Manual de la Política de

Seguridad, Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios de la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza - Emaaf E.S.P.

Contenido

Tablas

INTRODUCCIÓN

La información como activo intangible, representa para la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza en -EMAAF E.S.P.,- el más alto valor puesto que a través de los datos consolidados y transformados en información, son requeridos para la toma de decisiones en el cumplimiento del componente estratégico y objetivos en pro de la visión de la empresa.

Las tecnologías de la información y las comunicaciones son clave para el buen manejo de la información, por lo cual es necesario integrar los componentes de hardware y software en el desarrollo diario de las funciones de la gestión del talento humano y la seguridad de la información como instrumentos que disminuyan la vulnerabilidad a accesos no autorizados y pérdida de información.

En este sentido la definición de la política general, ha sido un documento construido bajo una metodología y revisado bajo los lineamientos, estándares y la normatividad vigente, definiendo así, la gestión de la seguridad de la información durante las operaciones y la continuidad de la prestación de servicios públicos.

La implementación de la política general, está dada por la declaración de aplicabilidad que se encuentra en el presente Manual de la Política General de Seguridad, Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, con un alto grado de aseguramiento del riesgo, las buenas prácticas de la ISO/IEC 27001 anexo A y el Anexo 1, Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones que define los lineamientos para la implementación de la Política de seguridad digital.

El Manual de la Política General de Seguridad, Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, articula el ciclo del modelo de seguridad y privacidad de la información con sus tres fases (fase de planificación, de operación, de evaluación de desempeño y fase de mejoramiento continuo) con la relación entre la ciber seguridad y los ámbitos de esta (seguridad de la información, seguridad de las aplicaciones, ciber seguridad digital, seguridad de la Red, seguridad de Internet que redunda en la protección de la infraestructura de información crítica.

2. OBJETIVO

Proteger los activos de la información, grupos de valor, información, procesos, tecnologías incluido el hardware y software, mediante lineamientos para la aplicación de la seguridad de la información bajo el marco del Modelo Integrado de Planeación y Gestión -MIPG-.

3. ALCANCE

Las Políticas de la política general de seguridad de la información definidas en la Resolución 050/2022, son de obligatorio cumplimiento para todos los trabajadores oficiales, aprendices y contratistas de la Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza Emaaf E.S.P.

4. MARCO NORMATIVO

Constitución Política de Colombia Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar". De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.

Constitución Política de Colombia Articulo 20. Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura.

Ley 23 de 1982, Sobre derechos de autor.

Ley 527 de 1999, Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos.

Ley 594 de 2000, Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones.

Ley 603 de 2000, Por la cual se modifica el artículo 47 de la Ley 222 de 1995, Artículo 2. Artículo 2o. Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos.

Decreto 1747 de 2000, por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales.

Ley 679 de 2001, Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.

Ley 734 de 2002, Por medio de la cual se expide del código único disciplinario.

Ley 1032 de 2006, Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000.

Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

Ley 1341 de 2009, Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TI.

Ley 1273 de 2009, Por medio de la cual se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Ley 1336 de 2009 (Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.) por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

Ley 1437 DE 2011, por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Articulo 1 de la ley 1755 de 2015.

Ley 1474 DE 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales.

Ley 1672 de 2013, Lineamientos para la Adopción de una política Pública de gestión integral de residuos de aparatos eléctricos y electrónicos

Ley 1712 de 2014, Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información pública Nacional y se dictan otras disposiciones.

Ley 128 de 2018, Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Ley 1955 del 25 de mayo de 2019. "Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022. "Pacto por Colombia, Pacto por la Equidad". Incluyó el artículo 147 de Transformación Digital pública y 148 de Gobierno Digital como política de gestión y desempeño institucional.

Decreto 1474 de 2002, por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996).

Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.

Decreto 2609 de 2012. Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Decreto 103 de 2015, Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (DUR-TI).

Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

Decreto 1081 de 2015 (Decreto Reglamentario Único del Sector Presidencia de la Republica), Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, Título 1, Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.

Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función pública.

Decreto 1494 de 2015, Por el cual se corrigen yerros en la Ley 1712 de 2014.

El Decreto 1499 de 2017, modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, sustituyendo los Títulos 22 y 23 de la Parte 2

del Libro 2, en lo relacionado con el Sistema de Gestión y se establece su articulación con el Sistema de Control Interno; adoptando el Modelo Integrado de Planeación y Gestión – MIPG como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio. Así mismo, ubica en la dimensión tres (3) Gestión con valor para resultados, para el desarrollo de esta dimensión deberán tenerse en cuenta los lineamientos de las siguientes políticas de gestión: Política de Gobierno Digital y Seguridad Digital.

Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto No. 2106 del 22 de noviembre de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública."

Documento CONPES 3854, Política Nacional de Seguridad Digital.

Documento CONPES 3975, Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES).

Directiva Presidencial 02 del 2 de abril de 2019. Simplificación de la interacción digital los ciudadanos y el Estado.

Circular Externa Conjunta No. 04 del 5 de septiembre de 2019. Tratamiento de datos personales en sistemas de información interoperables.

Resolución 500 de 2021, por medio de la cual se establecen los lineamientos y estándares para la política de seguridad digital y se adopta modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"

Directiva presidencial 03 de 2021, con los lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Resolución 460 de 2022, por la cual se expide el Plan nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital y se dictan los lineamientos generales para su implementación.

Decreto 338 de 2022, por el cual se adiciona el Título 21 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la

Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital y se dictan otras disposiciones.

Resolución 746 de 2002, por el cual se fortalece el Modelo Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.

Decreto 767 de 2022, por medio por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Norma Técnica Colombiana NTC- ISO/IEC colombiana 27001:2013. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

Manual Fundamentos de Preservación Digital a Largo Plazo. Instrumento brinda una estructura conceptual de la preservación digital, así como elementos normativos, técnicos y metodológicos, para orientar a las entidades en la formulación de la política de gestión documental y en la definición de acciones y buenas prácticas que les permitan asumir el gran reto de la preservación digital a largo plazo.

Sistema de Gestión de Documentos Electrónicos de Archivo. Este documento pretende proporcionar un enfoque general acerca de la implementación del Sistema de Gestión de Documentos Electrónicos de Archivo. SGDEA

Plan Institucional de Archivos PINAR: El PINAR se desarrolla para asegurar la articulación del PGD con la misión, objetivos y metas estratégicas del AGN.

Guía de documentos y expedientes electrónicos: Orientar a las entidades públicas y privadas que cumplen funciones públicas, en la producción, gestión y tratamiento de los expedientes y documentos electrónicos, desde su creación hasta la preservación a largo plazo con el fin de garantizar su autenticidad, integridad, fiabilidad y disponibilidad durante su ciclo vital.

Requisitos mínimos de digitalización: Este documento busca establecer los requisitos mínimos para llevar a cabo un proyecto de digitalización, proponiéndolos como una lista de verificación fácil de seguir e implementar.

Instructivo de limpieza y desinfección de áreas y de documentos de archivo. Este instructivo aplica para los procedimientos que tienen que ver directamente con la conservación preventiva de los acervos documentales y se enmarca dentro del Sistema Integrado de Conservación.

5. GLOSARIO

Activo: cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Activo de Información: recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).

Amenaza: causa potencial de un incidente no deseado que pueda provocar daños a un sistema o a la organización.

Amenaza informática: situación potencial o actual que tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado.

Antivirus: programas cuyo objetivo es detectar y eliminar software malicioso.

Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.

Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas), direcciones, información de contacto, números identificativos, apodos o cargo por otros datos para evitar la identificación de personas y preservar la confidencialidad de la información.

Archivos PST: son archivos electrónicos creados desde el software de mensajería Outlook con el fin de almacenar de forma local (computadores), copia de elementos de un buzón de correo electrónico.

Autenticación: mecanismo técnico que permite garantizar que una persona o entidad es la correcta.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

Back up: se refiere a una copia de respaldo de información.

Buzón: espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros.

Canal de comunicación: medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.

Centro de cómputo: espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización llamado también data center por su término anglosajón.

Ciberseguridad: capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética.

Confidencialidad: propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control informático: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.

Correo electrónico: servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.

Claves, contraseña o password: forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.

Criterios para adquisición de tecnología: condiciones o requisitos mínimos para tener en cuenta al momento de implementar y/o adquirir tecnología, como:

Compatibilidad: el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad.

Calidad: se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo en el mercado.

Acuerdos de servicio: se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes.

Mantenimiento, actualizaciones y soporte: se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice.

Transacciones: se deben identificar cuales transacciones realiza el sistema, de qué manera las realiza y donde se almacenan.

Reportes o salidas: se deben identificar las salidas de información de los sistemas, reportes, consultas en pantalla o impresiones.

Custodio de activo de información: individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

Datos personales sensibles: aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado: dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, comprende la identificación, evaluación y el tratamiento de riesgos.

Grupos de Valor: para Función Pública corresponden a las entidades del estado, servidores públicos y ciudadanos.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

Infraestructura tecnológica: elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.

Impacto: el coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., perdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: 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.

Integridad: la propiedad de salvaguardar la exactitud y completitud de la información.

Internet: corresponde a una interconexión de diferentes redes de computadoras, permitiendo la creación de una red única de alcance mundial.

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

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

Parte interesada (Stakeholder): persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012).

Responsable de activo de información: Identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

Responsable del tratamiento: Persona natural o jurídica, pública o privada que por sí misma o en asocio con otros decida sobre la base de datos y/o el tratamiento de los datos.

Segregación de tareas: Reparto de tareas sensibles entre distintos servidores públicos para reducir el riesgo de un mal uso de los sistemas informáticos e información de manera deliberada o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Titular de la información: Persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de habas data y demás derechos y garantías a que se refiere la presente ley.

Teletrabajo: Actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo.

