TABLA DE CONTENIDO

INTRODUCCIÓN

Los activos de información y los equipos informáticos son recursos importantes y vitales de nuestra organización. Sin ellos estaría seriamente comprometida nuestra participación en el mercado y por tal razón tenemos la obligación de preservarlos, utilizarlos y mejorarlos con el fin de garantizar la buena marcha y crecimiento de nuestra institución.

Desde el punto de vista de los riesgos informáticos, los computadores representan la mayor fuente de vulnerabilidad para la información manejada a través de sistemas de procesamiento de datos, y para los recursos computacionales de la empresa (red de datos, sistemas de información, computadores personales), por lo que se hace necesario establecer normas que permitan ejercer una adecuada administración y control sobre estos recursos, además las acciones apropiadas para asegurar que la información y los sistemas informáticos estén protegidos de muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje extorsión, violación de la privacidad, hackers, interrupción del servicio, accidentes y desastres naturales.

Hacen parte del contenido de este manual, aspectos como la seguridad física, seguridad lógica, inventario de hardware y software, procedimientos de backup y recuperación, acciones preventivas contra virus informáticos; normas relacionadas con la ley de derechos de autor en cuanto al uso legal de software, prevención de riesgos sobre datos, software y hardware durante el mantenimiento de los equipos, entre otras.

Igualmente establecer un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización, así como crear una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos por tal razón, la política de seguridad debe concluir en una posición consciente y vigilante del personal por el uso y las racionalmente limitaciones de los recursos y servicios informáticos.

En este sentido, la organización define un Manual de Seguridad Informática, el cual busca describir los riesgos informáticos asociados a sus actividades, así como, las políticas para asegurar la integridad de los activos de información y su uso adecuado con el fin de garantizar la disponibilidad, trazabilidad, confidencialidad y seguridad de la información de la organización.

NORMATIVIDAD Y ESTANDARES DE CIBERSEGURIDAD

Este manual está basado en la normatividad y estándares de ciberseguridad vigentes.

- Norma Técnica Colombiana NTC-ISO/IEC 27001 Sistemas de Gestión de la Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC 27002 Tecnología de la Información. Técnica de Seguridad. Código de Práctica para Controles de Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC 27003. Guía para la implementación de un Sistema de Gestión de Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC 27005. Gestión de la Seguridad de la Información.
- Norma Técnica Colombiana NTC-ISO/IEC 27032. Directrices para la Ciberprotección.
- Norma Técnica Colombiana NTC-ISO/IEC 27040. Seguridad de almacenamiento
- Norma Técnica Colombiana NTC-ISO/IEC 9001 Sistema de Gestión de la Calidad.
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL hoy Gobierno Digital.

1. TÉRMINOS Y DEFINICIONES

- **Activo:** Según (ISO/IEC 13335-12004) Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma con valor para la organización. Se pueden clasificar de la siguiente manera:
  - Datos: Todos aquellos elementos básicos de la información, que se generan, recogen, gestionan, transmiten y destruyen en la empresa.
  - Aplicaciones: Software que se utiliza para la gestión de información.
  - Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como externos, aquellos que la organización suministra a clientes y usuarios.
  - Tecnología: Todos los equipos utilizados para gestionar la información y las comunicaciones. Ejemplo: Equipos de cómputo, teléfonos, impresoras.
  - Instalaciones: Son todos los lugares en los que se alojan los sistemas de información.
  - Equipamiento Auxiliar: Todos aquellos activos que dan soporte a los sistemas de información y que no se hallan ninguno de los tipos definidos. Ejemplo: Aire acondicionado.

- **Administración de riesgos:** Enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias, de desarrollo y mitigación del riesgo. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

- **Alerta:** Notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Amenaza:** Según (ISO/IEC 13335-1 20004) Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgo:** Según (ISO/IEF Guía 73:2002) Uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Antivirus:** Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.

- **Área Crítica**: Es el área física donde se encuentra instalado el equipo de informática y telecomunicaciones que requiere de cuidados especiales y que son indispensable para el funcionamiento continuo de los sistemas de comunicaciones.

- **Auditoría**: Proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, propiedad que garantiza que la identidad de un sujeto o recurso es la que declara.

- **Backup (Copia de Seguridad):** Programas y/o técnicas de respaldo que permiten realizar una copia idéntica de la información alojada en una base de datos, servidor, equipo de cómputo, etc., almacenándola en un dispositivo de

almacenamiento masivo como discos duros externos, cintas u otro dispositivo de red destinado para este fin, con el objetivo de realizar la recuperación de la información y evitando pérdidas de información críticas.

- **Base de datos**: Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos y ordenarlos bajo diferentes criterios.

- **Botnets**: Conjunto de equipos infectados que ejecutan programas de manera automática y autónoma, que permite al creador del botnet controlar los equipos infectados y utilizarlos para ataques más sofisticados como ataques DDoS/

- **Características de la información:** Principales características son la confidencialidad, la disponibilidad y la integridad.

- **Claves de sesión**: Se emplean para el cifrado de un único mensaje o para el cifrado de la información intercambiada en una sesión establecida entre dos equipos o usuarios.

- **Clave maestra**: Es generada aleatoriamente ya sea de forma manual o con un generador automático de claves, puede ser modificada por el usuario (el administrador de seguridad informática) y se usa para cifrar únicamente claves secundarias.

- **Claves de usuarios o primarias**: Se emplean para autenticación y para asegurar la confidencialidad de los datos, ya sea mediante el cifrado de datos transmitidos o bien por la protección de datos almacenados en un soporte informático.

- **Código malicioso:** También conocido como malware. Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos, son algunos ejemplos de códigos maliciosos.

- **Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de manera prevista. También se puede definir como la probabilidad en que un producto realizará su función prevista sin incidentes por un periodo de tiempo especificado.

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

- **Control:** Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado, pero que se corrige.

- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza. Ejemplo: Avisos.

- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Criptografía**: Es la ciencia que se encarga de estudiar las distintas técnicas empleadas para cifrar la información y hacerla irreconocible a todos aquellos usuarios no autorizados de un sistema informático, de modo que sólo los

propietarios legítimos o los usuarios autorizados puedan descifrar la información original.

- **Criptoanálisis**: Es la ciencia que se ocupa de estudiar herramientas y técnicas que permitan romper los códigos y sistemas de protección definidos por la criptografía.

- **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.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización – tras el resultado de los procesos de evaluación y tratamiento de riesgos – además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

- **Denegación de servicios:** Acción iniciada por una persona u otra causa que incapacite el hardware o el software o ampos y después niegue el servicio.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **DHCP:** Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración.

- **Directiva:** Según (ISO/IEC 13335-1: 2004) Descripción que clarifica qué debería ser hecho y como, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** Según (ISO/IEC 13335-1: 2004) Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **DNS:** Se define como la resolución de nombre de los equipos en la red de la organización.

- **Evaluación de riesgo:** Según (ISO/IEF Guía 73:2002) proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

- **Evento:** Según (ISO/IEC TR 18004:2004) suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

- **Firewall**: Sistema colocado entre una red local e internet asegurando la red local y controlando que usuarios no autorizados ingresen. El Firewall permite resguardar la información de los equipos locales de cualquier acceso remoto de tipo malicioso o ataques informáticos

- **Gestión claves:** Controles referido a la gestión de claves criptográficas.

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye valoración de riesgos y el tratamiento de riesgos.

- **Gusanos:** Programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre afectan la red.

- **Hacker:** Persona con grandes conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos y a manipularlos.

- **HOAX**: es un correo electrónico distribuido en formato de cadena, cuyo objetivo es hacer creer a los lectores que algo falso es real.

- **Impacto:** Resultado de un incidente de seguridad de la información.

- **Incidente:** Según (ISO/IER TR 18044:2004) evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información**: Se refiere a un conjunto organizado de datos contenido en cualquier documento que se generen, obtengan, adquieran, transformen o controle.

- **Ingeniería social:** Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces, para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

- **Internet:** Red de ordenadores conectados a toda extensión que ofrece diversos servicios a sus usuarios como pueden ser el correo electrónico, el chat o la web.

- **IPS:** Sistema de prevención de intrusos. Dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **Llaves de cifrado de archivos**: Llave cifrada con una frase de contraseña, su finalidad es cifrar archivos. Es utilizada únicamente en el cifrado de un archivo y después se destruye.

- **Malware**: Termino principal utilizado para hablar de todas las amenazas informáticas.

- **Phishing:** Delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta.

- **Plan de tratamiento de riesgos:** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger las mismas.

- **Política de seguridad:** Documento que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Política de escritorio despejado:** La política de la empresa que indica a los funcionarios, contratistas y demás colaboradores que deben dejar su escritorio libre de cualquier tipo de información susceptible de mal uso al finalizar el día

- **Protección de duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información.

- **Ransomware**: Software malicioso que infecta una o varias computadoras restringiendo el acceso a los archivos del equipo y solicitando un pago por la liberación o rescate de la información.

- **Redes VLAN /WLAN:** LAN es la interconexión de varias computadoras y periféricos. VLAN es un método de crear redes lógicamente independientes dentro de una misma red física. WLAN es lo mismo que VLAN, pero inalámbricamente.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

- **Riesgo residual:** Según (IS0/IEC Guía 73:2002) El riesgo que permanece tras el tratamiento del riesgo.

- **Rogue**: Código malicioso que simula ser un programa de seguridad, con el fin de lograr que el usuario pague por una aplicación dañina o inexistente.

- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad informática:** Consiste en asegurar que los recursos se utilicen de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación solo sea posible a las personas que se encuentran acreditadas y dentro de los límites de su autorización.

- **Seguridad de la información:** Según (ISO/IEC 27002:20005) preservación de la confidencialidad, integridad y disponibilidad de la información, además. Otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **Sistemas de criptografía simétrica**: Son en aquellos donde se emplea la misma llave tanto para cifrar como para descifrar el texto original.

- **Sistemas de criptografía asimétrica**: En estos sistemas se utilizan dos llaves distintas: una para realizar el cifrado y otra para el proceso de descifrado del texto original

- **Spamming:** Se llama SPAM, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario.

- **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad de control, aunque también puede ser utilizado con fines maliciosos.

- **Teletrabajo:** Es una forma de organización laboral, que se efectúa en el marco de un contrato de trabajo de una relación laboral dependiente, que consisten en el desempeño de actividades remuneradas utilizando como soporte las tecnologías de la información y de la comunicación – TIC para el contacto entre el trabajador y empleador sin requerirse la presencia física del trabajador en un sitio especifico (Ley 1221 de 2008).

- **Trabajo Remoto**: Se entiende como trabajo en casa la habilitación al funcionario para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza, sin modificar la naturaleza del contrato o relación laboral o legal y reglamentarias respectiva, ni tampoco desmejorar las condiciones del contrato laboral, cuando se presenten circunstancias ocasionales, excepciones o especiales

que impidan a que el funcionario pueda realizar sus funciones en su lugar de trabajo, privilegiando el uso de las tecnologías de la información y las comunicaciones (Ley 2088 de 2021).

- **Tratamiento de riesgos:** Según (ISO/IEC Guía 73:2002) proceso de selección e implementación de medidas para modificar el riesgo.
- **Tratamiento de riesgos:** Según (ISO/IEC Guía 73:2002) proceso de selección e implementación de medidas para modificar el riesgo.
- **Trazabilidad:** Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.
- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- **Usuario:** Se refieren a los funcionarios, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **Valoración de riesgos:** Según (ISO/IEC Guía 73:2002) Proceso completo de análisis y evaluación de riesgos.
- **Virus:** Tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo.

2. OBJETIVOS Y ÁMBITO DE APLICACIÓN

2.1. OBJETIVO GENERAL

Describir las políticas y controles para prevenir la materialización de riesgos informáticos, de tal manera que se vele por la integridad de los activos de información de la empresa y se garantice la disponibilidad, trazabilidad y confidencialidad de la información de la organización.

2.2. OBJETIVOS ESPECÍFICOS

- Garantizar el correcto uso de los activos físicos de información (computadores, impresoras, redes de datos, entre otros) como medios para almacenar, transferir y procesar la información.
- Garantizar el uso adecuado de aplicaciones electrónicas como e-mail, plataforma Google, internet, entre otros.
- Garantizar el correcto uso de los activos de almacenamiento de la información (bases de datos, medios de almacenamiento, software, entre otros) como medios para almacenar información de la organización.
- Generar conciencia y compromiso en seguridad de la información en los colaboradores.

2.3. ALCANCE

Las políticas de seguridad de la información adoptadas en este manual se enmarcan dentro del sistema de gestión de la organización y son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan alguna relación con la organización.

2.4. PRINCIPIOS DE SEGURIDAD

Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

2.5. CONSEJOS BÁSICOS SEGURIDAD INFORMÁTICA

Es recomendable seguir una serie de consejos, prácticas y costumbres para maximizar la seguridad informática en la organización, algunos de ellos son los siguientes:

- Mantener actualizado el equipo (Sistema Operativo y aplicaciones).
- Instalar software legal (se obtiene garantía y soporte).
- Usar contraseñas fuertes (evitar nombres, fechas, datos conocidos o deducibles, etc.).
- Utilizar herramientas de seguridad para proteger o reparar el equipo.
- No descargar o ejecutar ficheros desde sitios sospechosos o procedentes de correos sospechosos o no solicitados.
- Analizar con un antivirus todo lo que se descargue.
- No facilitar la cuenta de correo a desconocidos o publicarla en sitios desconocidos.
- No responder a mensajes falsos.
- Utilizar herramientas o sistemas de copias de seguridad para respalda la información.

3. RESPONSABILIDADES

3.1. DE LA DIVISIÓN DE TECNOLOGÍA E INNOVACIÓN

- Proporcionar los activos de información a los procesos, de acuerdo con sus requerimientos, así como, garantizar la disponibilidad y oportunidad de los mismos.
- Garantizar el oportuno y adecuado mantenimiento y soporte técnico a los activos de información.
- Asegurar la confiabilidad de los sistemas operativos y la red de datos de acuerdo con la utilizada por la organización.
- Velar por el cumplimiento de las políticas de seguridad informática definidas para la organización.
- Hacer entrega formal a los usuarios de los equipos, sus componentes y el software.
- Acompañar la entrega, de un inventario detallado de la configuración de hardware y licencias de software.
- Mantener control del uso de las licencias de software y su correspondencia con el hardware.
- Mantener actualizado el inventario de equipos y su configuración.
- Administrar la instalación, reinstalación y soporte del software de uso general.
- Mantener actualizado el inventario de equipos en arrendamiento y/o leasing.
- La documentación técnica de uso generalizado en cuanto a hardware y software de computadores, así como las copias originales de software deben ser administradas por el departamento de Sistemas de la empresa.
- El departamento de Sistemas instruirá sobre los servicios informáticos básicos (Acceso a la Red, Acceso a Aplicaciones, Correo Interno, Correo Institucional, Intranet) existentes en la FOSCAL - FOSCAL INTERNACIONAL para el correcto uso y mejor aprovechamiento.

3.2. DE LOS TRABAJADORES DE LA ORGANIZACIÓN

- Cumplir con las políticas establecidas e implementar los controles descritos en este manual.
- Garantizar el buen uso y custodia de los activos de información.
- Evitar en todo momento la fuga de información almacenada en las diferentes unidades definidas por la institución.
- Reportar de forma inmediata a la División de Tecnología e Innovación cuando se detecte riesgo alguno, real o potencial, sobre equipos de cómputo o de comunicaciones.
- En caso de identificar abusos o incumplimientos frente a las políticas establecidas en este manual, es responsabilidad de todo funcionario, reportar para realizar análisis y definición de acciones correctivas y/o preventivas y/o de mejora.
- Recibir formalmente el hardware y el software debidamente inventariado.
- Controlar y reportar al departamento de Sistemas cualquier irregularidad en el hardware y/o software que se presente en cualquiera de los elementos de cómputo que tenga a cargo.
- Solicitar al departamento de Sistemas los cambios de localización que haya que hacer a los equipos.
- Las solicitudes de servicios se deben realizar de acuerdo con el procedimiento "Realizar Solicitudes a Sistemas" aprobado por la unidad de Gestión de la Calidad de la FOSCAL - FOSCAL INTERNACIONAL.
- Es responsabilidad de los usuarios la adecuada conservación y custodia de la documentación que le sea entregada en relación con su hardware y/o software (manuales, CD's, Drivers, y demás).
- El control de acceso físico a los computadores es responsabilidad de los funcionarios, a cuyo cargo está cada equipo.

