro específico.

SGSI - SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN*:* Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Information Security Management System. En el contexto, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

SISTEMAS DE INFORMACIÓN: Un 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. Habitualmente el término se usa de manera errónea como sinónimo de sistema de información informático, en parte porque en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente hablando, un sistema de información no tiene por qué disponer de dichos recursos (aunque en la

práctica esto no suela ocurrir). Se podría decir entonces que los sistemas de información informáticos son una subclase o un subconjunto de los sistemas de información en general.

5. MARCO NORMATIVO O BASE LEGAL

Para la construcción de este manual se tiene como base, la norma ISO - lEC 27001: 2005 Sistema de Gestión de la Seguridad de la Información, el modelo de gestión de la seguridad de la información y la política de información de la E.S.E. FABIO JARAMILLO LONDOÑO.

6. POLÍTICA

La E.S.E. FABIO JARAMILLO LONDOÑO decide definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados con la misión, visión y funciones de la Institución.

La ESE FABIO JARAMILLO LONDOÑO, se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites del instituto, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas, practicantes y todo aquel que tenga interacción con esta información y la utilización físicamente o a través de equipos, plataformas o sistemas de información dispuestos para su gestión y resguardo.

Toda la información que es generada por los funcionarios, contratistas y practicantes de la E.S.E. FABIO JARAMILLO LONDOÑO en beneficio y desarrollo de las actividades propias de la Institución es propiedad de la E.S.E. FABIO JARAMILLO LONDOÑO, a menos que se acuerde lo contrario en los contratos escritos y autorizados. Esto también incluye la información que pueda ser adquirida o cedida a la Institución de parte de entidades o fuentes externas de información que sean contratadas o que tengan alguna relación con la Institución.

La ESE FABIO JARAMILLO LONDOÑO protege la información creada, procesada, transmitida o resguardada por los procesos de su competencia, su infraestructura tecnológica y activos, del riesgo que se genera con los accesos

otorgados a terceros (ej.: contratistas, proveedores o ciudadanos), o como resultado de servicios internos en outsourcing.

La ESE FABIO JARAMILLO LONDOÑO protege la información creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

La ESE FABIO JARAMILLO LONDOÑO protege su información de las amenazas originadas por parte de sus funcionarios, contratistas, practicantes y usuarios.

La ESE FABIO JARAMILLO LONDOÑO protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

La ESE FABIO JARAMILLO LONDOÑO controla la operación de sus procesos de operación garantizando la seguridad de los recursos tecnológicos, redes y bases de datos.

La ESE FABIO JARAMILLO LONDOÑO implementa control de acceso a la información, aplicativos, recursos de red, portales y sistemas de información internos y externos o con accesos remotos.

La ESE FABIO JARAMILLO LONDOÑO garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

La ESE FABIO JARAMILLO LONDOÑO garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

La ESE FABIO JARAMILLO LONDOÑO garantiza la disponibilidad de sus procesos de operación y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La ESE FABIO JARAMILLO LONDOÑO garantiza el cumplimiento de las obligaciones legales, regulatorias contractuales establecidas.

Las responsabilidades frente a la seguridad de la información del Instituto son definidas, compartidas, publicadas y deberán ser aceptadas por cada uno de los funcionarios, contratistas o practicantes del Instituto.

A este documento podrán integrarse en adelante lineamientos o políticas relativas a la seguridad de la información siempre y cuando no sea contrario a lo expresado en esta política.

6.1. RESPONSABILIDADES FRENTE A LA SEGURIDAD DE LA INFORMACIÓN Y AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

6.1.1. Responsabilidades oficina de tecnologías de la información

Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad de información y todos sus capítulos, el uso de los servicios tecnológicos en toda la institución de acuerdo a las mejores prácticas y lineamientos de la Dirección General del Instituto y directrices del Gobierno.

Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Institución.

Informar de los eventos que estén en contra de la seguridad de la información y de la infraestructura tecnológica de la Institución a la Dirección General, las diferentes Direcciones y Jefaturas de la ESE FABIO JARAMILLO LONDOÑO, así como a los entes de control e investigación que tienen injerencia sobre la Institución.

Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital del Instituto.

Aplicar y hacer cumplir la Política de Seguridad de la Información y sus componentes.

Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de la ESE FABIO JARAMILLO LONDOÑO.

Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Institución.

Resolver de común acuerdo con las áreas y los propietarios de la información los conflictos que se presenten por la propiedad de la información al interior del instituto. Esto incluye los posibles medios de acceso a la información, los datos derivados del procesamiento de la información a través de cualquier aplicación o sistema, los datos de entrada a las aplicaciones y los datos que son parte integral del apoyo de la solicitud.

Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Dirección General y las diferentes direcciones.

Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.

Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de los mismos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Direcciones, Jefaturas o Coordinaciones siguiendo el procedimiento establecido.

Establecer, mantener y divulgar las políticas y procedimientos de los servicios de tecnología, incluidos todos los capítulos que hacen parte de esta Política, en toda la institución de acuerdo a las mejores prácticas y directrices de la Entidad y del Gobierno.

Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.

Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la institución.

6.1.2. Responsabilidades de los propietarios de la información.

Son propietarios de la información cada uno de los directores, así como los jefes de las oficinas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades. Valorar y clasificar la información que está bajo su administración y/o generación.

