1. INTRODUCCIÓN

Oftalmólogos Asociados de la Costa S.A.S determina la información como un activo de alta importancia para la entidad que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

En el presente manual se establecen las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con Oftalmólogos Asociados de la Costa S.A.S; estas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001:2013 y al modelo de seguridad y privacidad de la información de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. OBJETIVO

Establecer las políticas que regulan la seguridad de la información y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la clinica, bajo el liderazgo del Área de Tecnologías y Sistemas de Información.

3. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con Medicosta, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el comité de seguridad de la información.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La presente política aplica para todos los empleados, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con oftalmólogos Asociados de la Costa S.A.S

5. TERMINOS Y DEFINICIONES

- Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.

- Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

- 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 que tenga valor para la organización.

Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la clinica. Se pueden clasificar de la siguiente manera:

- Datos: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en el DAPRE. Ejemplo: archivo de Word “listado de personal.docx”.

- Aplicaciones: Es todo el software que se utiliza para la gestión de la información. Ejemplo: SIGEPRE.

- Personal: Es todo el personal del DAPRE, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información del DAPRE. Ejemplo: Pedro Pérez.

- Servicios: Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios. Ejemplo: Publicación de hojas de vida, solicitud de vacaciones.

- Tecnología: Son todos los equipos utilizados para gestionar la información y las comunicaciones.
  Ejemplo: equipo de cómputo, teléfonos, impresoras.

- Instalaciones: Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Oficina Pagaduría.

- Equipamiento auxiliar: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

- Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

- Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

- Almacenamiento en la Nube: Del inglés cloud storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet. Esos lugares de Internet son aplicaciones o servicios que almacenan o guardan esos archivos.

- Amenaza: Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- Análisis de riesgos: A partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

- Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- 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, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

- Base de datos de gestión de configuraciones (CMDB, Configuration Management Database): Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

- Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

- Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave; un mensaje o texto cuyo contenido se quiere proteger.

- Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

- Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- Control: son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).

- Declaración de aplicabilidad (SOA - Statement of Applicability): 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 agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto a resaltar es el gran daño a la imagen y reputación de las entidades que estas acciones dejan en el ambiente público.

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

- Directiva: Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, 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.

- Evento: Según [ISO IEC TR 18044:2004]: 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.

- Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- FTP: (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar y/o subir archivos a él.
- Gestión de claves: Controles referidos 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 la valoración de riesgos y el tratamiento de riesgos.

- Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

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

- Incidente: Según [ISO IEC 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 los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

- Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

- Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados.

- Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos.

- Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red1 o faciliten información con clasificación confidencial o superior.

En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

- Protección de activos: Seguridad de la Información, ASIS International, 2011.

- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISO IEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

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

- ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

- ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

- ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

- ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

- ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

- ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

- ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información. Keyloggers: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este termino con malware del tipo daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

- Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

- No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

- PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

- Phishing: Tipo de 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 (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

- Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

- Plan de tratamiento de riesgos (Risk treatment plan): 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 la misma.

- Política de seguridad: Definición en la cual se establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- Punto Único de Contacto (PUC): Entiéndase como mesa de ayuda de acuerdo a las mejores prácticas basadas en ITIL.

- Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

- Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

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

- 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 de la información: Según [ISO IEC 27002:2005]: 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.

- SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera,

monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

- Spamming: Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

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

- Spoofing: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

- Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

- 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: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores del DAPRE, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red del DAPRE 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: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tardo tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

- VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

- Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

6. POLÍTICA DEL SIGEPRE

El Sistema de Gestión de Seguridad de la Información – SGSI, hace parte del Sistema Integrado de Gestión de la Presidencia de la República – SIGEPRE; por esta razón la política de seguridad de la información se describe en la política del SIGEPRE:

En el Departamento Administrativo de la Presidencia de la República, apoyamos al Presidente de la República en el cumplimiento de su Plan de Gobierno y servimos a la ciudadanía e instituciones usuarias, articulando esfuerzos con entidades del sector público y privado; implementando un sistema integrado de gestión, alineado con los Objetivos de Desarrollo Sostenible y el Modelo Integrado de Planeación y Gestión, dando cumplimiento a los requisitos legales, técnicos y de otro tipo, comprometidos con el mejoramiento continuo de la gestión así:

Con la calidad en la prestación de los servicios, de manera eficiente, transparente y oportuna, cumpliendo con las necesidades y expectativas pertinentes de nuestros clientes, usuarios y partes interesadas; con tecnología de última generación y gestión financiera con estándares internacionales; y con gestión documental como apoyo a la gestión del conocimiento, contando con personal competente y comprometido al servicio del país y de los ciudadanos.

Mediante el cumplimiento de los objetivos, requisitos y controles aplicables, al Sistema de Gestión de Seguridad de la información, que permiten mantener la confidencialidad, integridad y disponibilidad de los activos de información, con la promoción de una cultura en seguridad, para evitar y administrar incidentes; fomentando la mejora continua, a través de buenas prácticas de autocontrol y de la estrategia “La Seguridad Soy Yo”.