3.3. DE LA SEGURIDAD INFORMÁTICA

- Los equipos, software y suministros sólo serán utilizados para labores propias del trabajo. No podrán ser instalados en los equipos programas o archivos que afecten el proceso de licenciamiento Institucional y/o pongan en riesgo el buen funcionamiento del computador.

- La información sensible y/o confidencial que reside en los computadores debe tener implementado un adecuado control de acceso lógico, utilizando códigos de usuario, contraseñas y/o software específico de seguridad.
- Para dar a compartir directorios y/o archivos de los computadores, a través de la red, se debe especificar el tipo de acceso que otros usuarios pueden tener. Es responsabilidad del "Propietario" de la información, el control de acceso a datos y/o directorios personales en la red.
- Protección lógica de documentos: Es responsabilidad de cada usuario utilizar el mecanismo de protección mediante claves de acceso, a los documentos generados en procesador de palabra, hoja electrónica, graficadores, etc., de acuerdo con el grado de confidencialidad o sensibilidad de la información contenida.
- El usuario de común acuerdo con el Administrador de la Red de datos podrá hacer uso de los recursos del servidor de archivos para almacenar allí toda información sensible. Para que esta información entre en proceso de copias de seguridad, el usuario, debe elaborar el formato de copias de seguridad que para este fin tiene el departamento de Sistemas, informando el lugar de almacenamiento.
- Las claves de acceso a nivel del computador, la red y los sistemas de información son responsabilidad exclusiva del usuario final, sólo deberá ser conocida por él y será responsable del buen uso y custodia del mismo. Las siguientes son características de una clave confiable:

    - No tener lógica con información de usuario
    - No tener conexión lógica con el contenido de archivos
    - No tener relación con fechas
    - No tener palabras triviales del idioma
    - Longitud mínima de 8 caracteres
    - Debe contener mayúsculas, minúsculas, números y caracteres especiales.
    - Se debe cambiar periódicamente
    - Solo la debe conocer el dueño

3.4. DE LA SEGURIDAD FÍSICA

Los mecanismos de control de acceso físico para el personal y terceros deber permitir el acceso a las instalaciones y áreas restringidas de la FOSCAL - FOSCAL INTERNACIONAL sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de las comunicaciones.

3.4.1. Normas Dirigidas a la División de Tecnología e Innovación

- Las solicitudes de acceso al Data Center o a los centros de cableado deben ser aprobadas por funcionarios de la División de Tecnología e Innovación autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha área durante su visita.
- Se debe registrar el ingreso de los visitantes al Data Center y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Deshabilitar o modificar de manera inmediata los privilegios de acceso físico a Data Center o centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- Proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el Data Center y centros de cableado; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- Velar porque los recursos tecnológicos de la Institución ubicados en el Data Center y centros de cableado se encuentran protegidos contra fallas o interrupciones eléctricas.
- Certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

3.4.2. Normas Dirigidas a Directivos y Jefes de área

- Velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en sus áreas.
- Autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la institución.

3.4.3. Normas Dirigidas a todos los usuarios

- Los ingresos y egresos de personal a la institución deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones del instituto; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los funcionarios y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.
- Registrar al momento de su entrada, el equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propias de la institución o tramitar la autorización del elemento en el área de seguridad.

3.4.4. Normas Dirigidas a Mantenimiento y Planta Física

- Proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en la institución
- Identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones del instituto
- Es responsabilidad lo departamento Mantenimiento y Planta Física, aplicar normas mínimas de seguridad en las áreas en donde existan instalados computadores, específicamente en cuanto a:

    - Mecanismos para controlar el acceso sólo a personal autorizado.
    - Existencia de extintores manuales apropiados para áreas de cómputo y procedimientos de mantenimiento y control de vigencia de los mismos.
    - Protección del cableado eléctrico y de la red.
    - Conexiones eléctricas en buen estado.
    - Estabilización de la energía dentro de los rangos permisibles y/o tolerables por los equipos de cómputo.
    - Conservación de tierra de alta calidad dentro de los rangos permisibles
    - Conexión correcta de las tomas (Fase/Tierra/Neutro)
    - Existencia de un sistema ininterrumpido de energía (UPS) si la criticidad de las operaciones lo ameritan.
    - Control de acceso a los tableros del sistema eléctrico.
    - Inspección frecuente de empalmes, paneles, cableado, estabilidad de la corriente, voltaje frecuencia, etc.
    - Identificación de toma estabilizada.
    - Disposición de toma independiente para la conexión de otros aparatos eléctricos de alto consumo.
    - Otras normas de seguridad industrial aplicables a los ambientes de oficina.

- Para las instalaciones de redes y/o eléctricas, el departamento de Mantenimiento realizará su actividad en coordinación con el departamento de Sistemas.
- Ventilación apropiada, regulación de energía e implementación de cerraduras de seguridad a los cuartos técnicos.

3.4. DE TERCEROS

- Todo computador perteneciente a empresas outsourcing y/o terceros que necesite conectarse a la red de datos de la FOSCAL - FOSCAL INTERNACIONAL, deberá pasar por un proceso de autorización y revisión del mismo para evitar que éste pueda contaminar la red con virus y/o programas maliciosos.
- Todo usuario perteneciente a empresas outsourcing y/o terceros conectados a la red de datos de la FOSCAL - FOSCAL INTERNACIONAL deberá acatar las políticas descritas en este documento y seguir las normas para el uso de los equipos de cómputo, internet y correo electrónico establecidos por la institución.

4. ACTIVOS DE INFORMACIÓN

FOSCAL - FOSCAL INTERNACIONAL como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida a través de sus diferentes sistemas y servicios, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices descritas en este manual y que regulan el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de FOSCAL - FOSCAL INTERNACIONAL, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos y finalidades constituidas en las políticas de la institución.

Toda la información sensible, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

FOSCAL - FOSCAL INTERNACIONAL cuenta con los siguientes activos de información:

Activos físicos:

- Equipos de cómputo de escritorio
- Computadores portátiles
- Impresoras multifuncionales
- Scanner
- Red de datos
- Equipos de networking y seguridad perimetral

Activos de almacenamiento de la información:

- Medios de almacenamiento (Disco duros, Cintas de Seguridad, Almacenamiento en la Nube)
- Software (Indicar cuales son los softwares con activos de la información)

4.1. DIRECTRICES GENERALES

Todos los funcionarios, contratistas, pasantes proveedores y terceros o que, por su rol, tengan bajo su propiedad o custodia, activos de información de la institución deben acatar y dar estricto cumplimiento a los descrito en el presente manual

- Definición de controles para la protección de los activos de la información.
- Velar por el debido inventariado de los activos
- Mantener los controles definidos para la protección de los activos de información.
- Seguimiento y monitoreo de los responsables de los activos de la información para la verificación de los controles definidos.
- Verificación de la clasificación de los activos de la información acorde
    - Nivel de Criticidad
    - Valor
    - Disposiciones de normativa legal

4.2. NORMAS DE RESPONSABILIDAD

4.2.1. Propietarios o Responsables de los Activos de la Información

- Actuar como propietarios de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
- Generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

4.2.2. División de Tecnología e Innovación

- El área de Tecnología e Innovación es la propietaria de los activos de información correspondientes a la infraestructura, sistemas y servicios de la institución, en consecuencia, debe asegurar su apropiada operación y administración.
- Responsables de la instalación, cambio o eliminación de componentes de la infraestructura, sistemas y servicios de la institución.
- Debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.
- Responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

4.2.3. Directores y Jefes de área

- Autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por la Dirección de Tecnología.
- Recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran del instituto o son trasladados de área.

4.2.4. Usuarios

- Los recursos tecnológicos institucionales deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen del instituto.
- Los recursos tecnológicos provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la institución; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Todos los puestos de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los usuarios deben realizar la entrega de su puesto de trabajo; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.
- Los usuarios no deben realizar cambios en los puestos de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla definido.
- Los usuarios de los activos informáticos no deben realizar cambios físicos, tales como: cambio de ubicación, mantenimientos, repotenciación, modificaciones en su configuración física.

4.3. CLASIFICACIÓN Y MANEJO

FOSCAL - FOSCAL INTERNACIONAL define los niveles más adecuados para clasificar su información de acuerdo con los lineamientos establecidos en la política de tratamiento de datos PTI, las leyes y regulaciones vigentes del Estado Colombiano, con el objetivo que los propietarios o administradores de la misma la cataloguen y determinen los controles pertinentes para su protección.

Es importante que toda la información sea identificada, clasificada y documentada, así la FOSCAL - FOSCAL INTERNACIONAL proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios del y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

4.3.1. Comité de Protección de Datos Personales

- Definir y establecer dentro del Manual de Protección de Datos Personales la clasificación de la información para ser aprobados por la Junta Directiva.

4.3.2. División de Tecnología e Innovación

- Proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- Definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.
- Efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.
- Administrar el contrato de almacenamiento y resguardo de las cintas de backup, otros medios de almacenamiento y documentos físicos con el proveedor del servicio.

4.3.3. Archivo

- Utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- Realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

4.3.4. Propietarios o Administradores

- Clasificar su información de acuerdo con los lineamientos establecidos por la institución.
- Responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

4.3.5. Usuarios

- Deben acatar los lineamientos de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física instituto.
- La información física y digital debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias: verificar las áreas adyacentes a impresoras, escáneres y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

5. GESTIÓN DEL RIESGO

FOSCAL - FOSCAL INTERNACIONAL define, a través de la Gestión del Riesgo, las actividades que se deben llevar a cabo para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados a la operación en el servicio y administración de la institución, con el fin de garantizar la continuidad del negocio, cumpliendo los objetivos organizacionales, así como, velar por la seguridad de los activos, personas y procesos de la organización.

Los riesgos informáticos son aquellos asociados a fallas o mal uso de los activos de la información que puedan ocasionar daños o pérdidas a la organización.

Los riesgos informáticos identificados en el desarrollo de las actividades son:

5.1. ACCESO NO AUTORIZADO A UN ACTIVO DE LA INFORMACIÓN

El acceso no autorizado tiene lugar cuando una entidad o individuo no autorizado consigue acceder a un activo de la información de la organización, poniendo en riesgo la disponibilidad, integridad y confidencialidad.

El acceso no autorizado a un activo de la información se puede dar debido a:

- Ausencia de políticas y parámetros de configuración en el firewall perimetral de la organización.
- Falta de claves de acceso a los activos de la información.
- Acceso a las instalaciones donde se encuentran ubicados los medios de almacenamiento de la organización.
- Suplantación de la identidad.
- Incumplimiento de las políticas del uso de los activos de la información.

5.1.1. Controles para prevenir el acceso no autorizado a un activo de información

- La institución define claves de acceso con usuario y contraseña a los equipos de cómputo de escritorio y portátiles, así como, a la red WIFI. Estas claves son entregadas por la División de Tecnología e Innovación a los usuarios.
- La organización tiene instalado Firewall perimetral en la red de datos.
- Para impedir el acceso no autorizado a los diferentes Cuartos de Comunicaciones se tiene establecido dos tipos de controles: Control de Acceso a través tarjeta de proximidad y uso de llaves.
- Con el fin de garantizar que no haya suplantación de la identidad ni acceso a las claves establecidas, la Organización define las políticas de uso de los activos de la información.
- La organización establece a través del proceso de Desvinculación del personal, los parámetros para hacer entrega de claves y usuarios de los activos de la información de la organización, con el fin de garantizar y preservar la información de la organización.
- Servicios accesibles desde el exterior de la organización a través de VPN y bajo aprobación de la División de Tecnología e Innovación

5.2. PÉRDIDA DE INFORMACIÓN SENSIBLE

Alteración, pérdida o destrucción de la información de la organización que pueda generar daños.

La pérdida de la información se puede generar por:

- Por acceso no autorizado a un activo de la organización.
- Presencia de virus en equipos de cómputo (debido a desactualización del antivirus, descarga de archivos de correos electrónicos, uso inadecuado de memorias USB, ingreso a páginas riesgosas, entre otros)

- Fallas en el disco duro interno y externo.
- Fallas en el software.
- Ausencia de copias de seguridad de la información.
- Incumplimiento de las políticas del uso de los activos de la información.

5.2.1. Controles internos para prevenir la perdida de información sensible

- FOSCAL - FOSCAL INTERNACIONAL instala antivirus en todos los equipos de cómputo con el fin de detectar, bloquear y/o eliminar virus informáticos. Adicionalmente, establece políticas de uso de internet, correo electrónico y memorias con el fin de prevenir la presencia de virus en los equipos.
- La institución programa e implementa mantenimientos de software y hardware con el fin de garantizar el correcto funcionamiento de los equipos de cómputo.
- FOSCAL - FOSCAL INTERNACIONAL cuenta con procedimiento, con el fin de garantizar copias de seguridad de la información para los sistemas definidos.
- El software empleado para el desarrollo de las actividades de la empresa es contratado con proveedores calificados con el fin de garantizar la confiabilidad y disponibilidad de la información de la organización que reposa en los mismos.
- El control realizado a dichos proveedores se lleva a cabo a través de auditorías realizadas por los responsables.
- La institución define las políticas de uso de los activos de información, establecidas en este manual.

5.2.2. Controles externos para prevenir la perdida de información sensible

Los sistemas de información que almacenan, procesan o transmiten información clasificada como confidencial, en infraestructura tecnológica propia de la institución (Físicos o virtuales) o contratados a terceras partes (Físicos o en Internet), deberán asegurar la generación de copias de respaldo, su periodo de retención, rotación y métodos apropiados para su restauración. Estas copias de seguridad deben estar en lugares apropiados cumpliendo los requisitos de condiciones ambientales y de seguridad, en custodia para garantizar su integridad y disponibilidad y realizar una verificación periódica que los datos retenidos en los medios son fiables y garantizan una recuperación de los sistemas.

Para realizar el respaldo de la información de cada sistema en uso por la institución se manejan los siguientes controles para resguardar la información en cada uno de las plataformas:

- La División de Tecnología e Innovación define un procedimiento para las actividades de backup de la información de la institución, teniendo en cuenta la criticidad y las necesidades de disponibilidad de datos. Este procedimiento debe estar debidamente documentado para seguimiento y control.
- Se debe identificar el o los responsables que ejecuten las actividades de backup, validando y asegurando que el proceso se ejecute de acuerdo al cronograma.
- Quien ejecute el rol de administrador o supervisor de backup debe validar el resultado de la ejecución de las copias de seguridad y registrar las novedades o hallazgos identificados.

Para realizar los backups se tienen 3 opciones que son:

- **Backup Full o completo**: Es la copia completa de la información, este tipo de backup es el que requiere mayor espacio de almacenamiento.

- **Backup Incremental**: Es la copia con las modificaciones que se han realizado desde el último backup completo realizado, de manera que cuando se requiera una restauración, habrá que superponer todas las copias de seguridad incrementales que se tengan. En estos casos, es habitual realizar una copia completa tras realizar varios incrementales, para, así, comenzar desde cero la secuencia y minimizar los fallos en la recuperación en el caso de que alguna copia incremental estuviese corrupta.

- **Backup Diferencial**: Es la copia de los cambios realizados desde el último backup completo, es decir, que, si se realiza más de una copia diferencial, éstas se realizarán con respecto al último completo y, por tanto, estaremos duplicando datos durante la salvaguarda de ficheros.

El esquema de retención establecido por la institución se define de la siguiente manera:

- Backups Diarios. Retención 28 días.
- Backups Semanales. Retención 56 días.
- Backups Mensuales. Retención 1 año.
- Backups anuales. Retención permanente.

5.3. VULNERABILIDADES Y AMENAZAS

5.3.1. Vulnerabilidades

Una vulnerabilidad es un fallo o debilidad de un sistema de información que pone en riesgo la seguridad de la misma. Se trata de un "agujero" que puede ser producido por un error de configuración, una carencia de procedimientos o un fallo de diseño. Los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas informáticos (por ejemplo, de los sistemas operativos) para poder entrar en los mismos y realizar actividades ilegales, robar información sensible o interrumpir su funcionamiento.