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: Debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza, Emaaf E.S.P., entendiendo la importancia de una adecuada gestión de la información, implementa un Modelo Privacidad y Seguridad de la Información (MPSI), estableciendo un sello de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, enmarcado en el estricto cumplimiento de las leyes y en concordancia con su misión, visión, política de gestión y la plataforma estratégica digital, permitiendo la confiabilidad, disponibilidad e integridad de la información.

6.1. Directrices de Gestión de la Seguridad de la Información

Esta política está determinada por las siguientes premisas:

- Minimizar el riesgo de vulnerabilidades de la información en los procesos.
- Establecer los principios de seguridad de la información.
- Lograr la confianza de las partes interesadas.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios de la Emaaf E.S.P., y los terceros vinculados a ella en desarrollo de sus funciones y/o actividades.
- Velar por la continuidad de los procesos frente a incidentes de seguridad de la información.

6.2. Revisión de las políticas de seguridad de la información.

Las políticas de seguridad de la información se revisarán de forma anual y cuando se produzcan cambios tecnológicos o eventos que lleven al Comité Institucional de Gestión y Desempeño -CIGD- a concluir que el manual de políticas debe ser actualizado. La aprobación de las actualizaciones y/o modificaciones, serán realizadas por el -CIGD-.

6.3. Principios de seguridad que soportan el MPSI de la Emaaf E.S.P.,

La Emaaf E.S.P., revisará que se articulen y cumplan las siguientes directrices:

1. Proteger los activos de la información.
2. Continuar sus actividades misionales en medio de un evento catastrófico.
3. Cumplir las obligaciones legales, regulatorias y contractuales.
4. Proteger las instalaciones de almacenamiento de datos y la infraestructura tecnológica.
5. Controlar el acceso a la información, sistemas y recursos de red.

La seguridad será parte integral del ciclo de vida de los sistemas de información y se mejorará continuamente el modelo de seguridad y privacidad de la información.

6.4. Compromiso de la Alta Dirección

De acuerdo a los lineamientos y directrices entregadas por el Ministerio de Tecnologías de la Información y Comunicaciones -MinTIC- a través de la Política de Gobierno Digital y el Modelo Integrado de Planeación y Gestión -MIPG-, la Emaaf ESP:

El representante legal de la Empresa de Acueducto y Alcantarillado y Aseo de Funza Emaaf E.S.P., es el responsable institucional de la Política de Gobierno Digital, componentes y habilitadores entre los cuales se encuentra seguridad y privacidad de la información.

Comité Institucional de Gestión y Desempeño -CIGD- de la Emaaf E.S.P., se compromete a dar cumplimiento a la Política de Seguridad de la información y orientar la implementación de la política, de normas y demás procesos que mejoren continuamente la seguridad de la información. El -CIGD-, contribuye y demuestra su compromiso a través de:

- La revisión y aprobación de las políticas contenidas en este manual.
- La promoción activa de una cultura de seguridad.
- El apoyo en la divulgación de este manual a todos los funcionarios de la Empresa.
- La gestión de los recursos para implementar, mantener y mejorar las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Política de seguridad de la información	A.5.1.1 y A.5.1.2	Establecer, aprobar, comunicar y mantener actualizadas las políticas de seguridad de la información, de forma que reflejen la dirección y apoyo de la alta dirección, se alineen con los objetivos estratégicos del negocio, los requisitos legales y contractuales, y se adapten a los cambios organizacionales, tecnológicos y de riesgos..
Compromiso de la Alta Dirección	A.6.1	Lineamiento: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.

Tabla 1 - Seguridad de la información.

7. POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Empresa Municipal de Acueducto, Alcantarillado y Aseo de Funza -Emaaf ESP- como sujeto obligado define las responsabilidades para ejecutar las actividades específicas de seguridad de la información, designando la administración del Modelo de Seguridad y Privacidad de la Información -MSPI- a cargo de la Subgerencia Administrativa.

De esta forma la Emaaf E.S.P., asegura que las fases y actividades establecidas dentro de la etapa de planeación del MPSI, tenga un responsable claro y los miembros del equipo responsable de la ejecución, entiendan sus roles y responsabilidades enmarcados dentro de la Política de Gobierno Digital, sus componentes, los habilitadores y por ende la Seguridad de la Información.

En concordancia al Decreto 767 de 16 de mayo de 2022 de MinTIC, que establece la Política de Gobierno Digital y la Resolución Administrativa 052 de 2025 de la Emaaf ESP, la política de seguridad de la información es de aplicación obligatoria para todos los servidores públicos, contratistas, proveedores y cuando sea aplicable los grupos de valor, deben utilizar los activos de información institucionales para el desarrollo de las actividades misionales preservando la confidencialidad de la información.

Rol	Responsabilidad
Gerente de la EMAAF ESP	• Aprobar los actos administrativos referentes a las Políticas de Seguridad de la Información. • Evaluar el proceso de gestión de seguridad de la Información. • Aprobar las políticas y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucionales, generados como resultado de los reportes o propuestas del Comité Institucional de Gestión y Desempeño. • Aprobar el presupuesto de los recursos solicitados para el Modelo de Seguridad y privacidad de la Información.
Comité Institucional de Gestión y Desempeño -CIGD-	• Revisar la Política de Seguridad de la Información para la aprobación del gerente. • Supervisar la implementación de procedimientos y estándares que se desprenden de las políticas de seguridad de la información. • Proponer políticas y soluciones específicas para la implantación de los controles de las políticas de seguridad establecidas y la debida solución de las situaciones de riesgo detectadas. • Realizar seguimiento a la implementación de las políticas de seguridad de la información, los riesgos asociados y proponer soluciones.

	• Solicitar al Oficial de la Seguridad informe sobre las oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.
Oficial de Seguridad de la Información o quien haga sus veces.	• Presentar ante el CIGD el plan de trabajo establecido para la implementación del modelo de privacidad y seguridad de la información. • Desarrollar las políticas de seguridad al interior de la entidad, el control de su implementación y velar por su correcta aplicación. • Gestionar la coordinación con otras áreas de la entidad para apoyar los objetivos de seguridad. • Apoyar a los diferentes procesos institucionales en la adopción del MPSI. • Gestionar operativamente las soluciones a los incidentes de seguridad de la información que afecten los activos de la información institucionales. • Monitorear el avance de cada una de las etapas de la implementación de la Política de Seguridad de la Información.
Profesional Universitario de Tecnologías de Innovación y las Comunicaciones.	• Cumplir con los procedimientos relacionados a los dominios de control de acceso, adquisición, desarrollo y mantenimiento de los sistemas de información y gestión de los canales de comunicación y operaciones. • Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la entidad. • Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.
Subgerentes, directores y Jefes de Oficinas.	• Clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad en la entidad, documentando y manteniendo actualizada la clasificación. • Definir los usuarios qué deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia. • Transmitir las orientaciones establecidas por parte de la alta dirección y su equipo de trabajo en materia de seguridad de la información. • Ejercer liderazgo compromiso en la aplicación de la política de Seguridad de la Información.
Dirección de talento Humano.	• Dar cumplimiento a los procedimientos relacionados con la Seguridad de la Información del talento humano.

	• Informar a todo el talento humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y prácticas que de ella surjan. • Incorporar al Plan Institucional de Capacitación las actividades de sensibilización en seguridad de la información que requiera el Oficial de la Seguridad.
Oficina de control interno.	• Realizar auditorías periódicas, o cuando lo considere pertinente a los sistemas y actividades relacionadas a la política de seguridad de la información y al MPSI. • Entregar recomendaciones frente a las debilidades encontradas en las auditorías al oficial de la seguridad de la información. • Presentar ante el comité de Gestión y Desempeño informe de auditorías realizadas.
Profesionales, técnicos, asistenciales, practicantes, auxíliales y demás grupos de interés.	• Conocer, transmitir y cumplir la Política de Seguridad de la Información y todas las normas y procedimientos establecidos por la entidad en esta materia. • Dar uso correcto a los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones o actividades, la relación de estos debe estar registrada en el Sistema de Inventarios de la entidad. • Entregar en buen estado de los equipos de cómputo y periféricos que le sean asignados, cuando se presente retiro de la entidad, cambio de funciones o culminación del contrato según sea el caso. • Salvaguardar la información alojada en el equipo de cómputo y periféricos asignados. • Cumplir las políticas de respaldo, custodia y recuperación de la información definidas por la Oficina de Tecnologías de la Información y las Comunicaciones. • Permitir cuando la Emaaf E.S.P., lo requiera, la revisión del equipo de cómputo a nivel físico, software instalado e información guardada.
Terceros vinculados y visitantes.	• Cumplir las políticas de seguridad de la información institucionales cuando sea autorizado acceso a los activos de información institucionales. • Utilizar exclusivamente la red local de invitados, la cual restringe el acceso solo a internet. • Cumplir las disposiciones necesarias para custodiar, procesar, compartir, utilizar, recolectar e intercambiar información.

Tabla 2 - Organización de la seguridad de la información.

Teniendo en cuenta que el nuevo enfoque de Gobierno Digital es el uso de la tecnología como una herramienta que habilita la gestión de la EMAAF E.S.P., para la generación de valor público, todas las áreas o dependencias son corresponsables en su implementación. Por lo tanto, la seguridad de la información se incluirá en la gestión de cualquier tipo de proyecto de la EMAAF E.S.P.

7.1. Política uso de dispositivos móviles

La Emaaf E.S.P., proveerá las condiciones para el manejo de los dispositivos móviles institucionales y personales (portátiles, teléfonos inteligentes y tabletas, entre otros) que hagan uso de servicios de la EMAAF E.S.P., así mismo, velará porque los funcionarios utilicen responsablemente los servicios y equipos proporcionados por la entidad y los de uso propio.