Con la protección del medio ambiente y la prevención de la contaminación en las actividades que generan impacto adverso sobre el medio ambiente; a través de acciones para la conservación de los recursos naturales, con el uso eficiente de agua, energía y papel, con la adecuada gestión de los residuos y el control de las emisiones contaminantes; y con iniciativas que generen efecto positivo para el desarrollo sostenible, como la adopción de procesos y tecnologías limpias, el fomento de buenas prácticas ambientales y de una cultura cuidadosa de la “Casa Común” - el Planeta, entre nuestros colaboradores y los grupos de interés en los que nos sea posible influir, en apoyo a la adaptación y mitigación del cambio climático.

Con la seguridad y salud en el trabajo de nuestros funcionarios, contratistas, visitantes y partes interesadas, en actividades propias de la misión y otras complementarias al desempeño de los procesos y funcionamiento de la Entidad; dirigiendo acciones para reducir y eliminar peligros y factores de riesgo de enfermedad laboral, incidentes, accidentes de trabajo y tránsito; promoviendo ambientes de trabajo seguros y estilos de vida saludable, fomentando la prevención del alcoholismo y la drogadicción, el autocuidado y la bioseguridad; y disponiendo de canales de comunicación para la consulta y participación de los colaboradores y partes interesadas.

Tomado de: Manual del Sistema Integrado de Gestión de la Presidencia de la República SIGEPRE M-DE-02

7. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Generar una adecuada seguridad y protección de la información de los procesos de Oftalmólogos Asociados de la Costa S.A.S a través de pautas, directrices y reglas, estableciendo dentro del Plan Estratégico de TI su liderazgo y desarrollo y renovar la gestión de la Entidad bajo la norma NTC-ISO-27001:2013, a partir de la Certificación en Seguridad de la Información.

Directrices:

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
- Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los funcionarios, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones del Medicosta.
- Todos los usuarios de los sistemas de información y telecomunicaciones de la clinica, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente Manual de Políticas de Seguridad de la Información.
- Con la gestión de riesgos de seguridad de la información, se busca mediante la aplicación de las diferentes etapas preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, con los controles y la evaluación de su aplicación en el monitoreo trimestral se avalúa la eficacia de su aplicación.

- Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información - SGSI, los cuales estarán a cargo de la Oficina de Control Interno.

- Oftalmólogos Asociados de la Costa S.A.S debe contar con dispositivos y sistemas de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.

- Los Jefes de Área o dependencia deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de Oftalmólogos Asociados de la Costa S.A.S.

- Oftalmólogos Asociados de la Costa S.A.S debe mantener correspondencia y vínculos técnicos entre las normas NTC-IS0 9001, NTC- IS0-IEC 27001, NTC-ISO 14001 y NTC-ISO 45001.

- Se utiliza el requisito de la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013; numeral 9.3 Revisión por la dirección en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continúa.

7.1. Política de estructura organizacional de seguridad de la información

Oftalmólogos Asociados de la Costa S.A.S en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información - SGSI, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, así como la existencia del Comité de Seguridad de la información.

El Área de Tecnologías y Sistemas de Información debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información a los funcionarios disponibles en la clinica, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

Los roles y responsabilidades de seguridad de la información, se encuentran descritos en la Matriz Raci que se encuentra en el Lineamiento de Administración de Seguridad L-T-03.

7.2. Política para uso de dispositivos móviles

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smart phones”, tabletas), entre otros, suministrados por la entidad y personales que hagan uso de los servicios de información de la Entidad.

En el caso del nivel directivo se autoriza el uso de WhatsApp únicamente en dispositivos suministrados por Oftalmólogos Asociados de la Costa S.A.S, no se permite por esta aplicación, el envío de fotografías, audios, y videos y cualquier otro tipo de archivo clasificados como información pública reservada o información pública clasificada.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Las Directrices de uso de dispositivos móviles se encuentran definidas en el Lineamientos para Uso de Dispositivos Móviles L-TI-30.

7.3. Política de seguridad para los recursos humanos

Oftalmólogos Asociados de la Costa S.A.S implementa acciones para asegurar que los empleados, contratistas y demás colaboradores de la Entidad, entiendan sus responsabilidades, como usuarios y responsabilidad de los roles asignados, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Los candidatos, aspirantes, contratistas y proveedores deben dar aprobación a Oftalmólogos Asociados de la Costa S.A.S para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, lo que se deberá reflejado en las cláusulas de los contratos y en el aplicativo “aspirantes”.

Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

Se debe asegurar que los empleados, contratistas y demás colaboradores de Oftalmólogos Asociados de la Costa S.A.S, adopten sus responsabilidades en relación con las políticas de seguridad de la información del DAPRE y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información, el conocimiento de las políticas de seguridad de la información se notificaran mediante el diligenciamiento y firma del formato de entrega de usuario.

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la ley 734 de 2013, ley 200 de 1995 y demás normas que reglamenten los procesos disciplinarios para los empleados del estado.

7.4. Política de gestión de activos de Información

Oftalmólogos Asociados de la Costa S.A.S es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los empleados y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

Oftalmólogos Asociados de la Costa S.A.S es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores del (denominados “usuarios”) que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

Oftalmólogos Asociados de la Costa S.A.S mantiene un inventario actualizado de sus activos de información de acuerdo al Instructivo registro y actualización de los inventarios de información, quedando bajo la responsabilidad de cada propietario de información y centralizado por el Área de Tecnologías y Sistemas de Información, el cual se publicará en la página web de la Presidencia de la República de Colombia.