5.3.2. Amenaza

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

5.3.3. Recomendaciones

- Realizar un inventario de nuestros activos TI: servidores, infraestructura de redes, aplicaciones y periféricos (impresoras, etc.).
- Realizar pruebas de penetración para detectar posibles vulnerabilidades tanto externas como internas, simulando a un hacker externo (lo también se conoce como hacking ético) o a personal interno con determinados privilegios.
- Realizar copias de seguridad periódicas.
- Monitorizar constantemente los avisos de últimas vulnerabilidades conocidas. Una herramienta útil en este sentido es el repositorio de vulnerabilidades del CERTSI.
- Mantener las aplicaciones y sistemas actualizadas y parcheadas.
- Realizar escaneos de vulnerabilidades que permitan su detección y posterior corrección.
- Realizar seguimiento a los ciberataques identificados por servicios de ciberseguridad y seguridad de la información descritos en la Guía de Ciberataques.
- Realizar pruebas de penetración en los sistemas, red y aplicaciones para identificar debilidades.
- Utilizar solo webs seguras con https y certificado digital.
- Utilizar contraseñas robustas y diferentes para proteger todas tus cuentas.
- Utilizar un antivirus para analizar todas las descargas y archivos sospechosos.

5.4. CONTRASEÑAS

Las contraseñas o passwords constituyen el mecanismo básico que se emplea para la autenticación de los usuarios para el acceso a servicios y aplicaciones. La fortaleza del mecanismo de autenticación basado en contraseña se fundamenta en dos principios básicos. En primer lugar, la contraseña debe ser secreta; sólo debe conocerla el propio usuario que además es el responsable de su custodia. En segundo lugar, no debe ser posible averiguar la contraseña; las contraseñas no deben ser predecibles ni deducibles a partir de información disponible de forma pública.

5.4.1. Requisitos obligatorios de las contraseñas

- Se deben utilizar al menos 8 caracteres para crear la clave.
- Estar compuesta por uno o más caracteres de al menos 3 de estos grupos:
  - Letras mayúsculas
  - Letras minúsculas
  - Números
  - Símbolos o caracteres especiales
- La contraseña no deberá ser igual a ninguna de las 6 últimas contraseñas usadas
- No contendrá el nombre de cuenta del usuario o partes de su nombre completo.
- No se deben utilizar palabras que se contenga en diccionarios en ningún idioma.
- La contraseña se deberá cambiar periódicamente por los menos dos veces al año.
- Es recomendable que las letras alternen aleatoriamente mayúsculas y minúsculas.

5.4.2. Recomendaciones sobre el uso de la contraseña

Adicional a los requisitos obligatorios, puede incluir las siguientes recomendaciones;

- Evitar utilizar secuencias básicas de teclado (por ejemplo: qwerty, 12345…)
- No utilice la letra ñ si viaja mucho y no sabe cómo ponerla en teclados no españoles).
- No se debe utilizar información personal en la contraseña: nombre del usuario, apellidos, fecha de nacimiento. Aniversarios, nombres de familiares, documento de identificación o número de teléfono.
- No implementar la misma contraseña para varias cuentas
- Existen muchas guías y tutoriales sobre como elegir contraseñas. No elija en ningún caso alguna contraseña que se muestre como ejemplo.

5.4.3. Protección de la contraseña

Con respecto a la custodia confidencial de las contraseñas, se recomienda las siguientes prácticas.

- Las contraseñas no deben compartirse con nadie. Las contraseñas deben tratarse como información confidencial de la institución.
- La contraseña es una información sensible orientada a identificarle de forma unívoca que no debe compartirse con compañeros de trabajo o colaboradores.
- Las contraseñas no deben incluirse en ningún tipo de comunicación electrónica.
- No es recomendable habilitar los campos de recordar contraseñas.
- No escriba jamás su contraseña en ordenadores públicos, compartidos o aquellos en que se desconozca su nivel de seguridad o se estime que pueden estar monitorizados de forma remota.
- Ante cualquier sospecha de que su contraseña ha podido ser comprometida, informe a la División de Tecnología e Innovación y proceda a cambiarla.

6. NORMAS DE SEGURIDAD DE LA INFORMACIÓN

Para FOSCAL - FOSCAL INTERNACIONAL uno de sus principales activos estratégicos es la información, resultado de la prestación de servicios para la comunidad, como entidad de salud, por lo cual es fundamental generar y mantener un compromiso de protección de la información relevante orientada hacia la continuidad del negocio, administración de riesgos y consolidación de una cultura de seguridad.

Acorde a esta estrategia, surge el presente manual como herramienta institucional para concienciar a cada uno de los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos, lo que permite identificar y minimizar los riesgos a los cuales se expone la información, reducir costos operativos, financieros y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Todos los colaboradores, contratistas, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la organización, deben adoptar y cumplir los lineamientos del presente documento con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

Se establecerán políticas específicas de seguridad de la información como mecanismo de soporte a la Política Global de Seguridad de la Información de la FOSCAL - FOSCAL INTERNACIONAL.

6.1. COMPROMISOS DE LA DIRECCIÓN

La Gerencia aprueba las normas específicas de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de mecanismos de protección eficientes que garanticen la seguridad de la Información de la organización.

Compromiso demostrado a través de:

- Revisión y aprobación de las políticas de seguridad de la información permanentemente.
- Promoción activa de una cultura de seguridad
- Divulgar y facilitar su adopción a todos los colaboradores de la organización
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información
- La verificación del cumplimiento de las políticas estipuladas.

6.2. NORMAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.2.1. Norma de administración de la División de Tecnología e Innovación

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información por parte de la División de Tecnología e Innovación.
Directrices

- Los usuarios no deben dar a conocer su clave de usuario a terceros sin previa autorización de la División de Tecnología e Innovación
- Los usuarios y claves de los administradores de sistemas son de uso personal e intransferible.
- La División de Tecnología e Innovación debe emplear obligatoriamente las claves o contraseña con un alto nivel de complejidad.
- Los documentos y en general la información de procedimientos, seriales, software, etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.

- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ejemplo: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Para realizar instalación o distribución de software, solo se instalarán productos con licencia y software autorizado.
- La División de Tecnología e Innovación no debe otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del jefe inmediato y debe quedar constancia de dicha disposición.
- La División de Tecnología e Innovación no utilizará la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad.
- El acceso a cualquier servicio o sistema de información debe ser autenticado y autorizado.

6.2.2. Norma de clasificación de la información

Objetivo: Asegurar que la información recibe el nivel de protección apropiado, La FOSCAL - FOSCAL INTERNACIONAL definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, teniendo como referente la Política de Tratamiento de Información, documento que sirve para la clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.
Toda la información debe ser identificada, clasificada y documentada de acuerdo con los lineamientos establecidos por la organización.
Directrices:

- Los colaboradores deben implementar los parámetros definidos por la organización para la clasificación de la información referente al acceso, divulgación, almacenamiento, copia y eliminación de la información.
- La información física y digital de las áreas debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Cuando se imprima, escanee y saque copias, importante verificar las áreas adyacentes a impresoras, escáneres, y fotocopiadoras para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres y fotocopiadoras, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Todos los colaboradores deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.
- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que se genere, como, por ejemplo: Formularios, comprobantes, información en los sistemas, equipos informáticos, medios magnéticos, electrónicos o medios físicos como papel.
- Los usuarios responsables de la información deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

6.2.3. Norma específica para usuarios

Objetivo: Definir pautas generales para asegurar una adecuada protección de la información por parte de los usuarios de la organización.
Directrices:

- La División de Tecnología e Innovación ha definido diferentes medios o alternativas de almacenamiento de la información con los permisos necesarios para que la institución guarde toda la información que crea importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado, esta información será guardada por un periodo de 20 años; es de aclarar que los funcionarios responsables deberán copiar la información necesaria en la ubicación o ruta destinada para este fin.
- La División de Tecnología e Innovación instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin respectiva licencia y autorización de la División de Tecnología e Innovación (Imágenes, videos, software o música), obtenidos a partir de otras fuentes (Internet, dispositivos de almacenamiento externo), pueden implicar amenazas legales y de seguridad de la información para la organización, por lo que esta práctica no está autorizada.
- Todo el software usado en la plataforma tecnológica debe tener su respectiva licencia y acorde con los derechos de autor.
- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, Pendrive, etc.) pueden ocasionalmente generar riesgos para la institución al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informativos o pueden ser utilizados para la extracción de información no autorizada. Se requiere de previa autorización por el área encargada.
- Los programas instalados en los equipos, son propiedad de la FOSCAL - FOSCAL INTERNACIONAL, la copia no autorizada de programas o de su documentación, implica violación de las políticas institucionales. Aquellos funcionarios que utilicen copias no autorizadas de programas o su respectiva documentación, quedará sujeto a las acciones disciplinarias pertinentes.
- Los recursos tecnológicos y de software asignados a los trabajadores son responsabilidad de cada uno de ellos.
- Los funcionarios son los responsables de la información que administran en sus equipos y deben abstenerse de almacenar en ellos información no institucional.
- Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listas, etc., los cuales son el resultado de los procesos informáticos.
- Los dispositivos electrónicos (Computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la organización.
- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la División de Tecnología e Innovación.
- Los jefes de las diferentes áreas, en conjunto con la División de Tecnología e Innovación deben propiciaran actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial.
- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados

6.2.4. Norma de disponibilidad de la información, medios y equipos

Objetivo: Evitar las interrupciones en las actividades y proteger los procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación continua.
Directrices:

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección física y lógicas, que permitan su monitoreo y correcto funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

6.2.5. Norma para el manejo de medios removibles

Objetivo: Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.
Directrices:

- Se encuentra restringida la conexión a la infraestructura tecnológica (servidores, computadores, impresoras, scanner y demás dispositivos de tecnologías de la información) de FOSCAL – FOSCAL INTERNACIONAL de cualquier elemento de almacenamiento como dispositivos USB, discos duros externos, CD, DVD, cámaras fotográficas o de video, teléfonos celulares, tabletas, entre otros dispositivos no institucionales. Las excepciones especiales serán autorizadas por la Jefatura de Tecnológica e Innovación.
- Los medios de almacenamiento removibles autorizados, así como los medios impresos que contengan información Institucional, deben ser controlados y físicamente protegidos mediante algún mecanismo de cifrado que garantice su integridad y confidencialidad.
- Cada medio removible de almacenamiento autorizado deberá estar identificado de acuerdo con el tipo de información que almacene.

6.2.6. Norma de uso de los activos

Objetivo: Lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos a los colaboradores finales que deben administrarlos de acuerdo a sus roles y funciones.
Directrices:

- Los activos de información pertenecen a FOSCAL - FOSCAL INTERNACIONAL y el uso de los mismos debe emplearse exclusivamente para propósitos laborales.
- El personal que labora deberá utilizar únicamente los programas y equipos autorizados por División de Tecnología e Innovación
- FOSCAL - FOSCAL INTERNACIONAL proporcionará al usuario los equipos informáticos y los programas instalados; los datos y la información creada, almacenada y recibida de cada funcionario debe ser exclusivamente de uso laboral.
- La División de Tecnología e Innovación efectuará revisión de los programas utilizados en cada dependencia periódicamente.
- Todos los requerimientos de aplicativos, sistemas y equipos deben ser solicitados con su correspondiente justificación para analizar su viabilidad.
- Los colaboradores no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos.
- Los colaboradores no podrán efectuar ninguna de las siguientes labores sin previa autorización:
  - Instalar software en cualquier equipo.
  - Bajar o descargar software de internet.
  - Modificar, revisar, transformar o adaptar cualquier software propiedad de la entidad.
  - Copiar o distribuir cualquier software de propiedad de la organización.
- El funcionario debe informar a su superior o jefe inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento.
- El funcionario será responsable de todas las operaciones o acciones efectuadas con su cuenta de usuario.
- Ningún funcionario deberá acceder utilizando una cuenta de usuario o clave de otro colaborador.
- Cada funcionario es responsable de asegurar que el uso de redes externas, no comprometa la seguridad de los recursos informáticos.
- Todo archivo o material recibido a través de los diferentes medios o descarga, deberán ser analizados para detección de virus.
- Los trabajadores no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o CPU
- El funcionario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en caso de robo, pérdida o extravió del mismo y deberá dar aviso al área encargada.
- Está prohibido mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar, o desinstalar dispositivos, ni retirar sellos de los mismos sin autorización.

- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, estos deberán ser notificados por lo menos con una semana de anticipación a la División de Tecnología e Innovación para establecer el plan detallado de movimientos y acciones a ejecutar.
- El equipo de cómputo o cualquier recurso de tecnología que sufra algún daño por maltrato, descuido o negligencia por parte del colaborador, deberá ser cubierto el valor de la reparación o reposición por el mismo colaborador.
- La instalación de software en los equipos suministrados por la empresa, es una función exclusiva de la División de Tecnología e Innovación
- Los usuarios no deben mantener almacenados en los discos duros archivos de video, música y fotos que no sean de carácter institucional
- En el disco C:\ se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario no debe realizar modificaciones de estos archivos.
- La División de Tecnología e Innovación no prestará servicio de soporte técnico a equipos que no sean FOSCAL - FOSCAL INTERNACIONAL.

6.2.7. Norma de respaldo y restauración de la información

Objetivo: Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se puedan recuperar después de una falla.
Directrices:

- La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento.
- Definir la frecuencia de respaldo y los requerimientos de seguridad de la información.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus, defectos en discos de almacenamiento, problemas en equipos, catástrofes y por requerimiento legal.
- Desarrollar planes de emergencia para todas las aplicaciones que manejen información crítica.
- Debe existir al menos una copia de la información de los discos, fuera de las instalaciones de la FOSCAL - FOSCAL INTERNACIONAL.

6.2.8. Norma de manejo y protección de la información

Objetivo: Todos los colaboradores, consultores, contratistas y terceras partes que manejen información de la empresa, están obligados a salvaguardarla en los sitios dispuestos para tal fin, para garantizar la disponibilidad, confidencialidad y respaldo de la misma.
Directrices:

- Responsabilidad de uso: La institución pone al servicio de los trabajadores el uso de los medios necesarios para el normal desarrollo de las labores propias del cargo para lo cual adopta y comunica las políticas de uso aceptable, controles y medidas dirigidas a garantizar la seguridad y continuidad del servicio que presta. Es deber de los colaboradores acogerlas con integridad y dar a los recursos uso racional y eficiente.
- La institución, en respeto de los principios de libertad de expresión y privacidad de información, no genera a los colaboradores ninguna expectativa de privacidad en cualquier elemento que almacene, envié o que reciba por medios electrónicos que sean propiedad de la empresa. En consecuencia, podrá denegar el acceso a los servicios electrónicos, inspeccionar, monitorear y cancelar servicios asignados como correo electrónico, navegación en Internet y recursos compartidos, entre otros.
- Los usuarios de los servicios electrónicos aceptan y convienen que la institución puede conservar y revelar el contenido del correo si así le es requerido por ley o si de buena fe considera que dicha reserva o revelación es necesaria para: (a) cumplir con procesos legales, (b) responder a quejas de que algún contenido viola los derechos de terceras personas, o (c) proteger los derechos, propiedad o seguridad personal de la empresa, sus usuarios y el público en general.
- La violación de los controles de seguridad o el incumplimiento de las Políticas de la institución por parte de los colaboradores dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

6.2.9. Normas específicas para webmaster o área encargada de las comunicaciones

Objetivo: Proteger la integridad de las páginas web institucionales, el software y la información contenida.
Directrices:

- Los responsables de los contenidos de las páginas web, deben preparar y depurar la información, deben disponer de un archivo actualizado con la información de la página inicial del sitio.
- Las claves de acceso de los responsables de los contenidos de las páginas web son estrictamente confidenciales, personales e intransferibles.

6.2.10. Norma de uso de internet

Objetivo: Establecer lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los colaboradores.
Directrices:

- El acceso a Internet y a los servicios asociados que proporciona la institución deberán utilizarse para los propósitos de la propia empresa, de acuerdo con las atribuciones y funciones laborales del colaborador, establecidas en el manual de procedimientos.
- Cuando el trabajador haga uso del servicio de Internet, deberá mantener un comportamiento de acuerdo con los principios éticos establecidos por FOSCAL - FOSCAL INTERNACIONAL, esto es, abstenerse de realizar cualquier actividad que a continuación se describe:
  - Realizar cualquier actividad intencional que provoque problemas con el funcionamiento de las redes, con otros usuarios, canales de comunicación, sistemas y equipos, como, por ejemplo, propagar un virus informático.
  - Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible para la organización.
  - Visitar en horarios laborables sitios que no tengan relación con las funciones de su trabajo, así como consultar, enviar, propagar o promover material o sitios que vayan contra la moral y las buenas costumbres, o que constituya o fomente un comportamiento que dé lugar a responsabilidades civiles, administrativas o penales.
  - Visitar sitios de chat, que no tengan relación con actividades propias de la empresa.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de FOSCAL - FOSCAL INTERNACIONAL o que representen peligro para la empresa como: pornografía, terrorismo, segregación racial u otras fuentes.
- La descarga de archivos de internet debe ser con propósito laborales y de forma razonable para no afectar el servicio de internet/intranet.