El uso de los dispositivos móviles institucionales fuera de las instalaciones de la EMAAF E.S.P., se permitirá a usuarios autorizados por las Subgerencias Administrativa, Financiera, Técnica Operativa, Comercial, Oficinas Asesoras y directivos, quienes mediante correo electrónico enviarán (nombres y apellidos, nro documento de identidad del funcionario, tipo, marca y referencia del dispositivo) y entregarán los dispositivos al técnico del área TI quién revisará y hará lo necesario para que estén protegidos mediante el uso de los siguientes controles tecnológicos:

- Antivirus actualizado.
- Cifrado de datos.
- Ejecución de Backups.
- Restricción en la ejecución de aplicaciones.
- Restricción de conexión de dispositivos USB.

Para la implementación de este lineamiento, la EMAAF E.S.P., controlará el registro, la cancelación o anulación y gestión de los dispositivos móviles, por medio de una interfaz de software administrada por el Profesional Universitario de TI, que controle y gestione el acceso a las redes públicas o privadas de manera automatizada, dónde el usuario deberá diligenciar los datos básicos de forma segura y garantizando su protección.

La plataforma de administración permitirá generar informes con los datos de los usuarios autenticados, fechas de ingresos y demás datos contenidos de autenticación del usuario y del diseño del software.

7.2. Política de trabajo en casa

La Emaaf E.S.P., gestionará la seguridad de la información cuando se haga uso de los recursos tecnológicos y activos de información, para el desarrollo de modalidades de trabajo a distancia:

- Ley 2088 de 2021
- Modalidad de trabajo ocasional
- Se mantiene la relación en entre el trabajador y empleador
- Se mantiene la jornada de trabajo y el horario.
- El empleador debe establecer instrumentos, frecuencia y modelo de evolución de resultados

Nota: Antes de realizar cualquier actividad de Trabajo en casa, los Subgerentes, Directores o Jefes de Oficina deberá comunicar a través de correo electrónico dirigido a GESTIÓN TI, el alcance de las actividades a desarrollar, estableciendo el horario y los activos de información a acceder. De acuerdo a las políticas establecida por la Entidad.

GESTIÓN TI realizará:

- Aplicación de los controles para la seguridad de las comunicaciones.
- La entrega del acceso al escritorio virtual que impide el procesamiento y el almacenamiento de información sobre el equipo de propiedad privada.
- Las reglas y directrices del acceso de la familia al computador y visitas al equipo y la información.
- El suministro de soporte y mantenimiento de hardware y software sobre el equipo entregado.
- Suministrará a los usuarios los accesos y claves dinámicas por el tiempo definido por los Subgerentes y Jefes de Oficina.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2022

Política / lineamiento	Control norma	Descripción
Controles organizacionales.	A.5	
Políticas para la seguridad de la información	A.5.1	existencia de políticas aprobadas por la dirección y comunicadas.
Roles y responsabilidades	A.5.2	**Control**: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Tabla 3 - Organización de la seguridad de la información.

8. POLÍTICA DE SEGURIDAD DEL PERSONAL

Los controles de seguridad de información pretenden asegurar que los servidores públicos contratistas y pasantes comprendan sus responsabilidades y sean idóneos en los roles asignados respecto a la seguridad de la información, por lo tanto, la EMAAF E.S.P., define:

8.1. Lineamientos de vinculación y desvinculación de servidores públicos

Se gestiona la seguridad de los recursos humanos a través del proceso de Gestión del Talento Humano.

Los procesos de selección de los servidores públicos vinculados a la entidad cumplen con los requisitos de Gestión del Talento Humano, el cual incluye la verificación de antecedentes disciplinarios, fiscales y de policía, además de la verificación de experiencias académicas y laborales.

La selección y vinculación de servidores públicos sigue el procedimiento de Selección y Vinculación de Personal.

Durante la permanencia como servidores públicos de la entidad, éstos deben participar en las actividades definidas por el proceso Gestión del Talento Humano y lideradas por Gestión de las TI en relación a la formación, capacitación y sensibilización en materia de seguridad de la información.

Al momento de la finalización de su relación laboral el servidor público debe cumplir con el protocolo de retiro del personal del proceso de gestión de talento humano.

En cumplimiento de los requisitos del Código General Disciplinario (Ley 1952 de 2019) los servidores públicos aceptan la obligación legal de mantener la reserva de la información bajo su responsabilidad.

Todo el personal vinculado a la EMAAF E.S.P., deberá ser informado del cumplimiento de las políticas de seguridad de la información, las políticas de operación institucionales y los procedimientos del Modelo Integrado de Planeación y Gestión -MIPG-.

En el evento de la terminación y/o cambio de cargo al interior de la EMAAF E.S.P., el funcionario devolverá todos los activos de información y elementos asignados durante su relación contractual.

La vigencia de los derechos de acceso y su revocatoria, deberá estar estrechamente relacionados con la terminación de la relación laboral y/o cambio del rol del empleado en la EMAAF E.S.P.

Los derechos de acceso a todos los sistemas de información que tenga el funcionario, serán inactivados temporalmente por los períodos de licencia mayor a 5 días y/o vacaciones y volverán a ser activados al término de estas y regreso del empleado. Para lo cual Gestión del Talento Humano mediante correo electrónico dirigido al profesional universitario de las TI solicitará la inactivación de sistemas de información, correo electrónico y demás plataformas que deban ser bloqueadas.

Lineamientos de vinculación y desvinculación de pasantes: Los pasantes se vinculan a la EMAAF E.S.P., mediante documento de vinculación formativa, donde el supervisor delegado es el encargado de asignar tareas y realizar seguimiento al cumplimiento de las actividades asignadas.

Gestión del Talento Humano es el encargado de solicitar por medio del correo electrónico la creación, actualización y eliminación de cuentas de usuario y asignación de equipos de cómputo para el cumplimiento de las actividades que le sean asignadas.

Los pasantes universitarios deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información, las políticas de operación institucionales y los procedimientos del Modelo Integrado de Planeación y Gestión.

8.2. Lineamientos para contratistas respecto a la seguridad de la información

Para los contratos de prestación de servicios, cada supervisor es el responsable de realizar la solicitud de cuentas de usuario a las plataformas o herramientas que requiera el contratista mediante correo electrónico dirigido al profesional universitario de las TI, para lo cual debe proporcionar los datos del contratista, del contrato y los servicios tecnológicos autorizados.

Si el contrato establece que la EMAAF E.S.P., debe proporcionar el equipo de cómputo, el supervisor del contrato debe realizar la solicitud por medio de la mesa de ayuda para que Gestión de las TI verifique su disponibilidad y proceda a su entrega. El equipo de cómputo proporcionado al contratista debe quedar a cargo del supervisor.

Para los contratos con personas jurídicas, en el caso de requerirse, el supervisor debe realizar la solicitud de la cuenta de usuario proporcionando los datos del contrato y de las personas que tendrán a cargo dichas cuentas de usuario.

Al momento de terminar el plazo de ejecución del contrato, el supervisor del mismo debe solicitar la eliminación de la cuenta(s) de usuario asociada(s) al contrato, mediante correo electrónico dirigido al dirigido al profesional universitario de las TI. Si se asignó equipo de cómputo al contratista, el supervisor verificará el funcionamiento del equipo.

Los contratistas deben aceptar dentro de sus obligaciones la cláusula de confidencialidad sobre la información a la que tengan acceso y aceptar el cumplimiento de las políticas de seguridad de la información, las políticas de operación de la EMAAF E.S.P., y los procedimientos del Modelo Integrado de Planeación y Gestión.

8.3. Lineamientos de control para servidores públicos, contratistas, pasantes y visitantes

Los servidores públicos, contratistas, pasantes deben portar el carné que los identifica como tales en un lugar visible, mientras se encuentren en las instalaciones de la EMAAF E.S.P., para el caso de visitantes deben portar el registro de ingreso y/o sticker en un lugar visible durante su estadía en la empresa.

Si el servidor público, contratista o pasante porta un carné institucional que no le corresponde, será considerado como suplantación de identidad y deberá notificarse a Gestión del Talento Humano.

Los servidores públicos de la entidad deben registrar el ingreso y la salida de la jornada laboral en el dispositivo biométrico ubicado junto a la recepción en las instalaciones de EMAAF E.S.P., o donde sea informado su ubicación.

La EMAAF E.S.P., actuará como responsable del tratamiento de sus datos personales y hará uso de los mismos únicamente para las finalidades, según lo establecido en la política de tratamiento de datos personales aprobada por la entidad y publicado en la página web www.emaafesp.gov.co.

8.4. Lineamientos sobre el proceso de carnetización y registro

Se establece los lineamientos de uso, expedición, control y registro del carné utilizados en EMAAF E.S.P., estos controles aplican a todas las personas que hacen uso de un carné expedido por EMAAF E.S.P., en sus diferentes instalaciones y proyectos, así como los responsables de la solicitud y entrega de carnés.

|

Beneficios del carné

El carné, acredita a la persona como empleado activo de EMAAF E.S.P., le permite el ingreso laboral a los diferentes proyectos e instalaciones de la entidad, el titular del carné debe tener los siguientes cuidados físicos con el fin de conservar la integridad de este documento.

- Portar, usar y cuidar.
- Evitar escribir sobre el respaldo, cortarlo, plastificarlo, doblarlo, perforarlo o aplicarle algún tipo de fuerza.

- Evitar colocarlo cerca de objetos que generen calor, elementos corrosivos y/o solventes.
- Evitar guardarlo en los bolsillos del pantalón sin la debida protección.
- Evitar guardarlo con objetos metálicos como monedas o llaves.
- Mantenerlo seco, la humedad y los líquidos que afectan su vida útil.
- Limpiar la superficie con paños suaves, sin utilizar líquidos corrosivos.
- El carné debe conservarse en el correspondiente brazalete y/o porta carné proporcionados por la entidad según aplique.
- Portarlo todo el tiempo en el brazalete y/o porta carné, para facilitar su lectura deberá ubicarlo a una distancia máxima de diez (10) centímetros.