Autorizar, restringir y delimitar a los demás usuarios de la institución el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes

funcionarios, contratistas o practicantes que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información. Determinar los tiempos de retención de la información en conjunto con él grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes. Determinar y evaluar de forma permanente los riesgos asociados a la información así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de la misma.

Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y practicantes en las diferentes dependencias del Instituto.

6.1.3. Responsabilidades de los funcionarios, contratistas y practicantes usuarios de la información.

Manejar la Información de la Institución y rendir cuentas por el uso y protección de tal información, mientras que este bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.

Proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido

Evitar la divulgación no autorizada o el uso indebido de la información.

Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.

Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.

Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.

Reportar los Incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique. Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos o técnico- científicos designados para el desarrollo de sus funciones. No está permitida la conexión de equipos de cómputo y de comunicaciones ajenos al instituto al a red Institucional ni el uso

de dispositivos de acceso externo a Internet o de difusión de señales de red que no hayan sido previamente autorizadas por la Oficina de Tecnologías de la Información.

Usar software autorizado que haya sido adquirido legalmente por la Institución. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de la Oficina de Tecnologías de la Información.

Divulgar, aplicar y el cumplir con la presente Política.

Aceptar y reconocer que en cualquier momento y sin previo aviso, la Dirección General del Instituto puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad del Instituto, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la Institución. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

Proteger y resguardar su información personal que no esté relacionada con sus funciones en la Institución. El HMI no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito.

7. LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACION.

7.1. LINEAMIENTO 1: USO DE CONTRASEÑAS Y USUARIOS

La asignación de usuarios y contraseñas es un permiso que la institución otorga a sus funcionarios, contratistas o practicantes con el fin de que tengan acceso a los recursos tecnológicos como a las plataformas y sistemas de información que permiten la operación, consulta y resguardo de la información institucional.

Los objetivos específicos de los lineamientos para el uso de usuarios y contraseñas son:

Presentar a todos los funcionarios y contratistas que son responsables de la asignación, creación y modificación de usuarios y contraseñas, las directrices a seguir y verificar que se cumplan a cabalidad con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de la institución. Concientizar a todos los funcionarios, contratistas o practicantes sobre los riesgos asociados con el uso de las credenciales de acceso (usuario y contraseña) y las consecuencias de exponer de manera inadecuada la identidad ante cualquier tercero, en el entendido que los usuarios y claves asignados a cada funcionarios, contratistas o practicantes son personales e intransferibles.

Asegurar el correcto manejo de la información privada de la institución.

La asignación de credenciales: usuarios (Login o Userld) y contraseñas (Clave o Password) a los diferentes funcionarios, contratistas o practicantes así como su desactivación de los sistemas se harán de acuerdo a los procedimientos establecidos y según sea solicitado por los directores, jefes de oficina o por el área de Talento Humano.

Las cuentas de usuario son entera responsabilidad del funcionario, contratista o practicante al que se le asigne. La cuenta es para uso personal e intransferible.

Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad y seguridad de la información, el acceso a dicha cuenta es suspendido temporalmente y es reactivada sólo después de haber tomado las medidas necesarias a consideración.

TIPOS DE CUENTAS DE USUARIO

Se definen dos tipos de cuentas:

a. **Cuenta de Usuario de Sistema de Información:**

Son todas aquellas cuentas que sean utilizadas por los usuarios para acceder a los diferentes sistemas de información.

Estas cuentas permiten el acceso para consulta, modificación, actualización o eliminación de información, y se encuentran reguladas por los roles de usuario de cada Sistema de Información en particular.

b. **Cuenta de Administración de Sistema de Información:**

Corresponde a la cuenta de usuario que permite al administrador del Sistema, plataforma tecnológica o base de datos realizar tareas específicas de usuario a nivel administrativo, como por ejemplo: agregar/modificar/eliminar cuentas de usuario del sistema. Usualmente estas cuentas están asignadas para su gestión por parte del Proceso De Tecnología e Información.

El Jefe de la oficina de Tecnología e Información deberá contar en un sobre cerrado y sellado con la lista de las contraseñas sensibles para la administración de los sistemas de información, plataformas tecnológicas y bases de datos. Esto resguardado bien sea en caja fuerte interna o en proveedor externo de custodia y protección de copias de seguridad.

Estas cuentas de usuario igualmente deben mantener las siguientes políticas:

1. Todas las contraseñas de usuarios administradores deben ser cambiadas al menos cada 3 meses.

2. Todas las contraseñas de usuario de sistema de información deben ser cambiadas al menos cada 3 meses.

3. Todas las contraseñas deben ser tratadas con carácter confidencial.

4. Las contraseñas de ninguna manera podrán ser transmitidas mediante servicios de mensajería electrónica instantánea ni vía telefónica.

5. Se evitará mencionar y en la medida de lo posible, teclear las contraseñas en frente de otros.

6. Se evitará el revelar contraseñas en cuestionarios, reportes o formularios.

7. Se evitará el utilizar la misma contraseña para acceso a los sistemas operativos y/o a las bases de datos u otras aplicaciones.