La Entidad debe realizar el tratamiento de información documental de acuerdo a lo establecido en el manual de la institución.

Una parte de los activos de TIC, se debe mantener en una base de datos bajo la responsabilidad del Área de Tecnologías y Sistemas de Información. (CMDB - Base de datos de gestión de configuraciones / Configuration Management Database).

7.5. Política de uso de los activos

La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

Las directrices de uso de activos se encuentran definidas en el Lineamiento de uso de activos de Información y dispositivos móviles.

7.6. Política de uso de estaciones cliente

Oftalmólogos Asociados de la Costa S.A.S establece reglas que permitan orientar que la seguridad es parte integral de los activos de información y mediante la correcta utilización de estaciones por los usuarios finales.

7.7. Política de uso de internet

La Entidad permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
El Jefe del Área de Tecnologías y Sistemas de Información administrará autorización los cambios solicitados de permisos de navegación a los usuarios de la institución, previa solicitud del Jefe de cada una de las dependencias, de acuerdo a Lineamientos de Control de Acceso y Procedimiento para solicitud de creación de cuenta de usuario y servicios de tecnología de información.

El Área de Tecnologías y Sistemas de Información implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

Los usuarios de los activos de información del Oftalmólogos Asociados de la Costa S.A.S tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a Jefe de Área de Tecnologías y Sistemas de información, para que sea autorizado por el Comité de Seguridad de la Información y será objeto de auditorías de seguridad mediante el módulo de seguridad web de la entidad.

7.8. Política de calificación de la información

Oftalmólogos Asociados de la Costa S.A.S consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo al tipo de calificación establecido por la ley y Medicosta, define reglas de como calificar la información, liderado por el proceso de Gestión Documental de la Entidad.

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o
- medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.

- Información o conocimiento transmitido de manera verbal o por cualquier otro medio
- de comunicación.

- Los usuarios responsables de la información del Medicosta, 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.

- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para el DAPRE; Independiente del tipo de activo, se deben considerar las siguientes características.

- El activo de información es reconocido como valioso para el Oftalmólogos Asociados de la Costa S.A.S.

- No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
- Las categorías de calificación de la información son: INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.

- Se debe monitorear periódicamente la aplicación de la Guía para la calificación de acceso a la información producida por Medicosta.

7.9. Política de manejo disposición de información, medios y equipos

La entidad establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por el Oftalmólogos Asociados de la Costa S.A.S, velando por la disponibilidad y confidencialidad de la información.

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

En los casos en los que se almacene información en las pantallas y equipos que se encuentran en las salas de reuniones de la Entidad, salas de juntas y salones de capacitación; las personas que han realizado la reunión, en el momento que no se requiera su uso en estos dispositivos, deben eliminarla de forma permanente; con el fin de evitar que personas no autorizadas puedan conocerla.

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

Se debe aplicar el procedimiento de borrado seguro en los equipos de cómputo y demás dispositivos, una vez se realiza su devolución a almacén para dar de baja de bienes Ver: Procedimiento de Baja de Bienes de acuerdo a lo definido por Oftalmólogos Asociados de la Costa S.A.S, en el Procedimiento de Borrado Seguro para equipos.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Subdirección General de Medicosta y será objeto de auditorías de seguridad mediante el módulo de prevención de pérdidas de datos de la entidad.

Se debe implementar el procedimiento para la transferencia de medios físicos.

Para los soportes documentales asociados a la Tablas de Retención Documental TRD, aplicar lo establecido en el Manual de Gestión Documental, Guía para la Calificación de acceso a la Información producida por el y Procedimiento eliminación de documentos.

Las actividades se definen en el Procedimiento eliminación de Documentos, Procedimiento de Borrado Seguro para equipos y Procedimiento de Baja de Bienes

7.10. Política de control de acceso

La Entidad define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de Oftalmólogos Asociados de la Costa S.A.S, considerándolas como importantes para el SGSI.

Todo aplicativo informático o software debe ser comprado o aprobado por el Área de Tecnologías y Sistemas de información en concordancia con la política de adquisición de bienes de la entidad de acuerdo con lo definido en el proceso Adquisición de Bienes y Servicios.

El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.

El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.

Para el acceso a los espacios de archivo tanto en las dependencias como en el Archivo Central, se debe dar aplicación a los controles establecidos en el Lineamiento para el acceso a los espacios de archivo.

Los funcionarios, contratistas y demás colaboradores, que tengan bajo su responsabilidad la custodia de la información física almacenada en los archivadores que se encuentra en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave. Se recomienda que las llaves se guarden en un sitio seguro, bajo la custodia de las personas que la dependencia estime conveniente, lo anterior, siguiendo la Guía para la Conservación de Documentos.

7.11. Política de establecimiento, uso y protección de claves de acceso

Ningún usuario deberá acceder a la red o a los servicios TIC, utilizando una cuenta de usuario o clave de otro usuario.

Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó la clave.

Oftalmólogos Asociados de la Costa S.A.S suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose a PUC (Punto Único de Contacto), en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte del Jefe de Área de Tecnologías y Sistemas de información).