Uso del carné

Todos los empleados de EMAAF E.S.P., deberán portar el carné todo el tiempo durante la jornada laboral en el brazalete y/o porta carné entregado por la compañía para tal fin y será requerido para el inicio / finalización de actividades diarias.

El carné es personal e intransferible y todas las acciones realizadas con el carné se entienden como efectuadas por su titular.

Cualquier novedad sobre el carné (perdida, hurto, daño, etc.), genera un costo y debe reportarse a la dirección electrónica info@emaafesp.gov.co el mismo día, para su trámite respectivo.

El personal de la Dirección de Talento Humano de EMAAF E.S.P., está autorizado para verificar que quién porte el carné sea su titular, en caso que los datos no coincidan, este personal podrá retener el carné y deberá reportar a la Subgerencia Administrativa para las correspondientes acciones administrativas.

El titular del carné es responsable de reportar cualquier situación que amerite la reposición del carné, la cual tiene costo adicional y será asumido por el trabajador, anexando la denuncia de pérdida del carné.

Al finalizar su vínculo laboral, el titular debe retornar el carné a la EMAAF E.S.P., como parte de su proceso de retiro y obtención del Paz y Salvo o anexar la denuncia de pérdida del carné.

Sobre la expedición de carné

Talento Humano es la única dependencia autorizada para la emisión del carné corporativo, la EMAAF E.S.P., expide un carné a la persona cuando:

- Su vínculo laboral con la entidad ya está formalizado (Primera vez o reingreso).

- Los datos impresos en el carné no corresponden a los datos del documento de identidad vigente del titular.
- Deterioro natural por el uso legítimo.
- En el momento de la entrega del carné, el futuro titular debe identificarse con el documento de identidad vigente, leer y dejar constancia de la aceptación de la presente política de carnetización y registro (firmar planilla de entrega).

Entrega de carné

En el momento de la entrega del carné, el futuro titular debe identificarse con el documento de identidad vigente, leer y dejar constancia a través de registro firmando planilla de entrega.

Validez

El carné del personal de la Emaaf E.S.P., tendrá una validez igual a la vigencia del contrato laboral con la empresa.

Emisión y administración

La dirección de Talento Humano es responsable de la administración de los carnés y la Subgerencia Administrativa es responsable de su emisión.

Destrucción

Una vez desvinculado el trabajador (terminación del contrato), Gestión del Talento Humano, con autorización de la Subgerencia Administrativa realizará el acta del carné que serán destruidos, en la cual reposará imagen antes de su eliminación total.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad de los recursos humanos	A.7	
Antes de asumir el empleo	A.7.1	**Lineamiento**: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
Selección	A.7.1.1	**Control**: Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a

		que se va a tener acceso, y a los riesgos percibidos.
Términos y condiciones del empleo	A.7.1.2	**Control**: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
Durante la ejecución del empleo	A.7.2	**Control**: Lineamiento: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
Responsabilidades de la dirección	A.7.2.1	**Control**: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
Toma de conciencia, educación y formación en la seguridad de la información	A.7.2.2	**Control**: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
Terminación o cambio de responsabilidades de empleo	A.7.3.1	**Control:** Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deben definir, comunicar al empleado o contratista y se deberían hacer cumplir.
Proceso de desvinculación	A.7.4	**Control:** Procedimientos claros al finalizar la relación laboral o contractual, incluyendo retiro de accesos, devolución de activos y recordatorio de obligaciones de confidencialidad

Tabla 4 - Seguridad de los recursos humanos.

9. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

9.1. Responsabilidad por los activos

La información contenida en archivos físicos, sistemas de información y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, y teléfonos, entre otros) son propiedad de la EMAAF E.S.P., y se proporcionan a los funcionarios y terceros vinculados a la empresa, para cumplir con los propósitos misionales.

La EMAAF E.S.P., como propietario de la información delega en el Gerente, Subgerentes, Directores, Jefes de Oficina, los Líderes de Procesos, todos los funcionarios y terceros vinculados, el cumplimiento de las políticas del uso adecuado de los activos de la información en su ciclo de vida, las cuales se encuentran incluidas en este manual.

Los recursos tecnológicos de la EMAAF E.S.P., deberán ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la empresa.

9.2. Inventario de activos

Todos los activos de información de la EMAAF E.S.P., deberán ser identificados, inventariados y clasificados según su contenido; se definirán los responsables de su protección y serán implementados los controles adecuados.

9.3. Clasificación y manejo de la información

Los Líderes de cada proceso serán los responsables de los activos de información asignados a su área y anualmente deberán actualizar el inventario de estos activos. Como parte de esta actividad verificarán que estén clasificados de acuerdo Guía de Clasificación de Activos de Información y Análisis de Riesgos o su documento equivalente de acuerdo a las disposiciones del Ministerio de las Tecnologías de la Información y Comunicaciones -MinTIC-.

La información clasificada tendrá un conjunto de controles que se utilizarán para proveer un nivel de protección apropiado, sin importar el medio, formato o lugar donde se encuentre. Estos controles se aplicarán y mantendrán durante el ciclo de vida de la Información, desde su creación, durante su uso y hasta su apropiada disposición o destrucción.

Estos controles podrán ser complementados y robustecidos a solicitud del responsable de la Información, del Oficial de Seguridad de la Información o quien haga sus veces o del Comité Institucional de Gestión y Desempeño con apoyo de Gestión Informática.

9.4. Etiquetado y manipulado de la información

Los activos de información serán etiquetados de acuerdo con el esquema de clasificación de la información aprobada por la EMAAF E.S.P., lo anterior teniendo en cuenta las Tablas de Retención Documental.

9.5. Almacenamiento de Información

La información pública clasificada y/o pública reservada almacenada en cualquier medio electrónico, deberá ser cifrada. Los equipos de cómputo y/o portátiles que almacenen esta información deberán estar protegidos con mecanismos de control de acceso para evitar que personas no autorizadas puedan consultarla, manipularla o eliminarla.

9.6. Uso de medios de almacenamiento removibles

Trazar las responsabilidades y controles de la organización sobre el uso de medios removibles, incluyendo USB flash drives, discos duros externos, dispositivos móviles usados como almacenamiento externo, medio ópticos (CD, DVD, etc.) y cualquier otro dispositivo computacional que no esté físicamente fijo dentro de un equipo de cómputo. Está direccionada a minimizar el riesgo de pérdida o exposición de información sensible y reducir el riesgo de ser infectado con malware en los sistemas de información de la EMAAF E.S.P.

La política administra la interacción entre todos los activos y recursos, tanto para tecnología de la información como para tecnología de operaciones, incluye sistemas operativos, software de aplicaciones, hardware de cómputo, redes y servicios en nube, para todo equipo manejado por la empresa (de propiedad, bajo arrendamiento o personal) o donde residan datos de la EMAAF ESP. Para esto se deben bloquear todos los puertos USB de los equipos de cómputo mediante el software antimalware que la entidad posea, de tal forma que el uso de USB flash drives y discos duros externos sea controlada por el profesional universitario de sistemas.

El líder del proceso que, considerando las labores realizadas por los funcionarios y/ terceros vinculados, requiere USB flash drives, discos duros externos, dispositivos móviles usados como almacenamiento externo, medio ópticos (CD, DVD, etc.), para lo cual líder del proceso mediante correo electrónico dirigido al profesional universitario de sistemas, solicitará detalladamente la necesidad así:

- Asunto: Autorización medio de almacenamiento removible.
- Descripción: Razón por la cual solicita el uso, nombres y apellidos de la persona autorizada, tipo de medio autorizado, tiempo (cuando se trate de USB flash drives y discos duros externos los tiempos en consola son 15 o 30 minutos, 1 o 2 horas).

El profesional universitario de sistemas habilitará y dará respuesta al correo electrónico recibido.

El líder del proceso será el responsable del buen uso de estos dispositivos, siendo de su resorte evitar la divulgación, modificación, eliminación o destrucción no autorizada, de la información almacenada en los dispositivos de almacenamiento removibles a su cargo o aquellos autorizados.

9.7. Manejo de los soportes de almacenamiento

Gestión de soportes extraíbles: Los dispositivos electrónicos que tengan autorizado el manejo de USB y unidades reproductoras de CD/DVD, deberán cumplir los siguientes requisitos:

- Tener habilitado el escaneo automático de contra malware.
- Tener configurada en la herramienta antimalware, el bloqueo de la reproducción automática de archivos ejecutables.

Eliminación de soportes: La información será eliminada de forma segura cuando ya no sea necesaria, utilizando procedimientos formales de borrado seguro o destrucción del dispositivo.

Soportes físicos en tránsito: La información contenida en los medios de almacenamiento que deban salir de la EMAAF ESP, previamente deberá ser cifrada. Con el fin de evitar el deterioro físico de los dispositivos se deberá hacer uso de protectores como bolsas de seguridad.

9.8. Uso de tokens de seguridad

Los tokens de seguridad deberán ser entregados formalmente a los funcionarios que, por su trabajo necesiten usarlos para desarrollar sus actividades. Ellos deberán firmar acuerdos de buen uso y protección de estos dispositivos. La EMAAF E.S.P., proveerá las condiciones adecuadas para su protección y velará porque los funcionarios responsables de estos dispositivos hagan un uso responsable de éstos.

9.9. Borrado seguro

La EMAAF E.S.P., velará porque se realice borrado seguro en los dispositivos de almacenamiento de su propiedad y que contengan información. El responsable de la información debe revisar que se hayan realizado las copias de seguridad, las pruebas y el borrado seguro de la información.