8. Se evitará el activar o hacer uso de la utilidad de recordar clave o recordar Password de las aplicaciones.

Uso apropiado de usuarios y contraseñas:

Usar las credenciales de acceso sobre los sistemas otorgados exclusivamente para fines laborales y cuando sea necesario en cumplimiento de las funciones asignadas.

Monitoreo

Los administradores de los sistemas de información, bases de datos y plataformas tecnológicas pueden efectuar una revisión periódica de los accesos exitosos y no exitosos y al número de intentos efectuados a dichos sistemas para determinar posibles accesos indebidos o no autorizados.

La Oficina de Sistemas revisar las bitácoras y registros de control de los usuarios que puedan afectar la operación de cualquier sistema o plataforma.

7.2. LINEAMIENTO 2: USO DEL SERVICIO DE CORREO ELECTRÓNICO INSTITUCIONAL

El correo electrónico es un servicio basado en el intercambio de información a través de la red y el cual es provisto por la ESE FABIO JARAMILLO LONDOÑO para los funcionarios, contratistas, practicantes previamente autorizados para su acceso.

Los objetivos específicos de los lineamientos para el uso del correo electrónico son:

1. Incentivar el uso del servicio de correo electrónico para fines estrictamente laborales de la ESE FABIO JARAMILLO LONDOÑO.

2. Asegurar el correcto manejo de la información privada de la institución por parte de los funcionarios, contratistas o practicantes.

3. Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información a través de este servicio.

El acceso al servicio de correo electrónico es un privilegio otorgado por la ESE FABIO JARAMILLO LONDOÑO a sus funcionarios, contratistas y practicantes y el mismo sobrelleva responsabilidades y compromisos para su uso.

La ESE FABIO JARAMILLO LONDOÑO a criterio propio puede otorgar el acceso a los servicios de correo electrónico para la realización de actividades institucionales al personal de planta, contratistas y proveedores. El acceso incluye la preparación, transmisión, recepción y almacenamiento de mensajes de correo electrónico y sus adjuntos. Los jefes de área tienen la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio.

TIPOS DE CUENTAS DE CORREO ELECTRÓNICO

Todas las cuentas de correo electrónico que existen son propiedad de la Institución. Se consideran los siguientes tipos de cuenta de correo:

a. Cuentas personales:

Cualquier funcionario, contratista o practicante del Instituto puede ser autorizado a obtener y operar una cuenta de correo institucional para el uso diario de sus actividades laborales.

El nombre de dicha cuenta de correo se creará con el formato XYZ@esefjl.gov.co, donde la X corresponde al primer nombre, Y corresponde al primer apellido si dos o más personas tienen el mismo identificador de usuario se añadirá a la segunda persona y siguientes el segundo apellido Z.

Los conflictos no aclarados por las reglas anteriores serán resueltos a criterio propio, por el administrador del sistema de correo, o por la persona que solicita la cuenta.

En caso de combinaciones que deriven en palabras malsonantes podrá solicitarse el cambio de identificador de usuario.

b. Cuentas de dependencias o de grupos de trabajo:

Estas cuentas son creadas para las necesidades de comunicación oficial, dependencias, Direcciones, Grupos de trabajo, etc. Deben ser solicitadas directamente por el jefe del área que corresponda, a través de los medios ya establecidos de la institución asignando a su vez el responsable de manejo de la misma. El nombre de la cuenta de correo se definirá con el nombre del área o proceso así: proceso@esefjl.gov.co. El titular de la entidad será responsable del uso que se dé a dicha cuenta y del mantenimiento periódico de las claves de la misma.

Todo mensaje de correo electrónico que salga de una cuenta de Grupo de Trabajo debe llevar por regla general la siguiente estructura de firma, es responsabilidad del usuario su administración su configuración y/o inclusión.

Esta información debe ir en fondo blanco, letra color negro, negrilla, el tipo de letra es Arial y el tamaño es 10. Nombre del grupo.

Área o dependencia a la cual pertenece Correo Electrónico Institucional

Tel: (57(indicativo Ciudad) XXXXXX Ext: XXXX Ciudad, Colombia.

www.esefjl.gov.co

Ejemplo:

Grupo de Talento Humano Secretaría General talentohumano@esefjl.gov.co

c. Cuentas temporales:

Estas cuentas son creadas en forma temporal, con una vigencia definida previamente, con propósitos específicos de comunicación derivados de contratos temporales o provisionales. Estas cuentas tendrán una fecha de caducidad y se desactivarán automáticamente a su término, a menos que se solicite lo contrario. Se abrirán con una vigencia no mayor de 3 meses y podrán renovarse por periodos máximos similares.

Adicionalmente, será incluido de manera automática por el sistema, el lago vigente de la institución y la referencia al compromiso ambiental del Instituto, a criterio de la Dependencia encargada.

Todo correo electrónico que sea enviado fuera de la ESE FJL, a través de este servicio de correo, contendrá la siguiente clausula al pie de página del mensaje del mismo:

"Este correo electrónico y cualquier archivo(s) adjunto al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario(s). Si usted no es el destinatario indicado, queda notificado que la lectura, utilización, divulgación y/o copia sin autorización está prohibida en virtud de la legislación vigente. En el caso de haber recibido este correo electrónico por error, agradecemos informarnos inmediatamente de esta situación mediante el reenvío a la dirección electrónica del remitente. Las opiniones que contenga este mensaje son exclusivas de su autor y no necesariamente representan la opinión oficial de la Institución."