6.2.11. Norma de uso de mensajería instantánea y redes sociales

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería y de redes sociales por parte del personal autorizado.
Directrices:

- El uso de servicios de mensajería instantánea y el acceso a redes sociales estará autorizado solo a un grupo de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación.
- No se permite él envió de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
- La información que se publique o divulgue por cualquier medio de internet, de cualquier funcionario se considera fuera del alcance y por lo tanto la confiabilidad, integridad, disponibilidad, daños y perjuicios que pueda ocasionar será responsabilidad de la persona que las haya generado

6.2.12. Norma de uso de impresora y del servicio de impresión

Objetivo: Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Directrices:

- Los documentos que se impriman en las impresoras deben ser de carácter institucional
- Es responsabilidad del funcionario conocer el adecuado manejo de los equipos de impresión para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de falla comunicarle al área responsable

6.2.13. Norma de seguridad del centro de datos y cuartos de cableado

Objetivo: Asegurar la protección de la información en las redes y la protección de infraestructura de soporte
Directrices:

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar control de ingreso y salida del personal que visita el centro de datos.
- Cuando se realicen actividades en el centro de datos o cuartos de cableado es necesario que personal de la División de Tecnología e Innovación este presente.
- Se debe garantizar que el control de acceso al centro de datos, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.
- La División de Tecnología e Innovación deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del personal designado por la División de Tecnología e Innovación y debe efectuarse en presencia de un funcionario de la División de Tecnología e Innovación el cual le indicará las precauciones mínimas a seguir durante el proceso de limpieza.
- No se permite el ingreso de algún tipo de alimentos o bebidas en el centro de datos.
- El centro de datos debe estar provisto de:
  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión.
  - Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, para garantizar el servicio de energía eléctrica durante una falla.
  - Alarmas de detección de humo y sistemas automáticos de extinción de fuego.
  - Extintores de incendios o un sistema contra incendio debidamente probado y con la capacidad de detener el fuego.
  - El cableado de red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
  - Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
  - Las actividades de soporte y mantenimiento siempre deben estar supervisadas por el área encargada.
  - Las puertas del centro de datos deben permanecer cerradas.
  - Cuando se requiera realizar alguna actividad sobre algún armario, este debe quedar ordenado, cerrado y con llave al finalizar la misma
  - Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar fallas que se puedan presentar

6.2.14. Norma de seguridad de los equipos

Objetivo: Asegurar la protección de la información en los equipos
Directrices:

- Protecciones en el suministro de energía. A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, y pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área competente.
- Seguridad del cableado.
  - Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

- Deben existir planos que describan las conexiones del cableado
- El acceso a los centros de cableado debe estar protegido.

- Mantenimiento de equipos
  - Se debe mantener contratos de soporte y mantenimiento de los equipos críticos.
  - Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
  - Las actividades de mantenimiento que puedan ocasionar una suspensión en el servicio deben ser realizadas y programadas.
  - Los equipos que requieran salida de las instalaciones para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como critica.
  - Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda la información.

6.2.15. Norma de suministros de energía

Objetivo: Establecer los lineamientos para reducir las fallas en el suministro de energía u otras anomalías eléctricas, en la infraestructura tecnológica de la institución.
Directrices

- Disponer de múltiples líneas de suministro para evitar un único punto de falla en el suministro de energía.
- Contar con un suministro de energía ininterrumpido (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones institucionales.
- Contar con una planta eléctrica de respaldo para los casos en que el procesamiento deba continuar ante una falla prolongada en el suministro de energía.
- Implementar protección contra sobrecargas eléctricas en toda la institución y líneas de comunicaciones de acuerdo con las normativas vigentes.
- Contar con iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.

6.2.16. Norma de escritorio y pantalla limpia

Objetivo: Definir pautas generalas para reducir el riesgo de acceso no autorizado, perdida y daño de la información
Directrices:

- El personal debe conservar su escritorio libre de información, propia de la institución que pueda ser alcanzada, copiada o utilizada por terceros sin autorización.
- El personal debe bloquear la pantalla de su computador en los momentos que no esté utilizando el equipo o que deba ausentarse de su puesto de trabajo.
- Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente.
- En el momento de dejar o identificar un equipo desatendido se debe bloquear usando la combinación de teclas: Windows + L.

6.2.17. Norma de uso de correo electrónico

Objetivo: Definir pautas generales para asegurar una adecuada protección de la información, en el uso del correo electrónico por parte de los colaboradores.
Directrices:

- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o uso del correo que puedan comprometer la seguridad de la información
- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada y no para otra finalidad
- El usuario de este servicio deberá mantener una imagen y comportamiento profesional cuando haga uso del correo electrónico, deberá abstenerse de realizar cualquiera de las actividades que a continuación se describen:

- No está autorizado, él envió de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la organización.
- Enviar cadenas de mensajes a un grupo de colaboradores.
- Compartir o divulgar números de cuenta, claves de acceso y número de identificación personal u otra información confidencial o sensible de la organización.

- Con el propósito de contar con niveles de seguridad apropiados, el colaborador deberá manejar la contraseña de acceso al correo electrónico institucional con privacidad. En caso de que el colaborador requiera de cambio de contraseña, ésta deberá ser solicitada al área de la siguiente forma:
  - Deberá ser solicitada a través de los diferentes medios disponibles para soporte
  - Al digitar las claves de acceso no permitir que otros colaboradores observen cuáles son ni las comente con nadie.
- Los colaboradores deben realizar limpieza de sus buzones de correo periódicamente.

6.2.18. Norma de establecimiento, uso y protección de claves de acceso

Objetivo: Controlar el acceso a la información.
Directrices:

- Los usuarios son responsables del uso de las claves o contraseñas de acceso asignadas para la utilización de los equipos o servicios informáticos.
- Los usuarios deben tener en cuenta los siguientes aspectos:
  - No incluir contraseñas en ningún proceso de registro automatizado.
  - Se debe realizar cambio de contraseña cada periódicamente para el correo electrónico
  - Las claves deben poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de hijos, placas de automóvil etc.
  - Deben tener mínimo 8 caracteres alfanuméricos, mayúsculas, minúsculas y caracteres especiales.
  - Cada vez que se cambien las contraseñas deben ser distintas por lo menos de las últimas tres.
  - No registrarlas en papel, archivos digitales o dispositivos manuales.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la FOSCAL - FOSCAL INTERNACIONAL.
- Todo cambio en roles, funciones o cargo que requiere asignar al usuario atributos para acceso a diferentes prestaciones de la infraestructura tecnológica en la institución debe ser notificado a la División de Tecnología e Innovación por el jefe de área para su aprobación.

6.2.19. Norma de control de acceso a sistemas y aplicaciones

Objetivo: Asegurar, preservar y garantizar el control de acceso a los sistemas y/o aplicaciones institucionales.
Directrices:

- El acceso a los sistemas y servicios tecnológicos de la institución, a través del uso de usuario de dominio, debe estar restringido y delimitado a las tareas, funciones, responsabilidades y obligaciones que ejecuten los funcionarios, pasantes y terceros de la institución.
- El responsable de la aplicación y de la información, deberá identificar y documentar explícitamente la sensibilidad o confidencialidad de la información contenida en los sistemas de información y/o aplicaciones de la institución.
- No está permitido a los funcionarios, pasantes y terceros, acceder a los sistemas de información y/o aplicaciones para el no haya sido autorizado.
- El área responsable de los servicios y/o aplicaciones debe seguir los siguientes lineamientos:
  - Asegurar los grupos de servicios de información, usuarios y sistemas de información
  - Establecer los controles de acceso a los ambientes de producción de los sistemas de información
  - Asegurarse que los desarrolladores internos o externos; posean acceso limitado y controlado a los datos y archivos que se encuentran en los ambientes de producción de la institución.

- Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.
- Asegurar que en lo que respecta a los sistemas operativos, sistemas de información y/o aplicaciones de la institución, se bloquee la sesión automáticamente después de determinado tiempo de inactividad.
- En lo que respecta a la autorización y continuidad en el uso de los usuarios de los aplicativos, deberá ser responsabilidad de cada una de las áreas, dependencias y/o procesos de la institución.

6.2.20. Norma Seguridad Perimetral

Objetivo: Establecer los recursos de seguridad en el perímetro externo de la red y a diferentes niveles, garantizando confianza en los servicios y accesos requeridos para las funciones de la institución.
Directrices:

- La División de Tecnología e Innovación implementará soluciones lógicas y físicas que garanticen la protección de la información de la institución de posibles ataques internos o externos
- Rechazar conexiones a servicios comprometidos
- Permitir sólo cierto tipo de tráfico, por ejemplo: correo electrónico, https.
- Proporcionar un único punto de interconexión con el exterior.
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información como nombres de sistemas, topologías de la red, tipos de dispositivos de red, cuentas de usuarios internos, entre otros.

6.2.21. Norma Seguridad en las Redes

Objetivo: asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.
Directrices:

- Los sistemas deben permitir llevar un registro y seguimiento para detectar acciones que puedan afectar la seguridad de la información.
- Se deben controlar los accesos a servicios internos y externo conectados en red
- La División de Tecnología e Innovación, como responsable de las redes de datos y los recursos de red de la institución, deben velar por dichas redes sean debidamente protegidas contra acceso no autorizados a través de mecanismo de control de acceso lógico.
- La División de Tecnología e Innovación, debe implementar mecanismos de control a través de segmentación de redes en función de los grupos y servicios.
- La División de Tecnología e Innovación, debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica con el fin de reducir el acceso no autorizado y evitar cambios inadecuados sobre los servicios de TI (servicios de red, acceso a sistemas de información, servicios de internet).
- La División de Tecnología e Innovación, debe asegurar que las redes inalámbricas de la institución, cuenten con mecanismos de autenticación para evitar accesos no autorizados.

6.2.22. Norma de Uso de Redes Privadas Virtuales (VPN)

Objetivo: Establecer lineamientos de seguridad a conexiones que se encuentran fuera de la red interna privada.
Directrices:

- Para que un funcionario o proveedor de la FOSCAL - FOSCAL INTERNACIONAL pueda acceder a los equipos, ya sean servidores y otros equipos de la red interna de la FOSCAL - FOSCAL INTERNACIONAL desde una conexión externa con la tecnología VPN, deberá cumplir con los siguientes lineamientos:
  - Solicitud formal a través de los medios establecidos por la División de Tecnología e Innovación, incluyendo la justificación para la solicitud de este acceso e indicar el tiempo requerido para el mismo.
  - Evaluación y aprobación de la solicitud elevada a la División de Tecnología e Innovación.

- La División de Tecnología e Innovación se encarga de instalar y configurar el software necesario para las conexiones remotas a través de VPN
- El funcionario que solicite una VPN es responsable del acceso remoto y del uso de este.

6.2.23. Norma de Teletrabajo o Trabajo Remoto

Objetivo: Establecer lineamientos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza el trabajo.
Directrices:

- Suministrar a las personas que realizan trabajo remoto equipos para la ejecución de sus obligaciones (cuando a ello haya lugar) o autorizar la utilización de equipos personales para dicha función, siempre y cuando cumpla y acepten los mecanismos y medidas de Seguridad de la información definidos por la institución.
- La División de Tecnología e Innovación es responsable del licenciamiento del software de los equipos suministrados para las actividades de teletrabajo
- La División de Tecnología e Innovación no prestará ningún tipo de soporte por fallos de manejo en los equipos personales, que no estén relacionados con los servicios a través d ellos cuales accede al trabajo remoto. Ejemplo: NO - Ofimática, Antivirus, actualizaciones, lentitud del equipo. SI – Uso de VPN, Google Workspace, Aplicaciones y software institucional a las cuales va acceder.
- Dar a conocer a los usuarios los lineamientos a través de la presente política y con ello los riesgos de su que se derivan por el uso de equipos tecnológicos para la Seguridad de la Información de la institución.
- Definir los tipos de usuario que dispondrán la modalidad de teletrabajo y los permisos de acceso remoto pertinentes.
- Establecer un procedimiento de conexión remota de emergencia para solventar problemas e incidencias puntuales (En caso de existir alternativas o medios de conexión).
- La División de Tecnología e Innovación llevará seguimiento de las conexiones remotas para prestar atención a los intentos de conexiones sospechosas o no autorizadas.
- El usuario que realice labores de teletrabajo deberá cumplir con los siguientes lineamientos
  - No Cumplir con las políticas establecidas en este manual
  - Contar con sistema operativo licenciado y actualizado
  - Tener software antivirus licenciado y actualizado
  - Mantener las aplicaciones actualizadas
  - Mantener configuraciones seguras en aplicaciones (navegación web, correo electrónico, etc.)
  - Parametrizar el bloqueo automático por inactividad y en lo posible, utilizar un cifrado de disco
  - No facilitar a otra persona las credenciales de acceso o el perfil de acceso a los servicios o recursos tecnológicos de la institución.
- Es importante que para el transporte de equipos entre la oficina y el lugar o lugares donde se ejecute el teletrabajo o trabajo remoto disponer de elementos que permita una buena resistencia a caídas, golpes, aplastamiento, derrame de líquidos u otro riesgo al que se encuentre expuesto el equipo.
- No utilizar equipos portátiles asignados por la institución o personales en conexiones poco confiables como, por ejemplo: Redes Wifi abiertas, redes públicas de hoteles, biblioteca, auditorios, aeropuertos, entre otros)

6.2.24. Norma de Seguridad Física y del Entorno

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información e instalaciones de procesamiento de la información.
Directrices:

- Las áreas y dependencias de la institución deben encontrarse protegidas por controles físicos, monitoreados y supervisados. La institución define las siguientes áreas seguras:
  - Datacenter: Centro de procesamiento de datos en donde se encuentras sistemas de información, componentes de telecomunicaciones y los sistemas de almacenamiento (Servidores físicos y virtuales).

- Centros de cableado: espacios que se usan para conectar los dispositivos de la red LAN donde se encuentran paneles de conexión, Switches, Router, entre otros.
- Cuartos de suministro: Áreas donde se ubican los servicios de suministro como las UPS y plantas eléctricas.
- Archivo físico central: Área donde se administra, custodia y conserva los documentos físicos con valor administrativo, legal, permanente, histórico entre otros que son transferidos por las diferentes dependencias de la institución.
- Archivo físico de gestión: Aquella documentación en trámite que conservan las diferentes dependencias de la institución, así como aquella que aún después de finalizado el procedimiento, está sometida a uso continuo y de consulta, aplicando para ello lo dispuesto en las tablas de retención documental
- Oficinas: Todas aquellas áreas de la institución, que por sus competencias funcionales manejan información sensible y confidencial, serán consideradas áreas seguras, para lo cual debe adoptarse los mecanismos para asegurar dicha información.

- El acceso al datacenter está restringido y su ingreso es únicamente para el personal autorizado por la División de Tecnología e Innovación.
- Para acceder a los centros de cableados y cuartos de suministros, se debe diligenciar la bitácora de ingreso y salida. Esto debe aplicarse para los funcionarios, contratistas, proveedores y terceros autorizados por la División de Tecnología e Innovación.
- Todos los funcionarios, contratistas, pasantes, proveedores y terceros deben presentar su carné para el ingreso a las instalaciones de la institución.
- Los visitantes y pacientes deben presentar la documentación necesaria para el ingreso y en los casos donde se requiera realizar el registro de ingreso.