Para el borrado seguro, el líder del proceso mediante correo electrónico y registro de incidente en la mesa de servicios, con el diligenciamiento del formato respectivo

(*F.GTICS "SOLICITUD DE BORRADO SEGURO DE LA INFORMACIÓN"*) dirigido al profesional universitario de sistemas solicitará la destrucción de la información.

Cuando se haya dado la autorización por el responsable de la información, se dará un borrado a la información dependiendo del medio en que reposa; para cumplir con este requerimiento se pueden utilizar cualquiera de los siguientes métodos según sea conveniente.

- Desmagnetización: consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo. Este método es válido para la destrucción de datos de los dispositivos magnéticos.

- Destrucción Física: El objetivo de la destrucción física es la inutilización del soporte que almacena la información en el dispositivo para evitar la recuperación posterior de los datos que almacena.

- Dentro de este control, es válida la perforación con brocas para metal instaladas en un taladro, que calará las USB flash drives, discos duros externos, dispositivos móviles usados como almacenamiento externo y medios ópticos (CD, DVD) etc. Siempre el talento humano seguirá las normas señaladas, utilizará los elementos de protección personal -EPP- y las buenas prácticas del Sistema de Gestión de Salud y Seguridad en el Trabajo -SGST-.

Para la destrucción de la información se debe tener en cuenta restricción jurídica, y las tablas de retención documental.

9.10. Copias de respaldo

La Emaaf E.S.P. reconoce la información contenida en sus sistemas informáticos críticos en producción, así como en los equipos de cómputo corporativos, como un activo fundamental para la operación institucional. Con el fin de protegerla frente a pérdidas, daños o accesos no autorizados, esta información deberá ser respaldada diariamente en la nube institucional.

Cada responsable de proceso tendrá la obligación de identificar, clasificar y mantener actualizados los activos de información correspondientes a sus procedimientos.

El profesional universitario de sistemas será responsable de definir y administrar los tipos de copias de respaldo requeridos para cada sistema de información, de acuerdo con su criticidad y nivel de riesgo.

La información generada y gestionada en los computadores personales o estaciones de trabajo de la entidad deberá ser almacenada en la nube corporativa adquirida por

la Emaaf E.S.P. Cada colaborador será responsable de mantener actualizados sus datos en las unidades de almacenamiento asignadas según su rol, evitando que la información repose únicamente en los equipos locales.

9.11. Política mantenimiento de la infraestructura tecnológica

Se propenderá por una adecuada gestión de la infraestructura tecnológica, encaminada a administrar de manera eficiente y eficaz el hardware y software con que cuenta la EMAAF E.S.P.

Se deberán realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la EMAAF E.S.P., esto incluye instalación de parches de seguridad recomendados por los fabricantes de software. El área de gestión de la información TICS deberá establecer el cronograma anual conforme a lo establecido en el Plan de Mantenimientos a Sistemas Tecnológicos.

Se deberá realizar mantenimiento preventivo y correctivo de las estaciones de trabajo y equipos portátiles, esto incluye instalación de parches de seguridad recomendados por los fabricantes de software (compilaciones al sistema operativo, versiones a sistemas de información, plataforma antimalware y demás programas implementados). Así como su adecuación para la reutilización o reasignación de manera segura en el cual se conserve la disponibilidad, integridad y confidencialidad de la información contenida en los mismos.

9.12. Impresión de información confidencial

Cuando se imprime información pública clasificada y/o pública reservada deberá ser recogida inmediatamente, evitando que personal no autorizado tenga acceso a ésta. Para tal fin la EMMAF E.S.P., seleccionará un método de impresión confidencial, consistente en la inserción de un código o contraseña cada vez que se envíe imprimir un documento; los folios del archivo enviado no salen a la bandeja hasta que físicamente la respectiva persona se acerque a la impresora y digite el código personal.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Gestión de activos	A.8	
Responsabilidad por los activos	A.8.2	**Lineamiento**: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.

Gestión de medios removibles	A.8.3.1	**Control**: Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
Disposición de los medios	A.8.3.2	**Control**: Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
Transferencia de medios físicos	A.8.3.3	**Control**: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.

Tabla 5 - Gestión de activos

10. POLÍTICA CONTROL DE ACCESO PARA SEGURIDAD DE LAS REDES

En el marco del Modelo de Seguridad y Privacidad de la Información, se facilitarán entornos digitales con el fin de garantizar que la información, las áreas de su procesamiento, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la EMAAF E.S.P., se encuentren con la protección contra accesos o intrusiones no autorizadas y que disminuyan los riesgos de seguridad de la información.

La aplicación de esta política da alcance a cualquier medio en el cual se encuentra la información (digital o físico), sitios de procesamiento de información, redes de datos, recursos de la plataforma tecnológica y sistemas de información. Además, abarca a todos los directivos, trabajadores oficiales, contratistas y terceros vinculados, con acceso a las instalaciones de la entidad y sistemas de información.

10.1. Acceso a redes y recursos de red

La plataforma tecnológica es responsabilidad de la Subgerencia Administrativa y del área de gestión TI, así como los sistemas de información de la entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso lógico y físicos monitoreados y con capacidad de generar alertas.

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de la EMAAF E.S.P.
- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.
- Únicamente el propietario responsable de la información, podrá autorizar la creación de un usuario, el cual será asociado sólo a un individuo y la solicitud deberá obedecer a una razón legítima de la EMAAF E.S.P.
- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.
- Se deberá deshabilitar o borrar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con la EMAAF E.S.P.
- Se deberán realizar revisiones periódicas en los diferentes sistemas de la EMAAF E.S.P., para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.
- Cada miembro del personal de la de la EMAAF E.S.P., deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.
- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

10.2. Normas de seguridad para el control de acceso lógico

Los Subgerentes y Jefes de Oficina líderes de proceso deberán ser los únicos autorizados para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario, a través de correo electrónico así:

- Asunto: Autorización acceso a la red.
- Descripción: Razón por la cual solicita la autorización, nombres y apellidos de la persona autorizada y tipo de recursos autorizados (unidades de red, módulos del sistema de información).

Para estos requerimientos los deben hacer mediante la mesa de servicios y diligenciando el formato "*F.GTICS 1.1.1-01 ASIGNACION DE USUARIO Y TERMINOS DE USO" en la Ruta de Calidad ("Ruta de calidad\1. estratégico\3. gestión de la información y comunicaciones\3. gobierno digital*") para su respectivo proceso de creación.
La administración de los perfiles de usuario es responsabilidad de Gestión TI administradores del sistema de información y de las áreas responsables de dicho activo.

El profesional universitario de TI deberá utilizar el Servicio de Directorio Activo (AD) para la administración de los objetos de la red que usa el almacén de datos estructurados como base para una organización jerárquica lógica de la información del directorio activo a través de los protocolos TCP, ICMP y UDP con LDAP.

Los Subgerentes y Jefes de Oficina líder de proceso deberán establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.

Gestión TIC deberá crear, modificar, bloquear, inactivar o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por los Subgerentes y Jefes de Oficina.

Se deberá establecer la entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la EMAAF E.S.P., a los recursos de la plataforma tecnológica o a los sistemas de información. Para este fin el profesional universitario de TI entregará por medio del correo electrónico institucional la respuesta de notificación de envío de credenciales a las personas autorizadas.

Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la EMAAF E.S.P., Para lo cual, el profesional universitario de TI, solicitará a talento humano mediante correo electrónico con periodicidad trimestral, la lista de funcionarios y contratistas activos que desempeñan funciones y actividades

en la empresa, para ser contrastada con las personas que acceden a los sistemas de información, a la red de informática y sus recursos.

Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.

Se deberán establecer mecanismos de auditoría al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad física y del entorno	A.11	
Seguridad física y de las instalaciones	A.11.1	• Se implementan medidas para prevenir accesos no autorizados a edificios, oficinas, salas de servidores y demás áreas críticas. • Incluye barreras físicas, cerraduras, controles de acceso, cámaras de vigilancia y registro de visitas. • Las áreas con equipos críticos deben contar con medidas reforzadas (ej. control biométrico o credenciales restringidas).
Protección de equipos	A.11.2	• Los equipos y activos de información deben estar ubicados y protegidos adecuadamente para evitar daños, robos o accesos indebidos. • Se contemplan protecciones contra riesgos ambientales (fuego, inundaciones, temperatura, polvo). • Reglas para el cableado seguro, separación de ambientes y ubicación en áreas seguras. • Uso de medidas contra accesos físicos no autorizados a dispositivos (ej. bloqueo de racks, gabinetes).

Tabla 6 - Seguridad de las comunicaciones.

11. POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Partiendo que la información es el activo intangible más valorado de la EMAAF E.S.P., con la implementación de la política, se previene al acceso físico no autorizado, la alteración e interferencia de la información y a las instalaciones y/o lugares dónde se procesa la información.

A través de circuito cerrado de cámaras se lleva a cabo la verificación del acceso a entornos físicos mediante, los cuales asegurarán el perímetro, las oficinas, recintos, áreas de carga y descarga, plantas de tratamiento de agua y entornos abiertos para evitar el acceso no autorizado de personas, así mismo, el ingreso de personal administrativo, contratistas y/o visitantes, en horarios fuera de la jornada laboral establecido debe ser notificado vía correo electrónico a la subgerencia Administrativa, la cual procede a dar la autorización del respectivo ingreso.

La seguridad perimetral de las instalaciones físicas lo conforman muros robustos y fuertes, encerramiento metálico y cerraduras sobre el lateral hacia la entrada; el cerramiento restante está construido en ladrillo y tubo cuadrado metálico sobre el cual lleva un alambre de púas para cerca.

Controlará las amenazas físicas externas y velará por proveer las condiciones medioambientales requeridas para el funcionamiento de su infraestructura física, de la plataforma tecnológica y la preservación de sus activos de información.