Uso apropiado de los servicios de correo electrónico Institucional

Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas y practicantes con acceso a este servicio.

Usar el correo electrónico Institucional exclusivamente para fines laborales: para la difusión o el envío de circulares, memorandos, oficios y archivos de trabajo, cuando sea necesario en cumplimiento de las funciones asignadas.

Redactar los contenidos de un mensaje de correo electrónico de tal manera que sea serio, claro, conciso, cortés y respetuoso.

Cada funcionario, contratista o practicante tendrá un usuario y una clave asignada por el Área de Sistemas través de los procedimientos establecidos.

Uso indebido del servicio de correo electrónico Institucional

1. Participar en la difusión de "cartas en cadenas", en esquemas piramidales o de propagandas dentro y fuera de la institución.

2. Realizar intentos no autorizados para acceder a otra cuenta de correo electrónico Institucional.

3. Revelar o publicar cualquier información clasificada o reservada.

4. Descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.

5. Copiar ilegalmente o reenviar mensajes que hayan sido restringidos por parte del usuario o el emisor.

6. Descargar cualquier software o archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

7. Utilizar expresiones difamatorias o groseras en contra de individuos, clientes o entidades públicas o privadas. Los mensajes enviados a través de este servicio no pueden contener material insidioso, ofensivo, obsceno, vulgar, racista, pornográfico, subversivo u otro material no formal.

8. Enviar correos SPAM de cualquier índole.

9. Usar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales

10. Utilizar el correo electrónico para propósitos comerciales ajenos a la Institución.

11. Intentar o modificar los sistemas y parámetros de la seguridad de los sistemas de la red de la ESE FABIO JARAMILLO LONDOÑO.

12. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor
13. Usar correos públicos para la recepción, envío o distribución de información pública clasificada o reservada propia de la ESE FABIO JARAMILLO LONDOÑO.

14. Configurar y conectar los clientes de correo electrónico con los sitios de redes sociales o con fuentes RSS que no sean autorizadas.

15. Envío y transferencia sobre el servicio de correo electrónico.

16. Una vez superada la cuota asignada por usuario los mensajes no pueden ser descargados a sus buzones locales hasta no liberar el espacio necesario del servidor de correo. Se notifica a cada usuario con un mensaje cuando esté próximo a completar esta cuota.

Es una buena práctica comprimir los archivos a enviar a través de este servicio, para disminuir las exigencias técnicas en su transmisión.

Responsabilidades de los funcionarios, contratistas y practicantes que sean usuarios de los servicios de correo electrónico Institucional.

1. Cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de la Política de la Institución.

2. Usar correctamente las credenciales de ingreso (usuario y clave) asignadas. La cuenta de correo que proporciona la Entidad es personal e intransferible, por lo que no debe compartirse con otras personas.

3. Dar aviso al área de Sistemas, a través de los medios establecidos, de cualquier fallo de seguridad en su cuenta de correo, incluyendo su uso no autorizado, pérdida de la contraseña, suplantación, etc.

4. Responsabilizarse por la información o contenido que sea transmitido a través de la cuenta de correo asignada; Los usuarios del servicio deben considerar que los mensajes enviados a un destinatario pueden ser re-

enviados a cualquier número de cuentas de correo de otros individuos o grupos.

5. Descargar, verificar y resguardar la información recibida a través de este servicio en su buzón local de correo electrónico, de ser este configurado, en el cliente de correo instalado en su equipo de cómputo.

Monitoreo

La ESE FABIO JARAMILLO LONDOÑO tiene el derecho a acceder y revelar los contenidos electrónicos de los correos institucionales de sus funcionarios, contratistas y practicantes y estos deben dar su consentimiento a la ESE FJL en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.

El área de sistemas puede monitorear el cumplimiento de las directrices institucionales en el momento que así lo considere o le sea requerido, con las autorizaciones pertinentes para asegurar la integridad y confidencialidad del sistema.

7.3. LINEAMIENTO 3: USO DEL SERVICIO DE INTERNET

Los objetivos específicos del uso de servicio de internet son:

1. Incentivar el uso del servicio de Internet/Intranet para fines estrictamente laborales de la ESE FABIO JARAMILLO LONDOÑO.

2. Asegurar el correcto manejo de la información privada de la Institución.

3. Garantizar la confidencialidad, la privacidad y de uso adecuado y moderado de la información a través de este servicio.

El servicio de Internet es un servicio de gran importancia en el mundo laboral, de conocimiento y negocios basado en el acceso a diferentes fuentes de información en distintas ubicaciones a través de sistemas de cómputo interconectados en red a nivel local y mundial.

El acceso al servicio de Internet es un permiso otorgada por la ESE FJL a sus funcionarios, contratistas o practicantes y así mismo sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios de este servicio conserven normas de buen uso, confidencialidad y criterio ético.

Cada Jefe o Coordinador de área tiene la autonomía de otorgar y solicitar el acceso de sus funcionarios, contratistas o practicantes a este servicio, de acuerdo al procedimiento vigente.

El ingreso a este servicio se realiza por medio de la plataforma que el instituto destina, que para este caso es el navegador de internet instalado en cada máquina.