6.2.25. Norma de Seguridad para servicios de Cloud Computing y Hosting

Objetivo: Establecer los lineamientos específicos de seguridad de la información asociados a estos ambientes con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la institución.
Directrices:

- Para el despliegue e implementación de servicios en Cloud Computing y/o Hosting se deben tener en cuenta los requerimientos y lineamientos de seguridad establecidos por la institución.
- El proveedor de Servicios debe tener en funcionamiento una organización responsable de la seguridad de la información, en la que se defina los roles y responsabilidades frente a la seguridad de la información y deberá definir un rol dentro de la Organización que sea el punto de contacto oficial para todos los temas relacionados con la Seguridad de la Información que es de alcance del servicio contratado.
- El proveedor debe garantizar la realización de copias de respaldo periódicas a los datos que se encuentran en el alcance del servicio contratado y en el formato utilizado, definido y aprobado por la Institución de manera que permitan recuperar la información
- El proveedor de servicio deberá tener implementado un sistema de gestión de riesgo de seguridad de la información, comunicando a la institución sobre el análisis de los controles establecidos, así como de los planes o medidas de mitigación de los riesgos identificados.
- El proveedor debe establecer mecanismos que permitan contar con conexiones seguras de entre la institución y las aplicaciones y/o servicios ofrecidos por el proveedor.
- La institución y el proveedor deben establecer roles o niveles de acceso de acuerdo a las actividades, responsabilidades y necesidades de los diferentes usuarios; y se deben otorgar permisos de acceso a los recursos informáticos en función a los roles definidos.
- La institución es la dueña de la información a ser procesada por el proveedor independiente del modelo de despliegue o de servicio contratado.
- La información de las bases de datos en soluciones sobre Cloud y/o Hosting debe ser protegida mediante el uso de mecanismos de cifrado.
- El Proveedor de Cloud Computing y/o Hosting debe emplear una llave de cifrado diferente para cada cliente de sus servicios.

- El Proveedor deberá presentar a la institución su plan de continuidad para garantizar que puedan prestar sus servicios ante eventos de desastre o interrupciones mayores.

6.2.26. Norma de Seguridad para servicios de Videoconferencia

Objetivo: Establecer los lineamientos específicos de seguridad de sobre las herramientas de comunicación definidas por la institución para la realización de reuniones virtuales.

Directrices:

- El software debe provenir de los repositorios verificados y autenticados. Se debe tener instalada la aplicación correcta,
- Las conexiones entrantes deben ser aceptadas por el usuario que realizó el agendamiento de la reunión, no debe existir la posibilidad de autorrespuesta.
- Debe ofrecer la posibilidad de acceder a la sesión con o sin video/audio.
- En las reuniones, no compartas información personal, como contraseñas números de cuentas bancarias o números de tarjetas de crédito, ni siquiera tu fecha de nacimiento.
- Las sesiones de vídeo deben cumplir con los siguientes requisitos relativos a la seguridad en las comunicaciones:
  - Utilizar canales seguros TLS 1.2 en las llamadas cifradas para la señalización y AES 128 o 256 en el tráfico de media.
  - Recomendable el tráfico SRTP para audio, vídeo y contenido (media) con cifrado AES-128
  - Asegurar con cifrado AES-128 el tráfico UDP.
  - Verificación en dos pasos: Admitimos varias opciones de verificación en dos pasos (2SV) para Meet, como las llaves de seguridad, Autenticador de Google, los mensajes de Google y los SMS.
- Según los lineamientos establecidos en el Manual y Política de Tratamiento de Datos para asegurar la confidencialidad de los datos al momento de realizar intercambio de documentos o información.
- Programa de Protección Avanzada: Los usuarios de Meet pueden inscribirse en el Programa de Protección Avanzada (APP) de Google. El APP ofrece las protecciones más sólidas que tenemos disponibles contra la suplantación de identidad (phishing) y la usurpación de cuentas. Además, está específicamente diseñado para las cuentas de mayor riesgo y no hay ningún caso de ataques de suplantación de identidad (phishing) exitosos entre los participantes del APP, incluso aunque a los participantes se les hayan orientado esos ataques en repetidas ocasiones
- Para la herramienta Google Meet se establecen las siguientes medidas de seguridad y privacidad:
  - Se prohíbe la unión o acceso de usuarios anónimos a las reuniones.
  - Cifrado de todos los datos de forma predeterminada entre el cliente y Google tanto desde los navegadores como desde las aplicaciones Meet para sistemas operativos Android y iOS.
  - Los participantes no pueden unirse a la reunión con más de 15 minutos de antelación al horario programado.
  - Solo los usuarios que figuren en la invitación de calendario pueden ingresar a la reunión sin una solicitud explícita para unirse. Quienes no figuren en la invitación de calendario deberán solicitar permiso para unirse, y esperar a que el organizador de la reunión acepte la solicitud.
  - Solo el organizador de la reunión puede admitir a los participantes que no figuren en la invitación de calendario (deberá invitar a las personas desde la reunión y aceptar las solicitudes para unirse).
  - Los organizadores de la reunión pueden acceder fácilmente a los controles de seguridad, como las opciones para silenciar y quitar participantes, y solo ellos pueden realizar esas acciones directamente desde la reunión.
  - Meet impone límites con respecto a la cantidad de posibles vectores de abuso.
  - Los usuarios pueden denunciar comportamientos abusivos en las reuniones.
- Medidas de cifrado para Google Meet para garantizar la seguridad y privacidad de los datos
  - De forma predeterminada, todos los datos de Meet se encriptan en tránsito entre el cliente y Google en las videoconferencias que se realizan desde un navegador web, en las apps de Meet para Android y Apple® iOS®, y en las salas de reuniones que cuentan con el hardware de salas de reuniones de Google.

- Las grabaciones de Meet que se almacenan en Google Drive se encriptan en reposo de forma predeterminada.
- Meet cumple con los estándares de seguridad del Grupo de Trabajo de Ingeniería de Internet (IETF) para la seguridad de la capa de transporte de los datagramas (DTLS) y el protocolo de transporte seguro en tiempo real (SRTP).

6.2.27. Norma de Control de Acceso a Sistemas de Información y Plataformas Tecnológicas

Objetivo: Establecer los lineamientos específicos de seguridad al personal autorizado sobre el acceso a los sistemas de la información de la institución.
Directrices:

- Los responsables de la administración de los sistemas deben verificar los privilegios de acceso de los usuarios de acuerdo a los requerimientos o necesidades laborales.
- La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.
- Los privilegios de acceso asignados a los usuarios deben ser revisados por lo menos una vez al año por los responsables de la administración de los sistemas.
- Todas las cuentas de usuario son personales e intransferibles.
- Los usuarios deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.
- Las contraseñas de los diferentes sistemas de información son personales e intransferibles, cada usuario es responsable de su uso y preservar su confidencialidad.
- Los usuarios tiene la responsabilidad de cambiar su contraseña o solicitar el cambio, si es el caso, en el evento que fuese revelada o existiese alguna sospecha de ello.
- Todos los usuarios deben seguir los lineamientos para la creación de contraseñas seguras descritas en el presente manual.
- El acceso remoto a sistemas de información y plataformas de tecnología de la debe ser realizado a través de VPN u otros medios que garanticen la seguridad en la comunicación.

6.2.28. Norma de Adquisición, desarrollo y mantenimiento de sistemas de información

Objetivo: Asegurar los sistemas de información y aplicativos en sus fases de planeación, adquisición, desarrollo, implementación y operación.
Directrices:

- Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo o sistema, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.
- Se deben incorporar los lineamientos de seguridad informático los requisitos de seguridad para los diferentes a sistemas y aplicativos.
- La contratación de un desarrollo a medida, adquisición de software o sistemas de información debe incluir entrenamiento en administración de las funciones de seguridad de dichas aplicaciones.
- La contratación de un desarrollo a medida, adquisición o modificación de software o sistemas de información debe incluir la entrega de la documentación y la transferencia de conocimiento técnico y operativo suficiente al personal encargado de la administración y soporte.
- Identificar los requisitos previos para el desarrollo o soporte de sistemas de información y aplicativos que incluyan:
  - Aseguramientos de la disponibilidad y continuidad del servicio
  - Documentación del código fuente.
  - Requisitos de seguridad listados en instructivos del sistema de información o aplicativo.
  - Verificaciones de seguridad sobre los sistemas de información o aplicativos.
- Se debe verificar que el procesamiento de los sistemas de información y aplicativos es el adecuado, tanto en ambiente de pruebas como en producción.

- Las vulnerabilidades técnicas deber ser objeto de un procedimiento de gestión orientado a la remediación de las mismas.
- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información
- Solo el personal de desarrollo de software debe tener acceso al código fuente o en su defecto el jefe del área de Tecnología e Innovación.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por Dirección de Tecnología e Innovación.
- La Dirección de Tecnología e Innovación en conjunto con la Coordinación de Seguridad Informática deben verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.

6.2.29. Norma de Seguridad Asociado a los Servicios de Red

Objetivo: Establecer las responsabilidades y conceptos necesarios para implementar mecanismos de seguridad en el entorno de los servicios de red de la organización.
Directrices:

- Se debe tener documentación de la identificación de los activos más importantes para la organización que pueden incluir:
  - Datos personales.
  - Información.
  - Procesos.
  - Aplicaciones.
  - Bases de Datos.
  - Sistemas operativos.
  - Sistemas de información.

- Identificar las vulnerabilidades asociadas a la infraestructura de red y a los sistemas de información.
- Realizar registro y cuantificación de los riesgos en orden de importancia e impacto.
- Realizar revisión continúa de la información mediante la ejecución de auditorías de seguridad informática y de la información

6.2.30. Norma de Intercambio de Información

Objetivo: Establecer procedimientos y controles formales para proteger el intercambio de información que contiene datos personales.
Directrices:

- Proteger los datos intercambiados de la intercepción, copia, modificación, enrutamiento y destrucción.
- Proteger información sensible que se encuentre en forma de archivo adjunto.
- Tener protección contra el código malicioso que pueda ser transmitido a través del uso de transacciones telemáticas.
- Definir buenas prácticas en el uso de las instalaciones de comunicación electrónicas.
- Restringir y dar un uso seguro a las redes inalámbricas.
- Definir responsabilidades a los usuarios, contratistas y cualquier otro usuario para no ver comprometida la imagen de la organización, a través de difamación, hostigamiento, personificación, reenvío de cadenas y redes sociales.
- Usar técnicas criptográficas para proteger la confidencialidad, integridad y autenticidad de la información.
- Capacitar a los usuarios sobre las precauciones que deben tomar a la hora de transmitir información importante para la empresa.
- Establecer acuerdos de confidencialidad y no divulgación en el proceso de Intercambio de Información.

- Cuando se realicen acuerdos entre la organización y otras organizaciones o entidades, para el intercambio de información, se debe especificar el nivel de criticidad de la información involucrada y las consideraciones de seguridad sobre la misma, teniendo en cuenta los siguientes aspectos:
- Establecer procedimientos y responsabilidades para el control y notificación de transmisiones, envíos y recepciones.
- Definir y monitorear procedimientos para garantizar la trazabilidad y el no repudio.
- Establecer normas técnicas para el empaquetado y la transmisión.
- Asignar responsabilidades y obligaciones en caso de pérdida, mal uso y divulgación no autorizada de datos personales.
- Proteger la información y los medios físicos en tránsito.
- Se deben revisar periódicamente, o implementar en su ausencia, acuerdos de confidencialidad sobre la información que será intercambiada o transferida dentro de la organización y con entidades externas a ella.

6.2.31. Norma de Protección de datos en tránsito vía electrónica

Objetivo: Establecer los lineamientos para disminuir el riesgo que implica el uso de herramientas de mensajería con relación a la protección de datos personales.
Directrices:

- Los usuarios comunes no pueden tener derechos de instalación de programas en sus estaciones de trabajo.
- Se debe bloquear el acceso a servidores públicos conocidos de mensajería instantánea que no han sido autorizados por la organización para el desarrollo de las funciones. Cabe resaltar que esto solo ofrece una protección parcial debido a la gran cantidad de servidores públicos que existen.
- Realizar bloqueo de los puertos populares utilizados para mensajería instantánea.
- No compartir información que contenga datos personales a través de mensajería instantánea, salvo que exista previa autorización del responsable del tratamiento y se tomen las medidas de seguridad adecuadas.
- Proteger el correo electrónico contra ataques informáticos.
- Protección de archivos adjuntos de correo electrónico (cifrado).
- Uso de técnicas criptográficas para proteger la confidencialidad e integridad de la información.
- Implementar controles adicionales para aquellos mensajes de correo electrónico que no pueden ser autenticados.
- Se debe definir el alcance sobre el uso del correo electrónico institucional por parte del personal de la organización.

6.2.32. Norma de uso equipos fuera de la institución

Objetivo: Establecer los lineamientos que implica el uso de equipos de cómputo institucionales de fuera de las instalaciones de FOSCAL – FOSCAL INTERNACIONAL
Directrices:

- El departamento de tecnología e innovación al recibir una solicitud de traslado de un equipo informático fuera de la institución, se compromete:
  - Verificar el estado de los equipos tecnológicos para comprobar su salida y recepción en buen estado.
  - Verificar el plazo otorgado a los equipos tecnológicos que serán utilizados fuera de la institución.

- El compromiso de los usuarios al momento de solicitar el traslado del equipo fuera de la institución son los siguientes:
  - Solicitud y aprobación por el departamento de Tecnología e Innovación.
  - Reportar cualquier daño o deterioro de los equipos informáticos facilitados.
  - Responsabilizarse de cualquier pérdida o robo del equipo tecnológico.
  - Asumir las responsabilidades que procedan en caso de determinar responsabilidad en el daño o perdida del equipo informático.

7. CONTROLES CRIPTOGRÁFICOS

Es un conjunto de lineamientos que permiten a la organización proteger los datos personales sensibles de la pérdida de confidencialidad e integridad, mediante la aplicación de algoritmos de cifrado a aquellos datos o a la infraestructura de almacenamiento y comunicación de información que incluya datos personales.

7.1. OBJETIVO

Definir la implementación de algoritmos de cifrado y mecanismos de protección de información para proteger la confidencialidad e integridad de los datos personales a utilizar en los procesos de la organización.

7.2. ÁMBITO DE APLICACIÓN

Este documento es aplicable a todos los usuarios de la organización, ya sean trabajadores de planta, contratistas u otros trabajadores, incluyendo las empresas que le presten algún servicio a la FOSCAL – FOSCAL INTERNACIONAL.

7.3. RESPONSABLES

- Responsable de Tecnología e Innovación
  - Autorizar los métodos de cifrado a utilizar en los sistemas de información, aplicaciones, bases de datos y comunicaciones. Así mismo, administrar y salvaguardar las claves criptográficas y utilizar solo los algoritmos autorizados por las directivas de la organización.
  - Asignar funciones sobre la generación, cambio, transmisión, activación, utilización, almacenamiento y destrucción de las llaves criptográficas, es quien se encarga de establecer cuál es el algoritmo de cifrado más adecuado y acorde con los requerimientos de protección de datos personales y con las especificaciones técnicas de la organización.
  - Establecer los recursos técnicos necesarios para asegurar el almacenamiento de las llaves de cifrado, la capacidad de procesamiento necesaria para el cifrado y descifrado de información.

- Coordinadores de Área
  - Asignar los roles y determinar la criticidad de la información que necesita ser cifrada, seguir las recomendaciones del responsable de Tecnología de Innovación en cuanto a los algoritmos de cifrado, su implementación en los sistemas de información y la capacitación a los usuarios a los que se les ha asignado roles en los que tienen a su cargo información crítica que incluya datos personales y que deben usar cifrado en sus comunicaciones.

- Colaboradores
  - Cumplir con cada una de las definiciones y procedimientos establecidos por el responsable de Tecnología e Innovación y asistir a las capacitaciones en el uso y administración de las llaves criptográficas que se les han asignado.

7.4. POLÍTICA PARA CONTROLES CRIPTOGRÁFICOS

7.4.1. Normativa Institucional

En virtud de las operaciones de la FOSCAL – FOSCAL INTERNACIONAL, que en sus procesos realiza tratamiento de datos personales de especial protección (Datos de menores o datos sensibles), se debe definir la implementación de algoritmos

de cifrado y mecanismos de protección de información para proteger la confidencialidad, disponibilidad e integridad de los datos.

7.4.2. Controles Criptográficos

- Se deben utilizar técnicas de cifrado para garantizar la integridad, confidencialidad y no repudio de la información personal sensible.
- Se deben definir los algoritmos de cifrado que se van a utilizar en cada uno de los procesos de la organización, teniendo en cuenta el nivel de riesgo y criticidad de los datos personales que se tratan.
- Sólo se deben usar algoritmos de cifrados definidos por estándares internacionales, de tal manera que sean fiables y genere confianza en el uso de los sistemas de información y comunicaciones.
- Las contraseñas de acceso a los sistemas de información, datos y servicios de la organización, deben ser protegidas por medio de técnicas de cifrado.
- En caso de transmisión de información sensible por medio de redes públicas, se deben usar controles criptográficos.