También exigirá a los proveedores el cumplimiento de mecanismos de seguridad física, los controles de acceso a zonas restringidas y condiciones medioambientales para reducir el riesgo de incidentes de seguridad en su funcionamiento que pudieran afectar de forma indirecta las operaciones de la EMAAF E.S.P.

11.1. Áreas seguras

La EMAAF E.S.P., ha identificado el centro de datos con la información confidencial como el espacio con acceso restringido y controlado por medio de la aplicación de barreras físicas y procedimientos de control. Esta área con acceso restringido es el lugar donde se procesa y almacena la información en digital, pública clasificada o pública reservada. Otra área controlada y definida, es el archivo por ser el lugar donde se almacena la información en físico bajo las normas de gestión archivística.

El acceso a áreas restringidas deberá limitarse a personas autorizadas. El acceso a estas áreas requerirá de esquemas de control de acceso, como acceso biométrico, llaves o candados, entre otros. Se deberán utilizar bitácoras para registrar la entrada y salida del personal a las áreas restringidas.

Las instalaciones y oficinas con acceso restringido deben ser monitoreadas y contar con cámaras de video que almacenan en sistema DVR (Digital Video Recorder).

Las llaves, contraseñas de cajas fuertes y otros mecanismos de seguridad de acceso a sitios restringidos solo serán utilizadas por los funcionarios designados por la subgerentes o jefes de área por la EMAAF E.S.P., y salvo situaciones de emergencia, no podrán ser transferidos.

Todos los funcionarios y terceros vinculados deberán portar el carné que los identifique de forma visible, mientras permanezcan en las instalaciones de la EMAAF E.S.P., y reportar a la mayor brevedad, cualquier sospecha de pérdida o robo de carnet de identificación de la empresa.

Todos los visitantes que ingresen a la EMAAF E.S.P., deberán ser registrados en bitácora de visitantes con su nombre, identificación, EPS, ARL, el nombre del funcionario que visitan, la hora de entrada y la de salida de las instalaciones. Todos los visitantes que ingresan a la EMAAF E.S.P., serán recibidos y estarán acompañados por la persona a quien visitan durante su permanencia en las instalaciones de la empresa. En la salida, deberán ser escoltados por su anfitrión hasta la salida.

11.2. Seguridad para el centro de datos

Punto clave para la seguridad física es la estructura envolvente, que garantiza protección contra cualquier amenaza del exterior como, intrusiones, vandalismos, inundaciones, polvo, incendios, evitando la penetración de sustancias contaminantes y líquidos inflamables. Los techos, puertas y llegadas del cableado deben garantizar resistencia al fuego.

El centro de datos cuenta con un extintor Co2 de incendios para la protección contra conatos y conflagraciones. Este sistema lo acompañará una alerta auditiva como mecanismo de protección para las personas y puesta en funcionamiento de protocolos y del plan de contingencia.

Se cuenta con un sistema de enfriamiento y/o de aire acondicionado que regule la temperatura sea interna, evitando daños en los dispositivos eléctricos y electrónicos ubicados en el centro de datos.

Se realizarán periódicamente mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS y del sistema de aire acondicionado. La UPS se probará según las recomendaciones del fabricante, de tal forma que se garantice su operación y el suficiente tiempo de autonomía para realizar las funciones de respaldo y apagado de equipos. El sistema de enfriamiento y/o de aire acondicionado y los detectores deberán probarse regularmente, de acuerdo a las recomendaciones del fabricante.

Se tendrán extintores debidamente aprovisionados, con carga vigente y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales. Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, serán realizados por personal especialista y debidamente autorizado e identificado.

El cableado lógico, deberá estar protegido de Interferencia eléctrica y/o radiación electromagnética interna y externa. Los cables de potencia deberán estar separados de los cables de datos, siguiendo normas técnicas. Los equipos deberán protegerse de fallas de potencia u otras anomalías de tipo eléctrico.

Se deberán tener interruptores eléctricos adicionales, localizados cerca de las salidas de emergencia, para lograr un rápido apagado de los sistemas en caso de una falla o contingencia.

11.3. Política de escritorio limpio y pantalla limpia

Los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o fuera de las horas laborales.

Los sitios de trabajo del personal de la EMAAF E.S.P., deben localizarse en ubicaciones que no queden expuestas al acceso de personas externas, exceptuando la oficina de atención al ciudadano, para este caso los monitores están ubicarse de forma que no puedan ser visualizados por personas externas.

Escritorios limpios: Siempre que el personal se ausente de su estación de trabajo, deberá guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información pública de uso interno, pública clasificada o pública reservada, además deben bloquear los equipos de cómputo (por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L y no solo apagar el monitor).

Para el personal que esté ubicado en zonas de atención al público, al ausentarse de su estación de trabajo deberá guardar los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada.

Al finalizar la jornada de trabajo, los colaboradores deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, pública clasificada o pública reservada y apagar el computador y el monitor.

La información pública reservada y pública clasificada, cuando se imprima se deberá retirar inmediatamente de las impresoras.

11.4. Responsabilidades

Personal: Es responsabilidad del personal cumplir las directrices de la presente política, respetando las restricciones que se establezcan y haciendo buen uso de los derechos, permisos y privilegios que le hayan sido otorgados, pues cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información de EMAAF E.S.P.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad física y del entorno	A.11	
Seguridad física y de las instalaciones	A.11.1	• Se implementan medidas para prevenir accesos no autorizados a edificios, oficinas, salas de servidores y demás áreas críticas. • Incluye barreras físicas, cerraduras, controles de acceso, cámaras de vigilancia y registro de visitas. • Las áreas con equipos críticos deben contar con medidas reforzadas (ej. control biométrico o credenciales restringidas).
Protección de equipos	A.11.2	• Los equipos y activos de información deben estar ubicados y protegidos adecuadamente para evitar daños, robos o accesos indebidos. • Se contemplan protecciones contra riesgos ambientales (fuego, inundaciones, temperatura, polvo). • Reglas para el cableado seguro, separación de ambientes y ubicación en áreas seguras. • Uso de medidas contra accesos físicos no autorizados a dispositivos (ej. bloqueo de racks, gabinetes).

Tabla 7 - Seguridad física y del entorno.

12. POLÍTICA SEGURIDAD EN LAS OPERACIONES

La EMAAF E.S.P., busca controlar las operaciones correctas y seguras del procesamiento de información cuando el emisor de la información se encuentre en las instalaciones de la empresa.

Los controles sobre las operaciones serán administrados por el proceso de gestión de las tecnologías de la información, desarrollando procedimientos para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación.

Dichas operaciones incluyen la gestión de capacidad, gestión de cambios, controles contra código malicioso, respaldo de la información, registro de eventos, protección de la información de registro, registro del administrador y operadores, sincronización de relojes, instalación de software, actualizaciones de sistemas operativos, gestión de vulnerabilidades técnicas, restricción sobre la instalación de software y controles de auditorías de sistemas de información.

12.1. Asignación de responsabilidades operativas

Gestión de las TI será responsable de la operación y administración de los recursos tecnológicos de la siguiente manera:

- Asignará oficios a los funcionarios y terceros vinculados, quienes velarán por la adecuada operación y administración de los recursos TI, manteniendo y actualizando la documentación de los procesos operativos.
- Se ocupará de la eficiencia de los controles asociados a la infraestructura de TI y vigilará que los cambios efectuados sobre ésta sean debidamente autorizados de acuerdo al procedimiento "Procedimientos Política Seguridad en las Operaciones".
- Gestionará la capacidad de procesamiento necesaria de los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones.

12.2. Documentación de procedimientos de operación

Los procedimientos de operación deberán ser documentados, actualizados, versionados, almacenados de forma intuitiva y puestos a disposición de los funcionarios y terceros vinculados que los necesitan.

Dentro de la documentación se deberán tener procedimientos para la configuración y operación de los sistemas operativos, servicios de red, bases de datos y sistemas de información, así como de todos los componentes de la plataforma tecnológica de la EMAAF E.S.P.

12.3. Protección frente a software malicioso

La EMAAF E.S.P., adoptará los controles necesarios para evitar el contagio de software malicioso y amenazas cibernéticas. Aunará esfuerzos por generar cultura de seguridad de la información entre sus funcionarios y terceros vinculados.

GESTIÓN TI aplicará controles de detección, prevención y recuperación para proteger la información electrónica de incidentes informáticos como un ataque de código malicioso.

Velará para que los activos de información se actualicen periódicamente, evitando que se exploten vulnerabilidades en la plataforma tecnológica de la Empresa. Para esto, vigilará que los siguientes controles operen satisfactoriamente:

- El antimalware cuente con las licencias de uso actualizadas, garantizando su autenticidad y actualización periódica.
- La información almacenada o que se transporte por la red de datos, deberá ser escaneada de software malicioso.
- Exclusivamente los admiradores con perfil privilegiado (personal TI) podrán modificar la configuración del software antimalware.
- Los funcionarios y contratistas deberán hacer uso exclusivo de hardware y software autorizado para desarrollar sus actividades.
- Los funcionarios y contratistas deberán realizar la revisión antimalware de los de archivos adjuntos que llegan a sus correos electrónicos o los que descarguen de cualquier fuente, incluso de fuentes conocidas antes de ser ejecutados, visualizados o abiertos.
- Los funcionarios y contratistas deberán comunicar a GESTIÓN DE LAS TI la sospecha de presencia de malware, que no sea eliminado por el sistema antimalware de forma automática.

Talento Humano proyectara en el PIC por vigencia las necesidades de formación y capacitación presentadas por el proceso de gestión de las TI en temas relacionados con la prevención y gestión de software malicioso.

12.4. Copias de respaldo de la información

La información como activo estratégico de la EMAAF E.S.P., deberá ser protegida y salvaguardada para que pueda ser recuperada ante cualquier incidente de seguridad que se presente y que esté relacionado con el deterioro, modificación o pérdida de información.