El punto de inicio para acceder a este servicio se hace desde la página web institucional a través de la dirección:

www.esefjl.gov.co

Uso apropiado del servicio de Internet

Todos los funcionarios, contratistas y practicantes con autorización al uso y acceso a estos servicios deben: Utilizar este servicio exclusivamente para fines laborales.

Conservar normas de respeto, confidencialidad y criterio ético por parte de todos los funcionarios, contratistas o practicantes con acceso a este servicio.

Descargar documentos o archivo tomando las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

Uso indebido del servicio de Internet

1. Acceder a sitios de juegos o apuestas en línea.

2. Acceder a sitios de divulgación, descarga o distribución de películas, videos, música, webcams, emisoras online, etc.

3. Acceder y/o descargar material pornográfico u ofensivo.

4. Utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por el área de sistemas.

5. Compartir en sitios web información institucional clasificada como reservada o clasificada sus usuarios, funcionarios, contratistas o practicantes.

6. Emplear este servicio para la recepción, envío o distribución de información pública clasificada o reservada del HMI a través de servicios y cuentas de correo públicos.

7. Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.
8. Cargar, descargar, enviar, imprimir o copiar archivos, software o contenidos en contra de las leyes de derecho de autor.

9. Utilizar el servicio de Internet para propósitos comerciales ajenos a la Entidad.

10. Intentar o modificar las opciones de configuración y/o parámetros de seguridad de los navegadores instalados.

11. Comprar o vender artículos personales a través de sitios web o de subastas en línea.

12. Acceder a sitios de contenido multimedia (videos, música, emisoras online, etc.) debido al alto consumo de canal de comunicaciones. Únicamente se autorizara el acceso a aquellos funcionarios, contratistas o practicantes que por sus actividades requieran monitorear estos sitios externos y tengan previa aprobación del Jefe Inmediato y la autorización del coordinador de sistemas

13. Publicar o enviar opiniones personales, declaraciones políticas y asuntos no propios de la Entidad, dirigidos a funcionarios, contratistas o practicantes y público en general, del sector oficial, de otras compañías y organizaciones, a través de este servicio.

14. Descargar, instalar y configurar navegadores distintos a los permitidos por el área de sistemas. Responsabilidades de los Usuarios de Internet:

a. Conocer, adoptar y acatar esta política cada vez que haga uso de este servicio.

b. Proteger los derechos de autor de la información obtenida a través de este servicio. Se recomienda citar la fuente (página web) en los documentos o informes generados con información obtenida por este medio.

Monitoreo:

Los funcionarios, contratistas y practicantes deben estar al tanto que se registra por cada usuario las visitas a los diferentes sitios y se registra estos eventos en archivos de auditoría tanto en los computadoras, propias o contratadas, como en los servidores donde se administran estos servicios.

1. El área de sistemas planifica periódicamente una revisión de los archivos de auditoría, las configuraciones y registros de cada una de las máquinas y navegación en Internet.

2. Si se determina que alguna de las páginas previamente restringidas por el Grupo área de sistemas es requerida para el desempeño de funciones de algún funcionario, contratista o practicante esta será habilitada únicamente con el consentimiento y solicitud de su jefe directo y con el visto bueno del coordinador de sistemas.

3. Los usuarios del servicio deben considerar que algunos sitios web no son seguros, especialmente los que hacen suplantación de entidades a los bancos y/o emisores de tarjetas de crédito (PH ISING) por lo que se recomienda confirmar esta información directamente con las mismas entidades. Igualmente no se debe proveer información personal ni laboral a sitios de dudosa validez. La ESE FJL no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al acceder a sitios de suplantación o al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito al hacer el uso de este servicio.

7.4. LINEAMIENTO 4: USO DEL SERVICIO MENSAJERÍA INSTANTÁNEA

El acceso al servicio de mensajería instantánea es un permiso otorgada por la ESE FABIO JARAMILLO LONDOÑO a sus funcionarios, contratistas o practicantes y la misma sobrelleva responsabilidades y compromisos para su uso. Se espera que los usuarios conserven normas de buen uso, confidencialidad y criterio ético.

Los objetivos específicos del uso de servicio de mensajería instantánea son:

1. Incentivar el uso del servicio de mensajería instantánea para fines estrictamente laborales.

2. Asegurar el correcto manejo de la información privada de los usuarios y de la institución

3. Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado del mismo.

Este servicio es suministrado para los funcionarios, contratistas y practicantes, previamente autorizados para su uso, con el propósito de agilizar la comunicación.

1. Uso apropiado del servicio de Mensajería Instantánea

2. Usar el servicio de mensajería instantánea institucional exclusivamente para fines laborales.

3. Transferir archivos que no tengan información sensible o reservada. Se debe revisar previamente que cualquier archivo a enviar esté libre de virus.

4. Abstenerse de compartir información o datos personales a través de este servicio. No es aconsejable incluir información personal como contraseñas o números de tarjetas de crédito, cuentas bancarias e incluso un número de teléfono en cierta manera confidencial.

5. Compartir por medio de este canal mensajes concisos, breves y veraces.

6. Mantener su estado actualizado en el sistema de modo que los demás usuarios sepan si están o no disponibles y si pueden o no contactarle.