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible, se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del Área de Tecnologías y Sistemas de la Información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Jefe del Área de Tecnologías y Sistemas de la Información.

Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnologías y Sistemas de la Información son de uso personal e intransferible.

Los Administradores de los sistemas de Información y el personal del Área de Tecnologías y Sistemas de la Información deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

Las Directrices de establecimiento, uso y protección de claves de acceso, se encuentran definidas en el documento de Lineamientos para el control de acceso.

7.12. Política de uso de discos de red o carpetas virtuales

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Las Directrices de uso de uso de discos de red o carpetas virtuales se encuentran definidas en el documento de Lineamiento de uso de servicios de.

7.13. Política de uso de puntos de red de datos (red de área local – LAN)

Asegurar la operación correcta y segura de los puntos de red.

Las Directrices de uso de puntos de red de datos, se encuentran definidas en el documento de Lineamiento de uso de servicios.

7.14. Política de uso de impresoras y del servicio de Impresión

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

Las Directrices de uso de impresoras y servicio de impresión, se encuentran definidas en el documento de Lineamiento de uso de servicios.

7.15. Política de controles criptográficos

Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

La Entidad no establece un lineamiento de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.
Se debe instalar y configurar herramienta de cifrado de información en los portátiles de la Entidad. Las Directrices controles criptográficos se encuentran definidas en el Documento de Lineamientos Controles criptográficos.

7.16. Política de seguridad física

Implementar el programa de seguridad física para el acceso a las instalaciones que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.

La Jefatura para la Protección Presidencial y el Área Administrativa deben implementar un sistema de seguridad física para las instalaciones de Oftalmólogos Asociados de la Costa S.A.S.

El Área de Tecnologías y Sistemas de Información debe tiene implementadas alarmas de detección de intrusos a los centros de datos y centros de cableado de Oftalmólogos Asociados de la Costa S.A.S.

El Área Administrativa del DAPRE debe mantener actualizado es programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a la Entidad.

La Jefatura para la Protección Presidencial informará las debilidades que encuentren a nivel de barreras físicas a la Subdirección General de Oftalmólogos Asociados de la Costa S.A.S para aprobación y corrección.

7.17. Políticas de seguridad del centro de datos y centros de cableado

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los sistemas de información o sus
- conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Cada Gabinete o armario contiene llave de ingreso y/o tarjeta de proximidad, así como cada centro de cableado, las cuales deben permanecer almacenadas en la debida caja de seguridad de doble factor (llave y clave) dispuesta para ello dentro del centro de cómputo.

Las Directrices de seguridad del centro de datos y centros de cableado, se encuentran definidas en el documento de Lineamientos para el control de acceso.

7.18. Política de seguridad de los equipos

Asegurar la protección de la información en los equipos.

En el caso que se requiera realizar el retiro de activos de información de las sedes de la Entidad, ya sean documentos, equipos tecnológicos que contengan información, se debe realizar el registro en el aplicativo: “Salida de elementos” que se encuentra en Intranet o diligenciar el formato Autorización Entrada y Salida de Elementos. Ver Procedimiento salida e Ingreso de bienes.
Las Directrices de seguridad de equipos se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones.

7.19. Política de escritorio y pantalla limpia

Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con Oftalmólogos Asociados de la Costa S.A.S debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones de Oftalmólogos Asociados de la Costa S.A.S deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Los usuarios de los sistemas de información y comunicaciones de Oftalmólogos Asociados de la Costa S.A.S deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

7.20. Política de seguridad de las operaciones de TIC

Definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de Oftalmólogos Asociados de la Costa S.A.S, con el fin de robustecer la continuidad de los sistemas de TIC.

Las Directrices de uso de seguridad de las operaciones de TIC se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones.

7.21. Política de adquisición, desarrollo y mantenimiento de sistemas de información

Garantizar que la seguridad es parte integral de los sistemas de información.

Las Directrices de adquisición, desarrollo y mantenimiento de sistemas de Información, se encuentran definidas en el documento de Lineamiento de adquisición, desarrollo y mantenimiento de sistemas de información.

7.22. Política de respaldo y restauración de información

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por entidad.

Los administradores de la plataforma de backup de Oftalmólogos Asociados de la Costa S.A.S, verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Los administradores de la plataforma de copias de respaldo (backup) de la entidad, quincenalmente deben generar tareas de restauración aleatorias de la información, quedando registradas en el formato diligenciado de Creación y ejecución de restauración de información y mensualmente se deben generar restauraciones de Bases de datos definidas por el administrador de Base de Datos; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la Entidad, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.

Las Directrices de respaldo y restauración de Información, se encuentran definidas en el documento de Lineamiento de copias de respaldo y restauración.

7.23. Política para realización de copias en estaciones de trabajo de usuario final

Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el Área de Tecnologías y Sistemas de Información generará una copia de la información contenida en el equipo asignado al perfil del usuario (C:\usuarios\nombre-usuario), a una unidad de almacenamiento.

Una vez esta información se encuentre ubicada en la unidad de almacenamiento, se le realiza copia de seguridad mensual en cinta magnética, la cual es enviada al custodio de medios magnéticos, para conservar esta información en el tiempo.

Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe enviar una comunicación oficial al Área de Tecnologías y Sistemas de Información, quien escalará la solicitud ante el comité de seguridad de la Información, para evaluar la pertinencia de la restauración y entrega de la copia.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la Entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal e individual de la Subdirección General de Oftalmólogos Asociados de la Costa S.A.S.

Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB y el agente de cliente fuga de información DLP instalado, el cual mantendrá un registro de los archivos copiados.

Las Directrices de copias en estaciones de trabajo de usuario final, se encuentran definidas en el documento de Lineamiento de copias de respaldo y restauración.

7.24. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) Generados por los sistemas de información y comunicaciones de Oftalmólogos Asociados de la Costa S.A.S.

Las Directrices de registro y seguimiento de eventos de Sistemas de Información y comunicaciones, se encuentran definidas en el documento de Lineamiento para registro y seguimiento de eventos de sistemas de información y comunicaciones.

7.25. Política de control de software operacional de Oftalmólogos Asociados de la Costa S.A.S

Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes a Oftalmólogos Asociados de la Costa S.A.S.

Las Directrices de control de software operacional se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones.

7.26. Política de gestión de vulnerabilidades

Evitar la utilización de vulnerabilidades técnicas de los sistemas de información y comunicaciones de Oftalmólogos Asociados de la Costa S.A.S, e implementar los lineamientos para gestión de vulnerabilidades.

Las directrices de gestión de vulnerabilidades se encuentran definidas en el documento de Lineamiento para gestión de incidentes y vulnerabilidades de Seguridad de la Información.

7.27. Política de seguridad de las comunicaciones

Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de Oftalmólogos Asociados de la Costa S.A.S.

7.28. Política para la transferencia de información

Proteger la información transferida al interior y exterior de Oftalmólogos Asociados de la Costa S.A.S.

El Área de Tecnologías y Sistemas de Información, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

Las directrices para transferencia de información se encuentran definidas en el documento de Lineamientos para acuerdos de transferencia de información.

7.29. Política de uso de correo electrónico

Definir las pautas generales para asegurar una adecuada protección de la información de Oftalmólogos Asociados de la Costa S.A.S, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Todos los mensajes de correo electrónico son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Entidad.

7.30. Políticas específicas para webmaster

Proteger la integridad de las páginas Web institucionales, el software y la información contenida. Las Directrices para web masters se encuentran definidas en el documento de Lineamientos para Usuarios y administradores de TI, en protección de Información y Lineamiento de la Política Editorial y Actualización de Contenidos Web.

7.31. Políticas específicas para funcionarios y contratistas del Área de Tecnologías y Sistemas de Información

Definir las pautas generales para asegurar una adecuada protección de la información de Oftalmólogos Asociados de la Costa S.A.S por parte de los funcionarios y contratistas de TI de la entidad.

7.32. Política de tercerización u outsourcing

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de Oftalmólogos Asociados de la Costa S.A.S, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por Medicosta.

El Área de Tecnologías y Sistemas de Información deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de Oftalmólogos Asociados de la Costa S.A.S. Los empleados que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

7.33. Política de gestión de los incidentes de la seguridad de la información

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

7.34. Política de cumplimiento de requisitos legales y contractuales

Prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.

Oftalmólogos Asociados de la Costa S.A.S respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.

Oftalmólogos Asociados de la Costa S.A.S establecerá el procedimiento para protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

El Área de Tecnologías y Sistemas de Información deberá garantizar que todo el software que se ejecute los activos de información de Oftalmólogos Asociados de la Costa S.A.S esté protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución y uso.

Los usuarios y/o funcionarios de Oftalmólogos Asociados de la Costa S.A.S deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.

El Área Tecnologías y Sistemas de Información realizará el procedimiento de Copias de respaldo (backup) de los registros alojados en los sistemas de información.
Oftalmólogos Asociados de la Costa S.A.S implementará los lineamientos para asegurar la privacidad y protección de datos personales, definiendo claramente los deberes en las actividades de recolección, procesamiento y transmisión de los mismos.

Las Dependencias del Departamento Administrativo de la Presidencia que tratan con datos personales de funcionarios, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Entidad, así mismo los Jefes de dependencias deben asegurar que tendrán acceso a los datos personales únicamente los funcionarios que tengan una necesidad laboral legitima.

Oftalmólogos Asociados de la Costa S.A.S a través del Área Tecnologías y Sistemas de Información debe implementar métodos y herramientas que permitan proteger la información personal de los funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro tipo de almacenamiento o repositorio previniendo su divulgación, alteración o eliminación sin la autorización.

7.35. Política de revisiones de seguridad de la información

Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados en Oftalmólogos Asociados de la Costa S.A.S.

Oftalmólogos Asociados de la Costa S.A.S realiza auditorias con personal externo a la entidad al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.

Los Altos Directivos, Altos Consejeros, Consejeros Presidenciales, Directores, Secretarios, Jefes de Oficina, Jefes de Área, deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

Medicosta asigna un empleado para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de gobierno.

El Área Tecnologías y Sistemas de Información debe establecer el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.