7.4.3. Cifrado de Información

- El responsable de Tecnología e Innovación o el designado por el área, debe realizar una evaluación del riesgo y la clasificación de la información personal almacenada en las bases de datos según su criticidad, para identificar el nivel requerido de protección y definir el tipo y la calidad del algoritmo de cifrado que se debe implementar, tomando en cuenta la longitud de las claves a utilizar.
- Una vez clasificada la información personal, se debe cifrar toda aquella que sea considerada por la ley como de especial protección (datos personales sensibles), que pudiera estar expuesta a usuarios no autorizados, en relación a su integridad, disponibilidad y confidencialidad.

7.4.4. Certificados Digitales

- En las páginas web que se implementen formularios de captura de información personal, se deben adquirir certificados digitales de una Autoridad Certificadora confiable, con el fin de que la información no circule por la red en texto plano y, por tanto, sea susceptible a ser conocida o manipulada por terceros. En la medida de lo posible, a través del protocolo TLS 1.3 o superior y algoritmos de cifrado SHA3.
- Cuando existan relaciones contractuales con proveedores de servicios de hosting, se les debe exigir la implementación de certificados digitales en sus plataformas.

7.4.5. Gestión de Llaves de Cifrado

En este punto se establecen procedimientos para realizar una gestión adecuada de llaves de cifrado, con el fin de sostener el uso de las técnicas criptográficas, transmitir las llaves de cifrado por medio de canales seguros, tener una distribución adecuada entre los usuarios de los sistemas, asegurar el almacenamiento y conservación en forma segura de las llaves y definir procedimientos de generación y revocación de claves dentro de la organización.

Para llevar a cabo una correcta gestión de las llaves de cifrado se deben tener en cuenta los siguientes aspectos:

- Generación y cambio de claves
  - La criticidad de la información personal que se va a cifrar
  - Los recursos técnicos y la capacidad de cómputo de los equipos que hacen parte de los sistemas de información (estaciones de trabajo, servidores, etc.).
  - Se debe tener en cuenta la velocidad de cifrado, uso de memoria, el rango de aplicaciones en el que se puede usar el protocolo de cifrado, el costo y la seguridad.
  - El algoritmo de cifrado que se va a utilizar y los mecanismos de implementación. Observando que algunos

algoritmos han perdido vigencia y han entrado en desuso. Se debe plantear el uso de combinaciones de algoritmos.

- Se debe establecer un servidor de claves donde se generen y al cual solo tenga acceso la persona determinada por la Coordinación de Sistemas.
- Se deben utilizar herramientas generadoras de números o cadenas de caracteres pseudoaleatorios, de manera que sean impredecibles y computacionalmente imposibles de descifrar.
- En el caso en el que una autoridad certificadora sea vulnerada o se descifre un algoritmo de cifrado, la organización debe estar preparada para reemplazar todos sus certificados y llaves de cifrado en el menor tiempo posible.
- Es necesario crear un registro de versiones de llaves de cifrado que incluya:
  - Algoritmo de cifrado
  - Longitud de la clave
  - Sistema operativo
  - Nombre del sistema de gestión de llaves criptográficas
  - Fecha de creación de las llaves.
  - Usuarios a los que se les asignó la llave
  - Tiempo de vida de la llave
  - Nombre del sistema o sistemas de información en los que se implementa el cifrado
  - Activos protegidos con las llaves.
  - Fecha de revocación, eliminación o borrado de las llaves criptográficas.

- Almacenamiento
  - El almacenamiento de las claves debe hacerse de forma segura, cifrándolas y protegiendo el sistema de almacenamiento con contraseña. El único usuario que puede acceder a este sistema es el Responsable de TIC o quien este delegue.
  - Si se hace uso de un sistema de gestión de llaves, se deben seguir las recomendaciones de seguridad que indique el fabricante.

- Distribución de llaves de cifrado
  - Para distribuir las llaves se debe tener en cuenta si se usa:
    - Infraestructura de clave pública,
    - Gestión de certificados y llaves corporativas,
    - Gestión grupal de llaves en transferencia, entre otras.

  Debido a que implica una gestión compleja de muchas llaves, existen problemas relacionados con la posibilidad de romper los algoritmos de cifrado, se debe asegurar que los datos son descifrados solo por aquellos que realmente tienen los privilegios para hacerlo. Es necesario que las llaves y los sistemas de cifrado sean compatibles o tengan soporte en varias bases de datos, aplicaciones y estándares.

- Destrucción de llaves de cifrado.

La destrucción de las llaves de cifrado implica que se debe eliminar el sistema de creación de las llaves, es decir, las aplicaciones de software, las copias de las llaves y el borrado seguro de los dispositivos donde estaban almacenadas o si es necesario la destrucción física de los dispositivos de almacenamiento, la revocación de privilegios a los usuarios mientras se establece el nuevo esquema de llaves de cifrado y la revisión del registro de versiones de las claves.

7.5. APLICACIONES RECOMENDADAS

- **Acero Docs**. Es una solución para el cifrado de datos que se ha convertido en una de las más solicitadas por las empresas. Se trata de una herramienta que emplea la tecnología IRM para ofrecer una gestión de permisos avanzada, Además, es compatible con sistemas operativos Windows, Android y iOS.

- **Enigmail**. Este programa de cifrado se utiliza principalmente para encriptar las comunicaciones por email. Gracias a esta herramienta se pueden enviar correos electrónicos cifrados, cuya clave se puede generar desde el propio programa, o con un software de terceros. Ha sido desarrollada para Mozilla Thunderbird y es compatible con sistemas operativos Windows, Mac y Linux.

- **HTTPS Everywhere**. Programa de cifrado y descifrado que permite enviar la información encriptada a través del navegador. Usando esta herramienta, todas las transferencias de datos que hagas a través del navegador de internet viajarán seguras y cifradas. Está disponible para los navegadores Chrome y Firefox.

- **BitLocker**. herramienta desarrollada por Microsoft bajo la plataforma Trusted Platform Module (TPM) que permite encriptar el disco duro para proteger todos los archivos del equipo e incluso el sistema operativo.

- **Whisply**. Herramienta para cifrado más interesantes, puesto que se emplea para cifrar datos almacenados en la nube. Puede usar esta solución desarrollada por BoxCryptor para encriptar archivos antes de subirlos a plataformas como One Drive, Google Drive o Dropbox.

- **DiskCryptor**. Es una de las mejores herramientas de cifrado gratuitas. Se utiliza principalmente para cifrar USB o discos duros. Una solución interesante para proteger los datos almacenados en el equipo o en dispositivos externos.

- **Cryptomator**. Se trata de un software de código abierto que permite crear una especie de caja fuerte en forma de gran carpeta cifrada, en la que se pueden guardar todo tipo de archivos. Gracias al cifrado AES, nadie podrá acceder a los archivos guardados en esa carpeta sin los permisos pertinentes. Es una herramienta gratuita que ni siquiera requiere registro y que está disponible para Windows, Mac OS, Linux, Android y iOS.

8. BRING YOUR OWN DEVICE

Estas siglas en inglés responden a “Bring Your Own Device”. Se denomina así al uso de dispositivos personales en el ámbito corporativo. En la actualidad, empresas y organizaciones utilizan diversas estrategias para aumentar la productividad de sus actividades y mantenerse a la vanguardia. Muchas de esas estrategias se encuentran relacionadas con la innovación y el desarrollo tecnológico, reconociendo una de ellas que ha cobrado relevancia por sus ventajas: el uso de dispositivos móviles, tablets o laptops personales para desarrollar actividades laborales. Esta tendencia genera beneficios como mayor movilidad y satisfacción por parte de los empleados y una reducción de costos institucionales a nivel de infraestructura tecnológica.

8.1. OBJETIVO

El propósito de esta normativa es **regular el uso de dispositivos personales en el entorno institucional** que se utilicen de formar permanente para el acceso y almacenamiento de información de la FOSCAL - FOSCAL INTERNACIONAL. Lo anterior tiene como finalidad la mitigación de los siguientes riesgos generales:

- Pérdida o robo de dispositivos, incluyendo los datos almacenados en ellos.
- Exposición de información clasificada debido al uso en lugares públicos.
- Introducción de virus y malware a la red institucional.
- Compromiso de la imagen institucional.

Es de importancia que los controles establecidos en esta normativa sean observados todo el tiempo que se haga uso de BYOD. Esta es una decisión conjunta entre la organización y los propietarios de dispositivos que se usen particularmente con fines laborales.

8.2. ÁMBITO DE APLICACIÓN

Aplica a todos los dispositivos personales que tienen la capacidad de almacenar, transferir o procesar cualquier tipo de información sensible dentro el alcance institucional. Entre estos dispositivos se incluye a los computadores personales, teléfonos inteligentes, unidades de memoria USB, cámaras digitales, discos externos, módems, etc. En esta normativa se identificará a estos dispositivos como BYOD.

La presente Normativa será de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la FOSCAL - FOSCAL INTERNACIONAL, incluyendo el personal de organizaciones externas.

8.3. VIGENCIA

La presente normativa ha sido aprobada por la Dirección Administrativa de la FOSCAL - FOSCAL INTERNACIONAL, estableciendo de esta forma las directrices generales para el control sobre la información institucional que sea accedida a través de dispositivos que no pertenecen a la organización, por lo cual los funcionarios asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la FOSCAL - FOSCAL INTERNACIONAL.

8.4. REVISIÓN Y EVALUACIÓN

La Coordinación de Seguridad de la Información del Departamento de Tecnología revisará la presente Normativa, que se someterá, de haber modificaciones, a la aprobación de la Dirección Administrativa de la FOSCAL - FOSCAL INTERNACIONAL.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

8.5. NORMATIVA

8.5.1. Normativa Institucional

La FOSCAL - FOSCAL INTERNACIONAL acepta el uso de dispositivos BYOD para el acceso y manejo de información institucional siempre que esta actividad se realice originada por las funciones propias del cargo del funcionario propietario del dispositivo que se desea usar con BYOD.

8.5.2. Proceso de Autorización

Los funcionarios no deberán usar sus dispositivos personales para mantener o procesar información de la empresa a menos que el jefe Inmediato realice una solicitud por GESTOR y que esta sea técnicamente aprobada por el Departamento de Tecnología, posterior a la lectura (por parte del funcionario) y aceptación escrita de las condiciones de esta normativa. La solicitud debe incluir la siguiente información:

- Datos del funcionario que hace la solicitud.
- La razón laboral por la cual se origina la solicitud.
- Los datos que serán manejados en el dispositivo.
- El dispositivo específico que será usado.

8.5.3. Condiciones de Uso

Todos los usuarios de dispositivos BYOD deben aceptar y cumplir con las siguientes condiciones de uso:
Directrices:

- La alta dirección de la institución debe aprobar el uso de dispositivos personales para el desarrollo de las funciones laborales.
- La División de Tecnología e Innovación debe llevar control e inventario de los dispositivos personales aprobados para desempeñar funciones laborales.
- La División de Tecnología e Innovación, mediante la mesa de servicio deberá realizar la verificación del dispositivo para que cumpla como mínimo con lo siguiente:
  - El dispositivo deberá contar con el Sistema Operativo Licenciado
  - El dispositivo deberá contar con un Software Antivirus Actualizado y Licenciado.
  - El dispositivo no deberá tener software instalado que permita saltarse los controles de seguridad de la institución.
  - Los dispositivos móviles personales que hayan pasado por procedimientos de rooteo o jailbreak quedarán prohibidos para uso laboral.
  - Cliente de VPN (Virtual Private Network) que permita la conexión remota de los dispositivos BYOD hacia la red institucional. Esto tiene como objetivo asegurar la confidencialidad e integridad de las comunicaciones.
  - Medidas de control de acceso suficientes en cuanto al uso de dispositivos. Así mismo, la responsabilidad de implementar medidas de control de acceso a la red, evitando posibles incidentes de seguridad.

- En estos dispositivos solo se tendrá la posibilidad de:
  - Instalar SAP, previamente autorizado por la dirección médica o administrativa e instalado por el personal técnico.
  - Los accesos a información compartida y al correo se deben realizar en la nube.
- Todo dispositivo BYOD autorizado para almacenar información de la entidad debe cumplir con la reglamentación vigente en materia de uso de software legal. El usuario es enteramente responsable de contar con todo el software de su dispositivo debidamente licenciado.
- El funcionario o contratista autorizado al uso de su dispositivo personal debe garantizar bajo compromiso de confidencialidad que la información pública reservada o información pública clasificada correspondiente a sus labores asignadas será almacenada de forma aislada a la información personal que guarde en el dispositivo.
- La División de Tecnología e Innovación, puede realizar revisiones a los equipos BYOD para certificar que estén cumpliendo con las políticas de seguridad de la información, las revisiones preservarán el derecho fundamental a la intimidad del usuario del BYOD y las normas sobre protección de datos de carácter personal.
- El propietario del dispositivo BYOD debe aplicar todas las medidas de seguridad razonables que estén a su alcance para preservar la integridad, confidencialidad y disponibilidad de la información que se encuentre en su dispositivo personal.
- El propietario del dispositivo BYOD debe aplicar las medidas de seguridad que minimicen la pérdida o hurto del mismo.
- El propietario del dispositivo debe informar sin demoras a la División de Tecnología e Innovación o la Coordinación de Seguridad de Información y a la autoridad competente el robo o pérdida de su dispositivo. La Institución gestionará la pérdida o divulgación de información almacenada en los dispositivos BYOD, mediante el procedimiento de gestión de incidentes de seguridad de la información.
- La información clasificada como pública reservada o pública clasificada deberá almacenarse en los repositorios establecidos por la institución “Google Drive y servidores”, no deberá guardarse en los discos duros de los dispositivos BYOD o en otros dispositivos personales.
- Es rotundamente prohibido conectar los dispositivos BYOD a las redes cableadas de la institución. La División de Tecnología e Innovación activa redes WIFI debidamente aseguradas para la conexión de dichos dispositivos.
- El propietario del dispositivo BYOD debe gestionar los parches, vulnerabilidades y actualizaciones de software requeridos por el mismo.
- El propietario del dispositivo debe abstenerse de visitar sitios o aplicaciones web de dudosa procedencia, con contenido inapropiado o confuso, ya que el riesgo de pérdida o robo de información puede ser mayor.
- La Coordinación de Seguridad informática de concientizar y formar a los usuarios en la protección de sus propios dispositivos y los datos que contienen.
  - Configuración de los parámetros de seguridad de los dispositivos.
  - Actualización tanto del Sistema Operativo como las aplicaciones periódicamente.
  - No instalar aplicaciones que exijan permisos que ponga en riesgo la información confidencial (Accesos, geolocalización, etc.)
  - Bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad
  - No desatender los dispositivos al viajar en transporte público.
  - Controlar el acceso a redes desconocidas o libres
- El incumplimiento de cualquiera de las condiciones de uso especificadas podrá generar la cancelación de la autorización para BYOD.

8.6. DERECHOS ESPECIALES

Con el objetivo de asegurar que la información está adecuadamente protegida es importante que la FOSCAL - FOSCAL INTERNACIONAL pueda monitorear y auditar el nivel de aplicación de esta normativa, los cuales serán apropiados a la clasificación de la información que se maneje a través del dispositivo. Debido a lo anterior la Coordinación de Seguridad de la Información del Departamento de Tecnología podrá solicitar el dispositivo BYOD para su revisión.

Los métodos y tiempos de monitorización y auditoría contemplarán la privacidad del propietario del dispositivo y no se realizará en horas fuera del horario laboral establecido.

En el evento de pérdida o robo del dispositivo, el propietario debe informar al Departamento de Tecnología lo más pronto posible, especificando las circunstancias que se produce la pérdida y la sensibilidad de la información almacenada. La FOSCAL - FOSCAL INTERNACIONAL se reserva el derecho de remover información o realizar la inactivación de usuarios como medio de precaución de seguridad. Lo anterior puede involucrar la pérdida de información personal que el funcionario almacenará en ambientes institucionales.

Al retiro del funcionario de la institución, se debe permitir una revisión del dispositivo BYOD y todos los datos institucionales y aplicaciones deben ser eliminadas.

8.7. REEMBOLSO

La FOSCAL - FOSCAL INTERNACIONAL no proporcionará ningún tipo de retribución económica a los funcionarios por el uso de BYOD y la aplicación de esta normativa institucional.