Uso indebido del servicio de mensajería instantánea:

1. Emplear el servicio de mensajería instantánea Institucional para extensas conversaciones personales.

2. Expresar opiniones difamatorias, ofensivas, obscenas, vulgar, racistas, calumniadoras y sexuales sobre superiores, compañeros o subalternos. Esto puede comprometer la reputación y su credibilidad tanto de índole personal como institucional.

3. Emplear las comunicaciones instantáneas con fines políticos, religiosos o comerciales.

4. Realizar cualquier tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.

5. Compartir por medio de este canal información clasificada o reservada de la ESE FJL, de sus funcionarios, contratistas o practicantes

6. Realizar intentos no autorizados para acceder a otra cuenta de usuario de este servicio.

7. Compartir documentos o archivos que sean ajenos a la operación de la institución.

8. Descargar, instalar y emplear sistemas de mensajería instantánea distintos al definido por la ESE FABIO JARAMILLO LONDOÑO y administrado por el área de sistemas.

9. El uso inapropiado o el abuso en el servicio de mensajería instantánea ocasionaran la desactivación temporal o permanente de las cuentas.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios del servicio de mensajería instantánea:

Conocer, adoptar y acatar este lineamiento cada vez que haga uso de este servicio.

Usar correctamente sus credenciales de ingreso (usuario y clave). La cuenta de acceso es personal e intransferible todos los mensajes compartidos y documentos archivos compartidos o descargados quedan bajo responsabilidad del dueño de la cuenta.

Cada jefe de área es responsable de revisar y autorizar o desautorizar cada requerimiento de acceso de sus funcionarios, contratistas o practicantes a este servicio. Solicitudes aprobadas de acceso deben ser sometidas de acuerdo con el procedimiento vigente para este caso.

Los usuarios del servicio deben considerar que los mensajes instantáneos pueden ser guardados por su interlocutor. Una de las partes que participa en la conversación puede copiar y pegar la conversación entera en un documento de texto.

7.5. LINEAMIENTO 5: USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

El uso de medios de almacenamiento externo disponibles en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la entidad, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, contratistas o practicantes de la Institución que a la vez puede exponer información confidencial y sensible de la entidad a diversos riesgos y peligros.

Los objetivos específicos del uso de dispositivos de almacenamiento externo son:

1. Concientizar a los funcionarios, contratistas o practicantes de la Entidad sobre los riesgos asociados con el uso de los medios de almacenamiento, tanto para los sistemas de información como para la infraestructura tecnológica de la Entidad.

2. Asegurar el correcto manejo de la información digital que reposa en la institución.

3. Delimitar el uso de estos medios de almacenamiento en las diferentes áreas.

La ESE FABIO JARAMILLO LONDOÑO es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón la ESE FABIO JARAMILLO LONDOÑO define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para asegurarse de que la información propietaria, adquirida o puesta en custodia en la entidad no está supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

El uso de dispositivos de almacenamiento externo está permitido en el HMI para los funcionarios, contratistas y practicantes; en general, con el fin de facilitar el compartir y transportar información que no sea de carácter clasificado ni reservado de la Institución dentro de las normas y responsabilidades del manejo de información institucional.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria USB, por medio de un cable de datos,

mediante una conexión inalámbrica directa a cualquier equipo de cómputo de la ESE FABIO JARAMILLO LONDOÑO. Entre estos, se pueden encontrar:

- Memorias Flash USB.
- Reproductores portátiles MP3/MP4.
- Cámaras con conexión USB.
- Phones/Smartphones.
- SD Cards/ Mini SD Cards/ Micro SD Cards.
- PDAS / Tablets.
- Dispositivos con tecnología Bluetooth.
- Tarjetas Compact Flash.
- Discos duros de uso externo.

Uso indebido de dispositivos de almacenamiento externo:

1. Almacenar o transportar información clasificada o reservada de la ESE FABIO JARAMILLO LONDOÑO.

2. Ejecutar cualquier tipo de programa no autorizado desde cualquiera de las unidades de almacenamiento en mención.

3. Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.

4. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.

5. Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, contratistas o practicantes.

Responsabilidades de los usuarios de dispositivos de almacenamiento externo:

Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.

Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Institución por medio del software de protección dispuesto para tal fin.

7.6. LINEAMIENTO 6: USO DE DISPOSITIVOS DE CAPTURA DE IMÁGENES Y/O GRABACIÓN DE VIDEO

Los objetivos específicos del uso de dispositivos de captura de imágenes y/o grabación de video son: Concientizar a los funcionarios, contratistas, practicantes y demás personas vinculadas con la ESE FABIO JARAMILLO LONDOÑO sobre los riesgos asociados al uso de dispositivos de registros de imagen y/o video, en sus instalaciones.

Fortalecer las medidas de seguridad en las áreas que gestionan documentos e información institucional.

Dar cumplimiento a las directrices determinadas en la Política de Seguridad de la Información de la institución. Restringir el uso de este tipo de dispositivos en áreas de manejo de información y documentación clasificada o reservada.

Entre los dispositivos de captura de imágenes y/o grabación de video se pueden encontrar.

Cámaras Fotográficas Videocámaras Celulares.
IPhones/Smarthphones PDAS/Tablets. WebCams Scanners Impresoras Multifuncionales.