7.36. Políticas específicas para usuarios de Oftalmólogos Asociados de la Costa S.A.S

Definir las pautas generales para asegurar una adecuada protección de la información de Oftalmólogos Asociados de la Costa S.A.S por parte de los usuarios de la entidad.

Las directrices se encuentran definidas en el documento de Lineamientos para usuarios y administradores de TI, en protección de Información.

7.37. Política de retención documental

Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley General de Archivos, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

Los tiempos de retención de los archivos durante su ciclo vital están establecidos en la Tabla de Retención Documental aprobada y convalidada y deberán ser aplicadas por cada una de las dependencias de Oftalmólogos Asociados de la Costa S.A.S en su etapa de gestión y así mismo, dar cumplimiento al Cronograma de Transferencias primarias.

Gestión Documental aplicará la Tabla de Retención Documental en la fase de Archivo Central y dará cumplimiento a la normatividad archivística para realizar las Transferencias Secundarias.

La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

7.38. Política de uso de mensajería instantánea y redes sociales

Oftalmólogos Asociados de la Costa S.A.S define las pautas generales para asegurar una adecuada protección de la información de la Presidencia de la República, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier empleado, contratista o colaborador de Oftalmólogos Asociados de la Costa S.A.S, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instaram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la entidad, debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario institucional.

No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

Las personas designadas para el manejo operativo de las redes sociales en la Entidad (Community Manager), los funcionarios, contratistas y demás colaboradores de Oftalmólogos Asociados de la Costa S.A.S, deben acatar las directrices dadas en la circular 01 de2019 Manejo y uso de redes sociales.

La dependencia que requiera la apertura de una red social bajo el dominio de Presidencia o que tenga nombre de las dependencias adscritas al Departamento Administrativo de la Presidencia de la República; debe presentar una solicitud por servicios en línea, motivada relacionando la necesidad, objeto y alcance de la cuenta institucional, enunciando los datos personales de los funcionarios administradores y dinamizadores de la red social.

Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de las mismas y realizando el cambio periódicamente, de acuerdo a lo establecido en el Manual de Políticas de Seguridad de la Información, “Política: Establecimiento, uso y protección de claves de acceso”.

El Equipo de Respuesta a Incidentes de Seguridad de la información, conformado en la jefatura para la Protección Presidencial; realiza la verificación de la adopción de medidas y controles de seguridad, encaminadas a evitar el acceso abusivo a la plataforma, que puedan afectar la imagen y la credibilidad de la entidad. Este acompañamiento es realizado con los diferentes gestores de comunicaciones (comunity manager), quienes son los encargados de crear, gestionar las audiencias en las redes sociales de la Entidad.

No se deben vincular cuentas de correo electrónico personales o comerciales, a las redes sociales que se apertura bajo el dominio de Oftalmólogos Asociados de la Costa S.A.S.

7.39. Política de tratamiento de datos personales

Establecer los lineamientos para administración y tratamiento de datos personales en el Departamento Administrativo de la Presidencia de la República.

Datos de menores de edad: El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia”. Datos personales y biométricos: En el ingreso a los edificios del Departamento Administrativo de la Presidencia de la República en los cuales se realiza recolección de datos personales y datos biométricos, se encuentran avisos y habladores, con el fin que sean conocidos por las personas que ingresan a la Entidad, con la siguiente información:

Al momento de registrar su huella, usted está aceptando el tratamiento de datos personales, si considera que la información registrada por usted, deba ser objeto de corrección, actualización o supresión, por favor solicitarlo a talento humano.

Se busca definir el mensaje de “Zona Monitoreada”, con el fin que las personas que se encuentran en los espacios de la Entidad, conozcan que están siendo monitoreados.

En los documentos formales en los cuales la Entidad recolecta información de los funcionarios, contratistas y demás colaboradores, se incluye la siguiente información:

El registro de datos personales en este formato, autoriza al Departamento Administrativo de la Presidencia de la República para la recolección, almacenamiento y uso de los mismos, en cumplimiento a la Ley 1581/12 y el Decreto 1377/13 y las demás normas que modifiquen, adicionen o complementen.

Conozca la política de tratamiento de los datos personales del Departamento Administrativo de la Presidencia de la República a través del siguiente link: http://es.presidencia.gov.co/dapre/politica-privacidad-condiciones-uso.”

Los organizadores de reuniones virtuales, deben indicar a los asistentes que se va a realizar la grabación de la misma, de tal forma que si algún asistente no está de acuerdo lo debe indicar al organizador; si no se recibe alguna observación, se da por entendido que ha dado su aprobación.

7.40. Política de trabajo en casa

Mediante Directiva Presidencial N° 2 de 12 de marzo de 2020: Medidas para atender la contingencia generada por el COVID-19, a partir del uso de tecnologías de la información y las telecomunicaciones – TIC. Se define, que como medida preventiva se pueda realizar trabajo en casa por medio del uso de las TIC, sin que constituya como modalidad de teletrabajo, descrito en el numeral 4 del artículo 6 de la Ley 1221 de 2008 “por el cual se establecen normas para promover y regular el teletrabajo” Por lo tanto, para el caso se denomina: trabajo en casa. Esta actividad se realiza mediante conexión remota a los equipos de la Entidad, ya que Oftalmólogos Asociados de la Costa S.A.S no cuenta con la implementación de teletrabajo en términos definidos por la Ley 1221 de 2008.