9. CORREO INSTITUCIONAL

El correo electrónico institucional es un medio formal y oficial de comunicaciones de la institución y una herramienta de trabajo que dispuesta para facilitar las labores propias de las labores institucionales; teniendo en cuenta esto, es primordial establecer los lineamientos que se deben tener presente de acuerdo con las obligaciones, prohibiciones que debe tener presente.

9.1. OBJETIVO

Establecer las responsabilidades y lineamientos que deben cumplir todos los usuarios del correo institucional para FOSCAL - FOSCAL INTERNACIONAL, con el fin de garantizar el correcto uso del mismo y asegurar un mejor aprovechamiento de la herramienta de correo como parte fundamental de las labores institucionales.

9.2. ALCANCE

Esta normativa es de obligatorio cumplimiento para los servicios de correo que se encuentren en la plataforma institucional, busca establecer los lineamientos, responsabilidades, normas y buenas prácticas que aplican para el uso adecuado del correo electrónico del dominio @foscal.com.co.

9.3. USUARIO SERVICIO DE CORREO

Podrá solicitar y utilizar una cuenta de correo electrónico de FOSCAL - FOSCAL INTERNACIONAL su personal funcionario, contratado o laboral, así como el resto de grupos que figuran en el cuadro “Usuarios del Servicio de Correo FOSCAL - FOSCAL INTERNACIONAL”, se regirán con las limitaciones que marca este documento.

Podrá solicitar y utilizar una cuenta de correo electrónico de FOSCAL - FOSCAL INTERNACIONAL su personal funcionario, contratado o laboral, así como el resto de grupos que figuran en el cuadro “Usuarios del Servicio de Correo FOSCAL - FOSCAL INTERNACIONAL”, se regirán con las limitaciones que marca este documento. (Ver Responsabilidades y Restricciones)

La siguiente tabla muestra la relación de los colectivos que pueden disponer de una cuenta de correo electrónico

Personal		**Grupo**	**Cuenta**	**Tipo Cuenta**	**Observaciones**
FOSCAL - FOSCAL INTERNACIONAL	Laboral /Contratados	1	Si	Personal	Equipo asignado
		2		Organizativa	Sin equipo asignado, se crea correo institucional por el área para ser administrado por un funcionario (secretaria o personal de turno)
	Residentes	3	Si	Personal	
NO FOSCAL - FOSCAL INTERNACIONAL	Practicantes	4	No	Institucional	(1)
	Estudiantes UNAB	5	No		
	Outsourcing	7	No	Institucional	(2)
	Interventorías	8	No	Institucional	
	Estancias breves	9	No	Personal	(1)

	Otros	10	No		(3)

(1) Si fuese necesario dotar de una cuenta de correo a una persona de este grupo, le podrá ser asignada siempre que su estancia en las dependencias del FOSCAL - FOSCAL INTERNACIONAL fuese superior a 6 meses y su actividad así lo requiriese. Cualquier excepción a esta norma deberá ser propuesta y autorizada por la Dirección Administrativa.
(2) No se podrán asignar cuentas de correo a personal de empresas de servicio contratadas. Si, por alguna razón excepcional esto fuera preciso, la cuenta será de uso temporal, debiendo ser autorizada previamente por la Dirección Administrativa
(3) La relación anterior es extensiva, por lo que sólo los grupos que figuran de manera expresa en esta relación están autorizados a disponer de cuentas de correo electrónico de FOSCAL - FOSCAL INTERNACIONAL. Se requiere, por tanto, la previa autorización y modificación de esta relación para autorizar el uso de cuentas de correo a otros grupos; siendo necesario para ello la previa autorización de la Dirección Administrativa

La posesión de una cuenta de correo no implicará EN NINGÚN CASO una vinculación laboral con FOSUNAB, y solamente se considera como una herramienta de trabajo necesaria para que el personal pueda desempeñar su labor eficazmente en la organización.

9.4. CUENTAS Y BUZONES DE CORREO

9.4.1. Tipología

Se pueden distinguir tres tipos de cuentas: Personales, Institucionales y Organizativas.

- **Cuentas Personales**: Identifican las direcciones de correo electrónico de una persona. Ej. Pedro Pérez – pedro.perez@foscal.com.co.
- **Cuentas Institucionales**: Asociadas a cargos. Una persona tendrá acceso a una cuenta institucional en función de su cargo o actividad. Ej. Director General – dir.general@foscal.com.co.
- **Cuenta Organizativas**: Orientadas fundamentalmente a unidades, grupos y servicios. Pueden ser utilizadas por una o varias personas conjuntamente y son gestionadas por un responsable. Normativa Institucional

9.4.2. Solicitud y Creación

Las cuentas personales e institucionales se crean a petición del Departamento de Gestión Humana o del área de la organización responsable.

La solicitud de una cuenta organizativa o genérica debe ser realizada por el jefe de las unidades, departamentos o grupos, al administrador del dominio de correo. Se requiere definir el responsable de la misma, que será el interlocutor o persona de contacto con los equipos de administración de correo.

9.4.3. Formato de las direcciones de correo

Las cuentas personales correspondientes al dominio institucional “foscal.com.co” se ajustan:

La forma común de una cuenta de correo electrónico para los alias del dominio "foscal.com.co" es:

<alias_del_usuario>@foscal.com.co

En el formulario de solicitud el generador de alias utiliza los siguientes criterios:

- Las direcciones estarán formadas por combinaciones del nombre y apellidos o iniciales de una persona:
  - Es obligatorio seleccionar el primer carácter de la columna "Nombre1"
  - Tiene que seleccionar la columna "Apellidos1"

- Si el alias elegido ya está en uso podrá utilizar el primer carácter de la columna “Nombre1” junto con el primero de “Nombre2”. En caso de que no exista “Nombre2” se deberán seleccionar los 2 primeros caracteres de “Nombre1” y así sucesivamente hasta encontrar un alias único.
- Los caracteres con tilde son sustituidos por el mismo carácter sin tilde. El carácter ñ es sustituido por la letra n.

- Cada persona podrá seleccionar hasta un máximo de dos alias para su cuenta "@foscal.com.co" entre las posibles combinaciones que ofrezca el generador.

9.4.4. Tamaño de los buzones de correo

La capacidad máxima para los buzones puede variar a lo largo del tiempo, y en caso de necesitarse cambios en el tamaño asignados debe ser solicitado al Administrador del correo. Una vez alcanzado el 100% de la cuota asignada, todos los mensajes son rechazados por el sistema, siendo necesario que el usuario vacíe el buzón para restablecer la recepción normal de mensajes.

9.4.5. Envío y recepción de mensajes

Se ha de considerar que el correo enviado circula por distintos servidores de Internet y que éstos imponen libremente restricciones sobre los tamaños admitidos, por lo que cuanto más grande sea el tamaño del mensaje de correo mayor es la probabilidad de que sea rechazado, impidiendo, de este modo, que llegue a su destino.

Para el envío de ficheros de gran tamaño, se recomienda el uso de otro tipo de servicios los cuales pueden ser consultados con el Departamento de TI.

El tamaño máximo de los correos que se pueden enviar y recibir se podrá modificar sin previo aviso. Asimismo, y por razones de disponibilidad del servicio se podrán incluir otro tipo de restricciones, como limitar el número máximo de mensajes enviados desde una cuenta durante un período de tiempo.

Es obligatorio enviar un correo con una dirección de retorno válida y propia del sistema a través del cual se está enviando el correo. No se podrá usar como remitente direcciones externas de otros proveedores (del tipo @gmail.com, @hotmail.com, etc.) para enviar correo mediante la plataforma de correo institucional.

9.4.6. Firma correo

Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar los lineamientos y recomendaciones para dicho tipo de documentos, tales como:

- Iniciar su correo con un saludo formal. Ejemplo: Buenos días Adriana.
- Nombrar al destinatario de correo por su nombre o profesión.
- Evitar tutear.
- Evitar el uso de palabras que puedan resultar ofensivas.
- Escribir puntualmente. No extenderse demasiado.
- Al final del correo agradecer por la atención prestada y firmar con los requerimientos establecidos para la firma electrónica institucional (ver al final).

Se deben tener en cuenta las siguientes normas para unificar los correos electrónicos y fortalecer la imagen corporativa:

- Los correos electrónicos institucionales deben estar escritos en Arial Narrow, tamaño 11 puntos.
- El texto debe estar escrito únicamente en color negro.
- No se debe escribir en mayúsculas, ya que puede ser interpretado como un grito u ofensa.
- Los correos enviados no deben tener ningún color o imagen sobre el fondo en el que se escribe el mensaje.

Todos los usuarios del correo institucional deben unificar la firma del correo electrónico y el disclaimer implementando el modelo que se encuentra a continuación. (Anexo Manual de Creación Firmas Institucionales)

Tatiana Angarita Rodríguez
Jefe Tecnología e Innovación
(57)(7)7000 300, ext 6123
tatiana.angarita@foscal.com.co
Clínica FOSCAL
Ave. El Bosque No 23-60 Torre TMS Piso 4
Floridablanca, Colombia
www.foscal.com.co

No me imprimas si no es necesario. Protejamos el medio ambiente

9.5. VIGENCIA, DESACTIVACIÓN Y ELIMINACIÓN DE CUENTAS DE CORREO

9.5.1. Vigencia

- **Cuentas Personales**: Se podrá disponer de una cuenta de correo personal hasta 1 mes después de la fecha de baja del funcionario o extinción de la situación que originó la creación de la cuenta en FOSCAL - FOSCAL INTERNACIONAL. Excepcionalmente, este periodo podrá variar por necesidades del servicio debidamente motivadas. Esta excepcionalidad no deberá exceder 1 año.
  A la finalización del plazo mencionado, se procederá a la cancelación de la cuenta y al consiguiente borrado de los correos almacenados.
  Para aquellas cuentas utilizadas por personal externo o ajeno a FOSCAL - FOSCAL INTERNACIONAL, el responsable de la persona ante FOSCAL - FOSCAL INTERNACIONAL deberá poner en conocimiento del administrador de correo la baja de dicha persona para que se proceda, entre otras acciones, a la cancelación de su cuenta en un plazo máximo de 3 meses desde la fecha de baja.
- **Cuentas Institucionales**: Las cuentas institucionales permanecen hasta que desaparece el cargo o función que las motivó; por lo que serán utilizadas por las personas que ocupan ese cargo o función a lo largo del tiempo. La baja de la persona en el cargo implica el cambio de contraseña de la cuenta de correo institucional.
- **Cuenta Organizativas**: Este tipo de cuentas se cancelan o gestionan a petición de la unidad o persona responsable de las mismas.

9.5.2. Desactivación y Eliminación

- **Borrado Automático de Cuentas**: Se eliminarán aquellas cuentas de correo que no han sido consultadas durante un periodo continuado de seis meses. Esto conlleva el borrado de los correos almacenados en dicha cuenta.
- **Cancelación Voluntaria de Cuentas:** Se podrá solicitar el cierre o cancelación de una cuenta de correo. Para ello, su titular deberá realizar la solicitud al administrador del dominio de correo, quién hará efectiva la solicitud tras la comprobación de su veracidad y la remisión de un correo de confirmación al solicitante dos días antes de efectuar la cancelación de la cuenta**.** La cancelación de una cuenta implica:

  - Imposibilidad de enviar y recibir nuevos correos.
  - Eliminación de los correos almacenados**.**

- **Desactivación Temporal de Cuentas:** El uso inapropiado o el abuso en el servicio de correo electrónico puede ocasionar la desactivación temporal o permanente de las cuentas. Las acciones en este sentido se pueden llevar a cabo en función de las posibles repercusiones en el buen funcionamiento del servicio.

  La desactivación de la cuenta implica la imposibilidad de enviar y recibir nuevos correos mientras esta no vuelva a ser activada. Ante situaciones de grave riesgo para la disponibilidad o continuidad del servicio, se podrá cambiar la contraseña de una cuenta.

9.6. RESPONSABILIDADES Y RESTRICCIONES

9.6.1. Responsabilidades

- Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional.
- Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla bajo ninguna circunstancia, salvo los casos en que las cuentas son genéricas y son gestionadas por varios usuarios.
- Las cuentas de correo institucional son creadas para el uso exclusivo de las funciones propias del usuario, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad y seguridad de la información.
- Antes de enviar un correo electrónico, el usuario debe utilizar el corrector ortográfico de la herramienta utiliza como gestor del correo.
- Él envió de correos electrónicos implica el consumo de recursos tecnológicos y demanda tiempo a la persona receptora, por tal razón se debe evitar el envió de correos innecesarios y que no guarden relación con el desempeño de las funciones asignadas.
- Antes de responder o reenviar un correo, el usuario debe validar si se requiere incluir todos los destinatarios, el historial y la información que posee el mismo.
- Todo correo de procedencia desconocida, correo basura, SPAM, correo no deseado, etc. que sea recibido en la los buzones de correo electrónico, debe ser ignorado, eliminado inmediatamente y reportado al área de tecnológica con el fin de evitar posibles infecciones por código malicioso o virus.
- El usuario del correo electrónico se compromete a reportar oportunamente cualquier fallo de seguridad de su cuenta institucional, incluyendo el uso no autorizado, perdida de contraseña, etc.
- Según lo establecido en la ley 524 de 1999, los mensajes de correo electrónico revisten la misma fuerza probatoria que tiene un documento físico.
- El correo electrónico institucional es una herramienta de trabajo, de uso exclusivamente laboral, por lo tanto la información contenida en ellos es propiedad de la institución.

9.6.2. Restricciones

- Envió de correos con mensajes que impliquen afectaciones sobre las normas legales, la moral, el orden público, la intimidad o el bueno nombre de las personas, que contengan contenido irrespetuoso, difamatorio, racista, religioso irrespetuoso, discriminatorio, de acoso o intimidación; así́ como imágenes o videos con contenidos ilegales, ofensivo, extorsivo, indecente o con material sexual.
- Se prohíbe el uso de correos personales con el fin de establecer o transferir información institucional.
- La propagación de correos de procedencia desconocida, SPAM, correo basura o no deseado, hacia cuentas institucionales.
- Es incorrecto enviar mensajes con direcciones (remitente) no asignadas por los responsables de nuestra institución y, en general, es ilegal manipular las cabeceras de correo electrónico saliente.
- Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para nuestra organización.
- Utilizar mecanismos y sistemas que intenten ocultar la identidad del emisor del correo.

10. AUDITORÍA Y CONTROL

La auditoría es una herramienta que permite determinar la eficacia y eficiencia del sistema, a través de la identificación de fortalezas y debilidades. En cuanto al control tiene como objetivo contrastar el resultado final obtenido contra lo deseado a fin de incorporar medidas correctivas para lograrlo, o bien verificar la efectividad de lo obtenido.

La auditoría informática permite a la institución comprobar la fiabilidad de las herramientas, servicios e infraestructura, analizando la aplicación de los diferentes recursos y sistemas informáticos existentes dentro de FOSCAL y FOSCAL INTERNACIONAL, los cuales están orientados al desarrollo de la misión y visión organizacional.

10.1. TIPOS DE AUDITORÍA

Existen distintos tipos de auditorías informáticas dependiendo del objetivo de las mismas, como auditorias técnicas, forenses, de cumplimiento de normativas o test de intrusión, entre otras, Las auditorias de seguridad pueden clasificarse en:

10.1.1. Auditorías Internas y Externas

Se denomina interna, cuando son ejecutadas por personal propio de la institución y externas cuando se realizan por empresas independientes a la empresa. Ambas tienen el objetivo de medir y evaluar la confiabilidad y eficacia del sistema con mira a lograr su mejoramiento.

10.1.2. Auditorías Técnica

Su objetivo está centrado en una parte concreta de un sistema informático. Entre estas auditorias podemos encontrar las de cumplimiento de normativas que tienen como objeto la verificación del cumplimiento de algún estándar de seguridad o si las políticas y protocolos de seguridad se están realizando de forma apropiada.