Nota: La captura de imágenes y/o grabación de video por parte de los ciudadanos o visitantes a la Institución está prohibida.

No se permite la captura de imágenes y/o grabación de video en las instalaciones o sedes de la ESE FABIO JARAMILLO LONDOÑO, así como del personal por parte de la ciudadanía, funcionarios, contratistas y practicantes, sin previa autorización de la oficina de sistemas.

El acceso y uso de equipos fotográficos y de video para fines Institucionales, prensa o de comunicación a la ESE FABIO JARAMILLO LONDOÑO, debe ser autorizado previamente.

En el caso de equipos de cómputo de la ESE FJL que cuenten con webcams integradas y los dispositivos de videoconferencia su uso es exclusivo para videoconferencias institucionales.

Responsabilidades de los funcionarios, contratistas y practicantes usuarios de dispositivos de captura de imágenes y/o grabación de video:

Adoptar, poner en práctica, socializar, y acatar estos lineamientos.

Usar los dispositivos de captura de imágenes y/o grabación de videos que sean de su propiedad o le hayan sido asignadas para el desempeño de sus actividades de acuerdo a lo estipulado anteriormente.

Abstenerse de fotografiar, escanear, grabar o copiar digitalmente información sensible, clasificada o reservada.

Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de la misma.

Informar a sus superiores sobre la violación de estos lineamientos o si conocen de alguna falta a alguna de ellas.

Monitoreo:

La ESE FABIO JARAMILLO LONDOÑO puede controlar el acceso de dispositivos de captura de imágenes y/o grabación de video a sus instalaciones en las entradas a cada una de sus sedes, por medio del personal de vigilancia y seguridad dispuesto en cada uno de los puntos de ingreso de la entidad.

El monitoreo permanente de uso y manipulación de dispositivos de captura de imágenes y/o grabación de video, es efectuado a través de los sistemas de video vigilancia instalados en las diferentes áreas y sedes de la Institución.

nbsp; La ESE FABIO JARAMILLO LONDOÑO requerirá y mantendrá bajo custodia del personal de vigilancia y seguridad los dispositivos de captura de imágenes y/o grabación de video en las dependencias restringidas y determinadas en esta Política a cualquier persona que ingrese a las mismas y durante el tiempo que permanezca al interior de las mismas.

7.7. LINEAMIENTO 7: USO DE ESCRITORIOS Y PANTALLAS DESPEJADAS

La política de escritorios y pantallas despejadas es extensiva para todos los funcionarios, contratistas y practicantes de la ESE FABIO JARAMILLO LONDOÑO y apoya en la seguridad de la información sensible o crítica del Instituto.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.

Crear conciencia sobre los riegos asociados al manejo de información tanto física como digital y la manera de reducirlos aplicando los lineamientos aquí determinados.

Especificar las recomendaciones y pautas necesarias para mantener las pantallas y escritorios organizados y controlando el reposo de información clasificada o reservada a la vista.

Dictar las pautas para mantener organizado y resguardado los documentos digitales y correos electrónicos en los computadores puestos a disposición de todos los usuarios de los sistemas de información y estructura tecnológica de la ESE FABIO JARAMILLO LONDOÑO.

Este lineamiento se define en el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico entendiéndose para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada funcionario, contratista o practicante del Instituto y pantalla, el área de trabajo virtual sobre el sistema operativo de su computador, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Institucionales.

El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los funcionarios, contratistas y practicantes que tengan acceso a la información de la ESE FABIO JARAMILLO LONDOÑO, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades. Para su definición y aplicación se define de la siguiente manera:

Escritorios:

Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información clasificada o reservada evitando que queden a la vista o al alcance de la mano de personal ajeno a la misma.

En la medida de lo posible los documentos con información clasificada o reservada debe quedar bajo llave o custodia en horas no laborables.

Se debe evitar el retiro de documentos clasificados o reservados de la institución y en el caso de ser necesario se debe propender por su protección fuera de la Entidad y su pronta devolución.

Se deben controlar la recepción y envío de documentos físicos en la institución por medio de registro de sus destinatarios desde el punto de ventanilla única.

Se debe restringir el fotocopiado de documentos fuera del horario normal de trabajo y fuera de las instalaciones. De ser necesario se debe autorizar el retiro de dichos documentos y garantizar su protección y confidencialidad fuera.

Al imprimir o fotocopiar documentos con información clasificada o reservada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.

No se debe enviar ni recibir documentos clasificados o reservados por medio de Fax. No se debe reutilizar papel que contenga información clasificada o reservada.

Pantallas:

Los computadores o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.

Las áreas de trabajo virtuales "pantallas" del computador deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información ya carpetas y unidades de red necesarios para la ejecución de las actividades.

Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los computadores.

Los funcionarios, contratistas y practicantes al retirarse del Instituto deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y estaciones de trabajo utilizados para acceso remoto. Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.

La Oficina de Sistemas determina una configuración automática en todos los equipos de cómputo, propiedad o contratados por el Instituto, para que se active el protector de pantalla del computador, bloqueando el acceso al computador al presentarse una inactividad de 15 minutos. Estos pueden ser nuevamente utilizados por los usuarios al volver a realizar la autenticación por medio de los usuarios y contraseñas asignados.