8. PROCEDIMIENTOS QUE APOYAN LA POLÍTICA DE SEGURIDAD

Los procedimientos son uno de los elementos dentro de la documentación del Manual de Políticas de Seguridad de la Información. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él, se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.
Los usuarios de Oftalmólogos Asociados de la Costa S.A.S pueden consultar las descripciones detalladas de cada procedimiento a través del sistema integrado de gestión SIGEPRE o en el Área de Tecnologías y Sistemas de Información de Oftalmólogos Asociados de la Costa S.A.S.

8.1. Procedimiento de control de documentos

Garantiza que la organización cuente con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa la entidad en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión, sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso, sean confiables y se mantengan actualizados, una vez se evidencie la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen; de igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

8.2. Procedimiento de control de registros

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que registro que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la organización y generar residuos sólidos como papel mal utilizado.

8.3. Procedimiento de auditoría interna

La auditoría interna es una herramienta para la alta dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión.

Se hacen auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-IS0: 9001 y NTC-IS0: 27001 se utiliza el documento administración de auditorías internas al SIGEPRE. Proceso evaluación control y mejoramiento.

8.3.1. Procedimiento de acción correctiva

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de Oftalmólogos Asociados de la Costa S.A.S, así como: definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-IS0: 9001 y NTC-IS0: 27001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento.

8.3.2. Procedimiento de acción preventiva

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real en el sistema de gestión de seguridad de la información y eliminar sus causas.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-ISO: 9001 y NTC-ISO: 27001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento. Proceso de evaluación, control y mejoramiento.

8.4. Procedimiento de revisión del Manual de Políticas de Seguridad de la Información

El objetivo de este procedimiento es revisar, por parte de la dirección o su representante, el Manual de la Políticas de Seguridad de la Información del Departamento Administrativo de la Presidencia de la República en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continua.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTC-ISO: 9001 y NTC-ISO: 27001 se utilizan los requisitos: 5.1.d Compromisos de la dirección y 5.6 Revisión por la dirección

9. PROCESO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información del Oftalmólogos Asociados de la Costa S.A.S, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y los otros colaboradores del violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al proceso de gestión del Área de Talento Humano.

Actuaciones que conllevan a la violación de la seguridad de la información establecidas por el Oftalmólogos Asociados de la Costa S.A.S:

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a carpetas de otros procesos, unidades, grupos o áreas, sin autorización y no reportarlo al punto único de contacto o al CSIRT - Equipo de respuesta a incidentes de seguridad de la información, conformado en la Jefatura para la Protección Presidencial.
- No mantener la confidencialidad de las contraseñas de acceso a las redes sociales y cuentas de correo electrónico asociadas a las mismas, o permitir que otras personas accedan con el usuario y clave del titular.
- Permitir el acceso u otorgar privilegios de acceso a las redes sociales a personas no autorizadas.
- Ejecución de cualquier acción que conlleve a la difamación, que llegue afectar la reputación o presentar una mala imagen a la Presidencia de la República.
- o Eliminar documentos de archivo

- Retener sin la debida justificación o enviar intencionalmente a un destinatario que no corresponde las comunicaciones recibidas en la entidad.
- Ocasionar daño o dar lugar a la pérdida de expedientes, documentos o archivos que hayan llegado a su poder por razón de sus funciones/actividades.
- Dar lugar al acceso o exhibir expedientes, documentos, información o archivos a personas no autorizadas.
- Realizar actividades tales como borrar, alterar o eliminar información de manera malintencionada. Sustraer de las instalaciones del DAPRE, documentos de archivo sin la debida autorización.
- No hacer entrega de los documentos de archivos que se encuentren a cargo de los funcionarios y contratistas, debidamente inventariados, cuando se presente su retiro o traslado.
- No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.
- No actualizar la información de los activos de información a su cargo.
- Calificar y registrar de manera inadecuada la información, desconociendo los estándares
- establecidos para este fin.
- No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral, “documentos impresos que contengan información pública reservada, información pública clasificada”.
- No guardar la información digital, producto del procesamiento de la información perteneciente a Oftalmólogos Asociados de la Costa S.A.S.
- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
- Dejar las gavetas abiertas o con las llaves puestas en los escritorios,
- Dejar los computadores encendidos en horas no laborables.
- Permitir que personas ajenas, deambulen sin acompañamiento, al interior de las
- instalaciones, en áreas no destinadas al público.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información de la entidad.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
- Enviar información pública reservada y/o información pública clasificada, por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.