10.1.3. Auditorías por Objetivo

Son auditorias de seguridad técnicas que se diferencia según el objetivo que se persiga. Las más comunes son:

- *Sitios Web*. Auditorias que tienen la finalidad de evaluar la seguridad de las páginas web para descubrir posibles vulnerabilidades que pueden ser utilizadas por terceros.
- *Forense*. Se realizan tras haberse producido un ataque o incidente de seguridad y persiguen descubrir las causas por las que se ha generado, el alcance del mismo, por qué no se ha evitado, etc.
- *Redes*. Evalúan el funcionamiento y seguridad de las redes institucionales. Ejemplo: VPN, WI-FI, Firewall, Antivirus, etc.
- *Control de Acceso*. Centradas en los controles de acceso y que están vinculadas a dispositivos tecnológicos físicos como cámaras de seguridad, mecanismos de apertura de puertas y software específico para el control de acceso.
- *Hacking Ético.* Se realizan para medir el nivel de seguridad de la institución realizando una simulación de ataque externo para evaluar los sistemas y medidas de protección, identificando sus vulnerabilidades y debilidades.

10.2. TIPOS DE CONTROL

A continuación, los diferentes tipos de control para las actividades de auditoria:

10.2.1. Controles Preventivos

Anticipan eventos no deseados antes de que sucedan.

- Son más rentables.
- Deben estar incorporados en los sistemas.
- Evitan costos de corrección o reproceso.

10.2.2. Controles Detectivos

Identifican los eventos en el momento en que se presentan.

- Costo elevado.
- Evalúan la efectividad de los preventivos.
- Incluyen revisiones y comparaciones como el registro de desempeño.

10.2.3. Controles Correctivos

Aseguran que las acciones correctivas sean tomadas para revertir un evento no deseado.

- Acciones y procedimiento de corrección.
- Documentación y reportes que informan a la dirección de la institución, el seguimiento de los eventos hasta corregirlos o solucionarlos.

10.3. ACCIONES

10.3.1. Acción Correctiva

Define los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de las políticas y manuales de seguridad establecidos dentro de la institución. Asimismo, define los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repitan las no conformidades.

10.3.2. Acción Preventiva

Define los lineamientos para identificar, registrar, controlar, desarrollar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real o potencial sobre los sistemas y servicios de seguridad informática y de la información, eliminando sus causas.

11. SUPRESIÓN DE DATOS O INFORMACIÓN

Para completar el ciclo de vida de la información es necesario pasar por el proceso de destrucción o eliminación de la misma, se deben emplear métodos de borrado seguro para garantizar que la información y/o los medios que la contienen o almacenan no se puedan recuperar.

En todos los casos de destrucción electrónica, se debe borrar la información original, todas sus copias y sus respectivos respaldos de seguridad. En el caso de la destrucción impresa se deberán eliminar todas las copias y respaldo existentes. Durante la destrucción de la información, es un deber velar por el cumplimiento del conjunto de políticas que afecten a la información, especialmente las vinculadas a su divulgación y acceso.

11.1. GESTIÓN ADECUADA DE DISPOSITIVOS

- Se debe tener un registro de los dispositivos operativos, funcionarios o departamentos responsables, la información contenida en ellos, su clasificación y grado de criticidad.
- Se debe llevar la supervisión de los dispositivos que almacenan las copias de seguridad de la información, de acuerdo con las leyes, normativas, procesos y procedimientos vigentes. Ley de protección de datos 1581.
- Controlar cualquier operación ejecutada sobre los dispositivos de almacenamiento: mantenimiento, reparación, sustitución, etc.
- En los traslados de los dispositivos de almacenamiento a instalaciones externas se debe asegurar el cumplimiento de la cadena de custodia de los mismos, evitando fugas de información.

11.2. REGISTRO DE LAS OPERACIONES DE BORRADO

- Debe existir una solicitud formal indicando los medios o información a destruir dirigida al responsable del archivo.
- Se debe elegir la herramienta que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo se realizó.
- Se debe generar un reporte de ejecución que identifique al personal actuante y la metodología empleada para la destrucción de la información.
- Se debe documentar los procesos cuando la destrucción de la información no se pueda realizar correctamente e implementar otros medios de destrucción.

11.3. TIPOS DE ALMACENAMIENTO

Para definir los métodos de borrado, es necesario establecer la naturaleza de los activos, es decir, si la información se resguarda en un medio de almacenamiento físico o un medio de almacenamiento electrónico.

11.3.1. Almacenamiento Físico

Los medios de almacenamiento físico son todo recurso inteligible a simple vista y con el que se puede interactuar sin la necesidad de ningún aparato que procese su contenido para examinar, modificar o almacenar información.

Dentro de los medios de almacenamiento físico se encuentran:

- Archivadores
- Bodegas
- Estantes
- Oficina

11.3.2. Almacenamiento Electrónico

Los medios de almacenamiento electrónico, son todo recurso al que se puede acceder solo mediante el uso de un equipo de cómputo que procese su contenido para examinar, modificar o almacenar la información.

Dentro de los medios electrónicos se encuentra:

- Medios Magnéticos
  - Disco Duro interno (Propios de los equipos de cómputo)
  - Disco Duro externo o portable
  - Cintas Magnéticas
- Medios Ópticos
  - CD's
  - DVD's
  - Blu-Ray
- Medios de estado solido
  - Memorias USB
  - Disco Duro SD
- Servicios de almacenamiento en línea

11.4. ELIMINACIÓN ERRÓNEA

11.4.1. Almacenamiento Físico

- La destrucción manual: Romper archivos y documentos a mano, con tijeras o rasgarlos con un bisturí son métodos inseguros para desechar este tipo de activos. Este método permite que una persona mal intencionada pueda recuperar los fragmentos de la basura y los ensamble a modo de rompecabezas para extraer información importante.
- Tirar documentos de forma íntegra a la basura: Arrojar a la basura documentos con información valiosa o utilizarlos como papel de reciclaje es una conducta aún más riesgosa que la anterior.

11.4.2. Almacenamiento Electrónico

Los sistemas operativos de los equipos de cómputo o dispositivos ordenan la información en archivos dentro de sus medios de almacenamiento. Para encontrar estos archivos en el espacio correspondiente, el sistema operativo acude a la "lista de archivos", donde se indica tanto el nombre del archivo como su ubicación dentro del espacio de almacenamiento.

Cuando se utilizan métodos de borrado dispuestos por el propio sistema operativo, la eliminación se realiza exclusivamente en la "lista de archivos" sin que se borre realmente el contenido del archivo que permanece en la zona de almacenamiento hasta que se reutilice este espacio con un nuevo archivo. Por tanto, toda aquella acción que no conlleve la eliminación, tanto de la información de la "lista de archivos" como del contenido del mismo, no consigue destruir eficazmente dicha información de forma específica.

- Los comandos de borrado por defecto de los sistemas operativos: Cuando se utiliza un comando o el botón de "borrar" o "eliminar", lo único que se está quitando de esa tabla es la referencia al archivo, pero la información permanece en el medio de almacenamiento, hasta que se reutilice este espacio con un nuevo archivo.
- Formatear: Cuando se formatea un medio de almacenamiento, se eliminan las tablas o listas de archivos mencionadas anteriormente, pero igual que en el caso anterior, la información sigue en el dispositivo y puede recuperarse con el uso de software.

11.5. ELIMINACIÓN SEGURA

Las técnicas de borrado seguro buscan que no sea posible recuperar la información tanto física como electrónica y evitan que personas no autorizadas puedan tener acceso a esos datos. De acuerdo a estándares internacionales en la materia, las características para este tipo de destrucción son:

- Irreversibilidad. Se debe garantizar que no existe un proceso que permita recuperar la información.
- Seguridad y confidencialidad. Los medios de almacenamiento se deben tratar durante el borrado con la misma seguridad con que se han mantenido durante su existencia.
- Favorable al medio ambiente. El método de borrado debe producir el mínimo de emisiones y desperdicios que afecten el medio ambiente.

11.5.1. Eliminación Física

11.5.1.1. Trituración

Uno de los procesos más intuitivos para la destrucción de activos, tales como documentos, carpetas o archivos, es la trituración. Las principales características que se deben considerar para la adquisición de una trituradora son el tipo y tamaño del corte o “partícula”, así como la capacidad de la trituradora.

Considerando el tipo de corte, existen dos tipos principales de trituradoras:

- En línea recta o tiras: Cortan el documento en tiras delgadas. Se recomienda usar el corte en tiras de 2 mm de ancho o menos, a fin de evitar que la información pueda ser recuperada rearmando los fragmentos.
- En corte cruzado o en partículas: Corta el documento de forma vertical y horizontal generando fragmentos diminutos, denominados “partículas”, lo cual hace prácticamente imposible que se puedan unir.

La norma DIN 32757 es un estándar que se ha adoptado a nivel mundial para la destrucción de documentos, creada por el Instituto Alemán para la Estandarización. Esta norma establece cinco grados de seguridad y determina el tamaño máximo de las tiras o partículas en función de la criticidad de la información.

- Estándar: Esta categoría considera información de identificación, contacto, datos laborales y académicos de una persona física identificada o identificable, tal como: nombre, teléfono, edad, sexo, RFC, CURP, estado civil, dirección de correo electrónico, lugar y fecha de nacimiento, nacionalidad, puesto de trabajo, lugar de trabajo, experiencia laboral, datos de contacto laborales, idioma o lengua, escolaridad, trayectoria educativa, títulos, certificados, cedula profesional, entre otros.
- Sensible: Aquellos que permitan inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores y fianzas. Incluye el número de tarjeta bancaria de crédito y/o débito, usuarios, contraseñas, información biométrica, datos jurídicos.
- Especial: Cuya naturaleza única, o bien debido a un cambio excepcional en el contexto de las operaciones usuales de la organización, pueden causar daño directo a los titulares, por ejemplo, la Información adicional de tarjeta bancaria que considera el número de la tarjeta de crédito y/o debito mencionado anteriormente en combinación con cualquier otro dato relacionado o contenido en la misma.
- No recomendable: Documentos generales que deben hacerse ilegibles
- No recomendable: Documentos internos que deben hacer ilegibles.

11.5.1.2. Incineración

La incineración de medios de almacenamiento físico consiste en su destrucción a través del uso del fuego. Actualmente la práctica de la incineración no es muy recomendable por cuestiones relacionadas con el cuidado del medio ambiente, sin embargo, es una opción segura para la destrucción.

11.5.1.3. Químicos

En algunos casos también es posible destruir documentos por medio de químicos, sin embargo, esta opción tampoco es muy recomendable por temas ecológicos.

11.5.2. Eliminación Electrónica

La destrucción de medios de almacenamiento electrónico utiliza técnicas tales como:

- Desintegración. Separación completa o pérdida de la unión de los elementos que conforman algo, de modo que deje de existir.
- Trituración o Pulverización. Procedimiento mediante el cual un cuerpo sólido se convierte en pequeñas partículas.
- Abrasión. Acción de arrancar, desgastar o pulir algo por rozamiento o fricción.
- Fundición o Fusión. Paso de un cuerpo del estado sólido al líquido por la acción del calor.

11.5.2.1. Desmagnetización

Este método expone a los dispositivos de almacenamiento a un campo magnético a través de un dispositivo denominado desmagnetizador. Debido a las fuerzas físicas del proceso, es posible que el hardware donde se encuentra la información se vuelva inoperable, por lo que se recomienda aplicar este método si no se volverá a utilizar el medio de almacenamiento.

La desmagnetización se considera más segura que algunos procesos de destrucción física, ya que altera directamente el contenido de información y no al medio de almacenamiento en sí mismo.

11.5.2.2. Sobreescritura

Consiste en sobrescribir todas las ubicaciones de almacenamiento utilizables en un medio de almacenamiento, es decir, se trata de escribir información nueva en la superficie de almacenamiento, en el mismo lugar que los datos existentes, utilizando herramientas de software.

El método más simple consiste en realizar una sola sobre-escritura, y para implementar una mayor seguridad se pueden efectuar múltiples sobreescrituras o “pasadas” con variaciones en los caracteres grabados al medio de almacenamiento.

11.5.2.3. Borrado Criptográfico

Consiste en el cifrado de la información almacenada en el soporte utilizando un algoritmo de cifrado de clave privada, con una longitud de clave suficiente para que el descifrado de la información sea técnicamente inviable con las herramientas informáticas disponibles en ese momento. Seguidamente, la clave de cifrado se elimina con alguna de las técnicas de borrado seguro.

11.6. HERRAMIENTAS

- **Darik’s Boot and Nuke**: Proyecto gratuito y de código abierto alojado en SourceForge . El programa está diseñado para borrar de forma segura un disco duro hasta que sus datos se eliminen de forma permanente y ya no se puedan recuperar , lo que se logra sobrescribiendo los datos con números pseudoaleatorios generados por Mersenne Twister o ISAAC.

- **HDShreader**: Tiene dos variantes que le permiten utilizar la herramienta tanto desde Windows como externamente. Puede utilizar la variante anterior cuando desee borrar permanentemente los datos de cualquier almacenamiento que no sea la unidad del sistema (donde está instalado Windows), mientras que la última variante se debe utilizar para limpiar la unidad que tiene Windows.
- **HDDErase:** Permite limpiar toda su unidad de disco duro, incluso si tiene el sistema operativo instalado en él.
- **KillDisk:** Programa multiplataforma que viene en dos variantes: instalador y arranque. La herramienta se puede instalar en sistemas operativos Windows o Linux para borrar los datos del Disco duro externo unidades u otros medios de almacenamiento. Con la variante de arranque, el programa es capaz de desmenuzar los datos incluso desde el disco del sistema donde está instalado el sistema operativo principal.
- **CBL Data Shreader:** Aplicación freeware, eliminar por completo los datos del disco que está usando.

12. MANTENIMIENTO DE EQUIPOS

Consiste en realizar labores de verificación, limpieza, entre otras actividades de los equipos de cómputo, impresoras y demás equipos, así mismo el mantenimiento preventivo permite prolongar la vida útil de los equipos de cómputo, minimiza la tasa de desperfectos y aumenta la productividad de los equipos al reducir el tiempo hora/equipo y hora/hombre no útil. El mantenimiento correctivo es el que requiere de solución inmediata por una circunstancia no prevista y consiste en la reparación y/o cambio de las piezas defectuosas, incluyendo el diagnóstico, mano de obra por la reparación y el repuesto.

12.1. MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE EQUIPOS DE CÓMPUTO

- La División de Tecnología e Innovación, planificará el mantenimiento preventivo tomando como base el inventario físico actualizado de los equipos de cómputo. Se deberá excluir de este listado a todos aquellos equipos que tengan garantía vigente o se hayan adquirido recientemente.
- El desarrollo del mantenimiento se efectuará en conformidad con un cronograma establecido, el mismo será coordinado con los funcionarios a fin de tener toda la disponibilidad de los equipos sin afectar sus labores cotidianas.
- Para ejecutar el mantenimiento deberá realizar las siguientes actividades durante el mantenimiento preventivo:
  - Comprobación del correcto funcionamiento, diagnóstico interno y externo de los equipos.
  - Entrega de Informe de Mantenimiento al final de cada servicio, donde se registre los datos de los equipos revisados, así como las incidencias encontradas durante la inspección efectuada.
- Para casos de mantenimiento correctivo en los que no pueda darse solución inmediata al requerimiento, se asignarán equipos en calidad de préstamo (Siempre y cuando exista disponibilidad en el inventario), para no afectar las actividades laborales del funcionario.
- Cuando se efectúen reparaciones realizadas por terceros la División de Tecnología e Innovación supervisará y verificará los trabajos efectuados.

12.2. MANTENIMIENTO PREVENTIVO Y CORRECTIVO INFRAESTRUCTURA DEL DATACENTER

- La División de Tecnología e Innovación está encargada de la infraestructura del DataCenter, por lo tanto, desde este proceso se desarrollarán las acciones para garantizar la operación permanente de los servidores alojados allí, de igual forma se protege la información almacenada en los sistemas de almacenamiento, para que esté segura y disponible.
- Los mantenimientos de la infraestructura del DataCenter esta definidos por la División de Tecnología e Innovación bajo cronograma de actividades y para no afectar las actividades laborales de la institución.

ELABORADO POR:	**REVISADO POR:**	**APROBADO POR:**
María Eugenia Gutiérrez Pico Yerman Sánchez Ascensio GSIF José William Londoño Roldan.	Coordinador Seguridad Informática – Ing. Diego Fernando Galeano Jefe Tecnología e Innovación Sistemas – Ing. Tatiana Angarita Rodríguez	Director General – Dr. Jorge Ricardo León Franco. Jefe Tecnología e Innovación Sistemas – Ing. Tatiana Angarita Rodríguez
FECHA DE ELABORACIÓN: Junio de 2007	**FECHA DE REVISIÓN:** Mayo a Julio de 2022	**FECHA DE APROBACIÓN:**