Gestión de la TI, deberá velar porque exista, los procesos y procedimientos que garanticen la correcta protección de la información de manera que pueda ser recuperada.

Los funcionarios y terceros vinculados de la EMAAF E.S.P., serán responsables de realizar los respaldos de la información institucional de sus equipos de escritorio o portátiles.

12.5. Registro y monitoreo de eventos de los recursos tecnológicos

La EMAAF E.S.P., podrá rastrear permanentemente el uso que se da a su plataforma tecnológica con el objeto de identificar posibles anomalías, generar alertas tempranas conducentes a reconstruir operaciones sensibles y tomar acciones relacionadas con la gestión de riesgos en la Empresa.

Los datos rastreados, conocidos como registros de auditoria necesitarán de condiciones de preservación similares a las establecidas para los datos y con los criterios de respaldo y recuperación fundamentados en los requerimientos de retención de la información definidas por GESTION DOCUMENTAL.

12.6. Protección de los registros de información

Los registros de información se protegerán contra la manipulación y el acceso no autorizado de acuerdo a los especificado en los lineamientos de copias de seguridad de la información.

12.7. Registros de actividad del administrador y operador del sistema

Las actividades de los usuarios administradores del sistema (Gestión de la TI) y de la red serán monitoreadas y registradas. Estos registros serán protegidos y regularmente revisados por el Oficial de Seguridad de la Información o quien haga sus veces.

12.8. Control de vulnerabilidades técnicas

La EMAAF E.S.P., gestionará las vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas periódicas de hacking ético, a fin de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, de acuerdo con los criterios establecidos.

La evaluación de vulnerabilidades deberá realizarse al menos una (1) vez al año o cada vez que haya cambios en la infraestructura tecnológica y por un evaluador externo y experto en el tema. La exposición de la EMAAF E.S.P., a tales vulnerabilidades será evaluada y se tomarán las medidas pertinentes para hacer frente a los riesgos identificados y a las recomendaciones sugeridas para la empresa.

12.9. Instalación de software

La instalación, reinstalación, desinstalación y configuración de software en cualquier equipo de la EMMAF E.S.P., estará restringido a GESTIÓN TI, quienes velarán porque permanezca únicamente lo autorizado.

Cada proceso tendrá el inventario de software licenciado para el desarrollo de sus actividades diarias. Dentro de las tareas periódicas de mantenimiento preventivo, GESTIÓN TI verificará que esté instalado y funcionando adecuadamente.

Si el líder de algún proceso precisa para su funcionamiento de un software adicional, solicitará a la Subgerencia y/o oficina asesora correspondiente, evaluar la pertinencia del mismo. Si se determina su conveniencia, dará el aval para que el área interesada proceda a gestionar la adquisición. Una vez disponible el aplicativo, contactará a gestión de las TI para su instalación, configuración, puesta en funcionamiento e inclusión en el inventario.

Si algún proceso necesita para su funcionamiento de algún software libre no incluido en el inventario de activos de información, solicitará a gestión de las TI su apoyo para la consecución del mismo. Estos últimos investigarán junto con el líder del proceso y la Subgerencia y/o oficina asesora correspondiente, la necesidad del aplicativo, y si es conveniente, procederá a descargarlo, instalarlo, configurarlo, probarlo, dejarlo funcional para su uso e incluirlo en el inventario. Si en el estudio se observa que no es pertinente, se dejará constancia de esto y no se instalará.

Los funcionarios y terceros vinculados son responsables del software no autorizado que se encuentre instalado en las estaciones de trabajo a su cargo. Cualquier desviación del software autorizado será considerada como un desacato a las normas de seguridad de la información, y será sancionado por violación a las políticas.

12.10. Gestión del cambio

Teniendo en cuenta que ya existe una POLÍTIA DE CONTROL DE CAMBIOS, la cual es transversal a todas las áreas y se encuentra inmersa por línea de MIPG en todas las dimensiones, se acudirá a ella.

Se deberá hacer un énfasis especial en la verificación de requisitos de seguridad del cambio, de continuidad de las actividades ante cambios no exitosos o de emergencia. Además, se deberá garantizar que todo cambio realizado sobre la plataforma tecnológica de la EMAAF E.S.P., quedará formalmente documentado desde su solicitud hasta su implantación cumpliendo con el procedimiento correspondiente

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad de las operaciones	A.12	
Protección contra software malicioso	A.12.1	• Implementar controles de seguridad para prevenir, detectar y responder a malware. • Uso de antivirus, filtros, listas negras/blancas, herramientas de detección avanzada (EDR, XDR). • Programas de concienciación a usuarios para identificar correos sospechosos o archivos maliciosos.
Gestión técnica de vulnerabilidades	A.12.2	• Realizar evaluaciones periódicas de vulnerabilidades en sistemas y aplicaciones. • Mantener procesos de parcheo y actualización de software oportunos. • Evaluar riesgos de nuevas vulnerabilidades y definir tiempos de corrección según criticidad.
Gestión de la configuración	A.12.3	• Aplicar configuraciones seguras en hardware, software y sistemas críticos. • Uso de estándares de configuración (ej. CIS Benchmarks, NIST). • Control de cambios en la configuración de plataformas y aplicaciones. • Deshabilitar servicios o funciones innecesarias que representen riesgos.

Tabla 8 - Seguridad de las operaciones.

13. POLÍTICA CONTROL DE ACCESO PARA SEGURIDAD DE LAS REDES

En el marco del Modelo de Seguridad y Privacidad de la Información, se facilitarán entornos digitales con el fin de garantizar que la información, las áreas de su procesamiento, las redes de datos, los recursos de la plataforma tecnológica y los sistemas de información de la EMAAF E.S.P., se encuentren con la protección contra accesos o intrusiones no autorizadas y que disminuyan los riesgos de seguridad de la información.

La aplicación de esta política da alcance a cualquier medio en el cual se encuentra la información (digital o físico), sitios de procesamiento de información, redes de datos, recursos de la plataforma tecnológica y sistemas de información. Además, abarca a todos los directivos, trabajadores oficiales, contratistas y terceros vinculados, con acceso a las instalaciones de la entidad y sistemas de información.

13.1. Acceso a redes y recursos de red

La plataforma tecnológica es responsabilidad de la Subgerencia Administrativa y del profesional de las TI, así como los sistemas de información de la entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso lógico y físicos monitoreados y con capacidad de generar alertas.

- Se deberá asignar un nombre de usuario para conceder el acceso a los sistemas de información de la EMAAF E.S.P.
- Para generar acceso tanto físico como lógico a proveedores como contratistas, el supervisor del contrato debe realizar la solicitud al área respectiva.
- Únicamente el propietario responsable de la información, podrá autorizar la creación de un usuario, el cual será asociado sólo a un individuo y la solicitud deberá obedecer a una razón legítima de la EMAAF E.S.P.
- Una vez que el contrato del contratista o proveedor haya finalizado, el supervisor del contrato tiene la responsabilidad de solicitar la cancelación de los derechos de acceso a el(los) usuario(s) vinculado(s) con ese contrato.
- Se deberá deshabilitar los usuarios y nombres de usuario correspondientes al personal que ya no tenga relación con la EMAAF E.S.P.
- Se deberán realizar revisiones periódicas en los diferentes sistemas de la EMAAF E.S.P., para garantizar que se remuevan los usuarios deshabilitados o redundantes, mínimo una vez al mes.
- Cada miembro del personal de la de la EMAAF E.S.P., deberá hacerse responsable de los usuarios y contraseñas asignados para el acceso a los servicios de red, los recursos de la plataforma tecnológica y los sistemas de información.
- El personal no deberá compartir sus cuentas de usuario y contraseñas con otros usuarios, con personal externo o con personal provisto por terceras partes.

Normas de seguridad para el control de acceso lógico

Los Subgerentes y Jefes de Oficina líderes de proceso deberán ser los únicos autorizados para solicitar el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario, a través de correo electrónico así:

- Asunto: Autorización acceso a la red.
- Descripción: Razón por la cual solicita la autorización, nombres y apellidos de la persona autorizada y tipo de recursos autorizados (unidades de red, módulos del sistema de información).

La administración de los perfiles de usuario es responsabilidad de Gestión TI administradores del sistema de información y de las áreas responsables de dicho activo.

El profesional universitario de TI deberá utilizar el Servicio de Directorio Activo (AD) para la administración de los objetos de la red que usa el almacén de datos estructurados como base para una organización jerárquica lógica de la información del directorio activo a través de los protocolos TCP, ICMP y UDP con LDAP.

Los Subgerentes y Jefes de Oficina líder de proceso deberán establecer los permisos que corresponde a cada perfil que puede acceder a los recursos de la plataforma tecnológica, servicios de red y los sistemas de información.

Gestión TI deberá crear, modificar, bloquear, inactivar o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información cuando esto sea solicitado por los Subgerentes y Jefes de Oficina.

Se deberá establecer la entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la EMAAF E.S.P., a los recursos de la plataforma tecnológica o a los sistemas de información. Para este fin el profesional universitario de TI entregará por medio del correo electrónico institucional la respuesta de notificación de envió de credenciales a las personas autorizadas.

Se deberá verificar periódicamente las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la EMAAF E.S.P., Para lo cual, el profesional universitario de TI, solicitará a talento humano mediante correo electrónico con periodicidad trimestral, la lista de funcionarios y contratistas activos que desempeñan funciones y actividades en la empresa, para ser contrastada con las personas que acceden a los sistemas de información, a la red de informática y sus recursos.

Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.