- Utilizar equipos electrónicos o tecnológicos desatendidos o que, a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
- Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada por el Área de Tecnologías y Sistemas de Información.
- Permitir el acceso de funcionarios a la red corporativa, sin la autorización de Área de
- Tecnologías y Sistemas de Información.
- Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de Oftalmólogos Asociados de la Costa S.A.S.
- No cumplir con las actividades designadas para la protección de los activos de información del Oftalmólogos Asociados de la Costa S.A.S.
- Descuidar documentación con información pública reservada o clasificada de la entidad, sin las medidas apropiadas de seguridad que garanticen su protección.
- Registrar información pública reservada o clasificada, en pos-it, apuntes, agendas, libretas, etc. Sin el debido cuidado.
- Almacenar información pública reservada o clasificada, en cualquier dispositivo de almacenamiento que no permanezca al DAPRE o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos, sin la debida autorización.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- Promoción o mantenimiento de negocios personales, o utilización de los recursos tecnológicos de Oftalmólogos Asociados de la Costa S.A.S para beneficio personal.
- El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de Oftalmólogos Asociados de la Costa S.A.S.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de Oftalmólogos Asociados de la Costa S.A.S, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información del Oftalmólogos Asociados de la Costa S.A.S.
- El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de Oftalmólogos Asociados de la Costa S.A.S.
- El que viole datos personales de las bases de datos de Oftalmólogos Asociados de la Costa S.A.S.
- El que superando las medidas de seguridad informática suplante un usuario ante los
- sistemas de autenticación y autorización establecidos por el Oftalmólogos Asociados de la Costa S.A.S.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de Oftalmólogos Asociados de la Costa S.A.S o permitir que otras personas accedan con el usuario y clave del titular a éstos.
- Permitir el acceso u otorgar privilegios de acceso a las redes de datos del DAPRE a personas no autorizadas.

- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de Oftalmólogos Asociados de la Costa S.A.S o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por Oftalmólogos Asociados de la Costa S.A.S.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores
- portátiles que contengan información institucional sin la autorización pertinente.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- o No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de Oftalmólogos Asociados de la Costa S.A.S, para traslado, reasignación o para disposición final.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de Oftalmólogos Asociados de la Costa S.A.S o de alguno de sus funcionarios.
- Realizar cambios no autorizados en la plataforma tecnológica de Oftalmólogos Asociados de la Costa S.A.S.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos
- portátiles institucionales, cuyo uso no esté autorizado por el Área de Tecnologías y Sistemas
- de Información de Oftalmólogos Asociados de la Costa S.A.S.
- Copiar sin autorización los programas de Oftalmólogos Asociados de la Costa S.A.S, o violar los derechos de autor o acuerdos de licenciamiento.

10. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la entidad, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

Prevenir interrupciones en las actividades de la plataforma informática de Oftalmólogos Asociados de la Costa S.A.S que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.

Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI de Oftalmólogos Asociados de la Costa S.A.S podrán ser restaurados dentro de escalas de tiempo razonables.
Oftalmólogos Asociados de la Costa S.A.S deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI del DAPRE de acuerdo con su impacto en el cumplimiento de la misión de la entidad.

- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definidaanteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

La continuidad del negocio deberá ser gestionada por la Dirección del Oftalmólogos Asociados de la Costa S.A.S.

La alta dirección de Oftalmólogos Asociados de la Costa S.A.S será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.

La alta dirección del Departamento, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

11. CUMPLIMIENTO

Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, personal en comisión permanente, contratistas y otros colaboradores de Oftalmólogos Asociados de la Costa S.A.S. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, el DAPRE tomará las acciones disciplinarias y legales correspondientes.

El Manual de la Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

12. CONTROLES

El Manual de la Política de Seguridad de la Información de Oftalmólogos Asociados de la Costa S.A.S esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología de Oftalmólogos Asociados de la Costa S.A.S pueden consultar los procedimientos a través del Área de Tecnologías y Sistemas de Información y/o en el SIGEPRE.

13. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA), es un documento que lista los objetivos y controles que se van a implementar en la Entidad, así como las justificaciones de aquellos controles que no van a ser implementados.

Para el caso específico de Oftalmólogos Asociados de la Costa S.A.S E, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO 27002, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica; y una vez se complete este análisis ya se puede realizar la Declaración de aplicabilidad. - SOA - Seguridad de la Información.

14. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- Artículo 20. Libertad de Información.
- Código Penal Colombiano - Decreto 599 de 2000
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las
- entidades y organismos del Estado, y demás normas que la modifiquen.
- Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI
- para el Estado Colombiano.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Ley 594 de 2000 - Ley General de Archivos.
- Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos,
- del comercio electrónico y de las firmas digitales y se establecen las entidades de
- certificación y se dictan otras disposiciones.
- Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
- Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso
- administrativo".
- Ley 1581 de 2012, "Protección de Datos personales".
- Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública
- nacional”.
- Ley 962 de 2005. “Simplificación y Racionalización de Trámite. Atributos de seguridad en la
- Información electrónica de entidades públicas;”
- Ley 1150 de 2007. “Seguridad de la información electrónica en contratación en línea”

- Ley 1341 de 2009. “Tecnologías de la Información y aplicación de seguridad”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de
- 2008”.
- Decreto 886 de 2014. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”.
- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

15. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 Sistemas de gestión de la seguridad de la información.
- Guía Técnica Colombiana GTC-ISO/IEC 27002:2015 Código de práctica para controles de seguridad de la información.
- Norma Técnica Colombiana NTC ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO IEC 27005 Information technology Systems- Security techniques- information security risk management.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC – ISO 19011:2018 Directrices para la Auditoría de los
- Sistemas de Gestión.

16. DOCUMENTOS ASOCIADOS

Los documentos mencionados en este documento, pueden ser consultados en SIGEPRE.