El fondo de pantalla de cada computador es único para todos las estaciones de trabajo y para todos los usuarios y puede ser cambiado únicamente por la Oficina de Sistemas o por solicitud del Grupo de Comunicaciones de la Oficina de Atención al Ciudadano o del Grupo de Sistemas integrados de Gestión de la Oficina Asesora de Planeación. Para el resto de las áreas, estos cambios deben ser solicitados y validados por el Grupo de Comunicaciones.

Monitoreo:

El área de Sistemas, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de los computadores, monitores y escritorios virtuales y generar el respectivo informe de lo encontrado.

7.8. LINEAMIENTO 8: USO DE DISPOSITIVOS MÓVILES (TABLETS)

La política de uso de dispositivos móviles (tablets) aplica a todos los funcionarios, contratistas y practicantes de LA ESE FABIO JARAMILLO LONDOÑO y apoya en la seguridad de la información sensible o crítica de La Institución.

Los objetivos específicos de este capítulo relacionado con el uso de dispositivos móviles son:

Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.

Crear conciencia sobre los riegos asociados al manejo de información a través de las Tablets y la manera de reducirlos aplicando los lineamientos aquí determinados.

Especificar las recomendaciones y pautas necesarias para mantener tanto los dispositivos como la información protegida.

Dictar las pautas para mantener la operación, y transmisión de la información registrada en las tablets.

Responsabilidades de la Oficina de Sistemas:

Determinar y avalar las opciones de protección de los dispositivos móviles institucionales que hagan uso de los servicios provistos por el instituto.

Establecer las configuraciones aceptables para los dispositivos móviles institucionales que hagan uso de los servicios provistos por ESE FABIO JARAMILLO LONDOÑO.

Determinar los métodos de protección de acceso (por ejemplo, contraseñas o patrones) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado. Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

Implementar una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo.

Instalar un software de antivirus en los dispositivos móviles institucionales que hagan uso de los servicios provistos por el instituto.

Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Responsabilidades de los usuarios:

Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

No deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

Aceptar y aplicar la nueva versión de las actualizaciones que sean notificadas en los dispositivos móviles asignados para su uso.

Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

Abstenerse de almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados

Monitoreo:

La Oficinas de Sistemas sin previo aviso, realizará brigadas de monitoreo para verificar el estado de las tablets y generar el respectivo informe de lo encontrado.

7.9. LINEAMIENTO 9: CONEXIONES REMOTAS

La política de conexiones remotas es extensiva para todos los funcionarios, contratistas y practicantes de la ESE FABIO JARAMILLO LONDOÑO que requieran y les sea autorizado el acceso a terminales o servidores institucionales a través de herramientas VPN para el desarrollo de sus actividades en horarios fuera de los normales o desde ubicaciones diferentes a las oficinas del de la Institución.

Los objetivos específicos de este capítulo relacionado con el uso de escritorios y pantallas despejadas son:

Garantizar la confidencialidad, la privacidad y el uso adecuado y moderado de la información.

Crear conciencia sobre los riegos asociados al acceso y gestión de información sobre las plataformas institucionales de manera remota y la manera de reducirlos aplicando los lineamientos aquí determinados. Especificar las recomendaciones y pautas necesarias para mantener segura la información y los elementos utilizados para el acceso y operación remota de información.

Dictar las pautas para mantener organizado y resguardado las credenciales de acceso así como los elementos de protección para asegurar la conexión remota.

Responsabilidades de la Oficina de Sistemas:

Establecer e implementar los métodos de conexión remota a la plataforma tecnológica de la ESE FABIO JARAMILLO LONDOÑO. Implementar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica Institucional.

Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la ESE FABIO JARAMILLO LONDOÑO de manera permanente.

Responsabilidades de los usuarios:

Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la ESE FABIO JARAMILLO LONDOÑO y deben acatar las condiciones de uso establecidas para dichas conexiones.

Mantener en total reserva las direcciones de entrada a las direcciones Institucionales (direcciones IP o direcciones Web) al igual que las credenciales que les han sido otorgadas para su resguardo.

Mantener la confidencialidad y protección de la información a la que tienen acceso fuera de las instalaciones Institucionales.

Aplicar herramientas de antivirus sobre sus computadores personales, en lo posible, para brindar una mayor protección a los archivos e información que están gestionando.

Dar aviso a la oficina de Sistemas de cualquier posible abuso o intento de violación tanto de los accesos como de las credenciales entregadas.

Monitoreo:

La Oficinas de Sistemas en, sin previo aviso, realizan brigadas de monitoreo para verificar el estado de las conexiones remotas, así como el tiempo y uso efectuado a través de este medio y generar el respectivo informe de lo encontrado.

8 BIBLIOGRAFIA:

ISO/IEC 27001 :2013.

9 CONTROL DE CAMBIOS:

CONTROL DE CAMBIOS		
VERSION	MODIFICACIÓN	FECHA APROBACIÓN
01	Se elabora formato por primera	2017/12/28.

Elaboro.	Reviso.	Aprobó.
Ingeniero De Sistemas Tecnología E Información	Ingeniero De Sistemas Tecnología E Información	Gerencia.
Documento de: Sistema Integrado de Gestión(SIG)		