Se deberán establecer mecanismos de auditoría al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad de las comunicaciones	A.13	
Gestión de la seguridad de las redes	A.13.1	**Lineamiento**: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
Controles de redes	A.13.1.1	**Control**: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
Seguridad de los servicios de red	A.13.1.2	**Control**: e deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Tabla 9 - Seguridad de las comunicaciones

14. POLÍTICA SEGURIDAD EN LAS COMUNICACIONES

La EMAAF E.S.P., para proteger la información, proveerá los recursos necesarios para optimizar la protección de la información, al momento de ser transferida y comunicada a un tercero o al salir de sus instalaciones según necesidad de la actividad o proceso particular.

El grupo de TI consciente que la información hoy en día viaja por la red de comunicaciones y se transmite por diferentes medios por ejemplo correo electrónico redes sociales, Internet, diligenciamiento de sistemas de información web y muchos otros; sabiendo que los intercambios de información se realizan a través de las redes de comunicaciones internas y externas ha decidido gestionar la seguridad de la red a tal grado que permita asegurar la protección de la información en las redes y en la infraestructura de soporte que se utiliza para enviar y recibir información.

14.1. Gestión de la red local

Gestión de las TI debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la EMAAF E.S.P.

Gestión de las TI debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.

Gestión de las TI debe monitorear continuamente el canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.

Gestión de las TI debe generar registros de navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.

Gestión de las TI debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.

Gestión de las TI debe proporcionar una plataforma tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.

Gestión de las TI debe realizar segmentación de redes para servidores públicos, contratistas y visitantes de la EMAAF E.S.P.

Gestión de las TI debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

Gestión de las TI debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la empresa.

Gestión de las TI debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la EMAAF E.S.P.

Gestión de las TI debe permitir el acceso a redes inalámbricas mediante un portal de acceso en donde permita al usuario ingresar un usuario y contraseña, controlando así el acceso, duración y sitios visitados durante la navegación.

Gestión de las TI debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la EMAAF E.S.P.

14.2. Uso de conexiones remotas

La EMAAF E.S.P., debe realizar los esfuerzos necesarios para que la información de la organización no se vea comprometida para ello debe cumplir con:

- En el catálogo de gestión de servicios de información TI se dispondrá de una lista con los servicios, redes, sistemas de información que pueden ser accedidos remotamente con la descripción del talento humano y cargos que realiza acceso remoto. De igual manera se debe contar con una lista de los equipos y/o tipos de equipos desde los cuales se puede acceder remotamente.

- Contar con un inventario de accesos remotos otorgados identificando a la persona que cuenta con el acceso, el motivo por el cual se le otorgó, quien autoriza y el plazo por el cual está autorizado.

- Se debe utilizar comunicaciones seguras para el acceso remoto; los equipos utilizados para el acceso remoto deben contar con protección ante software malicioso actualizado y licenciado.

14.3. Transferencia de la información

Gestión de las TI, debe establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la EMAAF E.S.P., donde se contemple la recepción o envió de la información, utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta.

Gestión de las TI, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas. El Profesional TI o su designado, documentará la forma de cifrar los mensajes de correo electrónico, se enviará la información y capacitará al talento humano.

Las personas de gestión documental deben trazar directrices sobre retención, disposición y transferencia de la información física de la EMAAF, de acuerdo con la normatividad vigente.

14.4. Uso adecuado de Internet y del correo electrónico

Gestión de las TI debe establecer controles para proteger la información por internet y que se transmite como documentos adjuntos a través del correo electrónico de la EMAAF E.S.P.

Los mensajes y la información contenida en los buzones de correo son propiedad de la EMAAF y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.

El único servicio de correo electrónico controlado por la Emaaf E.S.P., es el asignado directamente por Gestión de las TIC, a través del formato "*F.GTICS 1.1.1-04 ASIGNACION DE USUARIO Y CONTRASEÑA CORREO INSTITUCIONAL*", en la Ruta de Calidad (*"Ruta de calidad\1. estratégico\3. gestión de la información y comunicaciones\3. gobierno digital") para su respectivo proceso de creación,* el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la EMAAF E.S.P., y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

Los usuarios de correo electrónico tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos de la entidad y el personal provisto por terceras partes.

Está prohibido el envió de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.

Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación teniendo en cuenta el tipo de información que se pretende compartir.

Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia a Gestión de las TI, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.

Es responsabilidad de cada usuario asegurar los destinarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.

El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de la EMAAF E.S.P.

No es permitido el envió o recepción de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo de la EMAAF E.S.P., cuando su ausencia sea mayor a tres (3) días, igualmente, está deberá indicar quien es la persona asignada para cubrir su ausencia.

Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato quien lo hará a través de un correo electrónico dirigido al profesional TI.

La Subgerencia Administrativa y el profesional TI definen las pautas generales para asegurar un adecuado uso de Google Workspace (correo electrónico, grupos, drive, calendario, sitios y formularios) por parte de los usuarios, una vez la EMAAF E.S.P., adquiera estos servicios.

Está prohibida la divulgación no autorizada de información de propiedad de la EMAAF E.S.P., a través de la plataforma Google Workspace.

Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.

Se deben establecer acuerdos de confidencialidad o de no divulgación de Información.

Para el personal externo que ejecute tareas propias de la EMAAF E.S.P., y haya sido contratado en el marco de un contrato o convenio la EMAAF E.S.P., debe firmar un

acuerdo de confidencialidad y no divulgación de la información firmado entre la EMAAF E.S.P., (Supervisor del Contrato) y el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

14.5. Servicios de computación en la nube

El estándar ISO 27001 internacional, proporciona directrices para la implementación de los controles de seguridad de la información en los servicios de la computación en la nube, los cuales deben ser tenidos en cuenta a la hora de contratar o usar estos dentro de la EMAAF E.S.P.

En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información de la EMAAF E.S.P., acceso a información personal, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión externa de la información de la EMAAF E.S.P.

Para almacenar información de datos personales, en los términos definidos por la Ley 1266 de 2008 o 1581 de 2012, en servicios de almacenamiento en la nube fuera del territorio nacional se debe contar con la autorización del titular del dato personal.

El uso de los servicios de computación en la nube dentro de la EMAAF E.S.P., debe ser exclusivo para el cumplimiento de las funciones de las labores dentro de la empresa, no está autorizado el uso de servicios de computación en la nube para fines personales.

Los siguientes lineamientos específicos se aplican de acuerdo con el tipo de servicio de computación en la nube:

- En los servicios de correo electrónico se deben cumplir la política institucional de correo electrónico.
- En los servicios de correo electrónico y almacenamiento en la nube se deben cumplir los límites de espacio de almacenamiento que determine el proceso de gestión de tecnologías de información.
- Los archivos almacenados en las plataformas de nube se tendrán de acuerdo con los lineamientos que determinen las tablas de retención documental de cada proceso para sus respectivos registros electrónicos.

Cualquier servicio de computación en la nube que requiera o se utilice en cualquier proceso de la EMAAF E.S.P., debe ser aprobados por la Subgerencia Administrativa y el profesional TI.

Los operadores de servicios TI aportaran en:

- Realizar monitoreo a los logos de trasferencia de datos hacia la nube.

- Los servicios de cómputo en la nube deben cumplir con los procedimientos de capacidad, disponibilidad, cambios y backup de la EMAAF E.S.P.
- Proteger los volúmenes a cualquier exposición.
- Realizar backup de la información que se envía hacia la nube.
- Los usuarios de administración de la plataforma deben mantener en estricta confidencialidad las contraseñas para acceso a los servicios de computación en la nube y el acceso a la plataforma debe ser con doble factor de autenticación.

14.6. Ciberseguridad

La EMAAF E.S.P., gestionará la información que entra y sale del ciberespacio y que es considerada importante para la operación del negocio. Mediante controles tecnológicos, políticas de seguridad de la información, procedimientos y el trabajo conjunto con el Proveedor de Servicios de Internet y empresas especializadas en ciberseguridad y ciberdefensa, prevendrá, mitigará y reducirá los impactos negativos de amenazas potenciales y/o ataques cibernéticos.

La gestión de seguridad del ciberespacio tendrá en cuenta los principios de la ciberseguridad que incluyen prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, las cuales estarán enfocadas a una adecuada administración del riesgo de ciberseguridad y al mejoramiento continuo de la seguridad de la información.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Seguridad de las comunicaciones	A.13	
Gestión de la seguridad de las redes	A.13.1	**Lineamiento**: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
Controles de redes	A.13.1.1	**Control**: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
Seguridad de los servicios de red	A.13.1.2	**Control**: e deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.

Tabla 10 - Seguridad de las comunicaciones

15. POLÍTIA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La EMAAF E.S.P., no desarrollará software dentro de la Empresa mientras que no cuente con la necesidad y la infraestructura adecuada para hacerlo. Cualquier necesidad de software no comercial, se contratará para ser desarrollado por terceros y a la medida de las necesidades de la EMAAF E.S.P.

La adquisición y mantenimiento de sistemas de información incluirá buenas prácticas de seguridad de la información durante todo el ciclo de vida. Los requisitos relacionados con la seguridad de la información serán incorporados a los sistemas de información tanto nuevos como a los ya existentes.

La EMAAF E.S.P., deberá mantener contratos de soporte y mantenimiento de forma anual, para todos los sistemas de información.

15.1. Seguridad de software adquirido

La EMAAF E.S.P., demandará que el software adquirido o desarrollado a la medida por terceros, cumpla con los requisitos de seguridad y calidad establecidos en los pliegos de condiciones de las invitaciones a licitar.

Durante la entrega de los productos terminados, se realizarán las pruebas de funcionalidad y se verificarán que los requisitos de seguridad solicitados se encuentren generados a cabalidad.

15.2. Política para la protección de los datos de prueba

Por medio de acuerdos de confidencialidad previamente suscritos entre las partes, se establecerá que los desarrolladores externos no revelarán información pública reservada o pública clasificada de propiedad de la EMAAF E.S.P.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Adquisición, desarrollo y mantenimientos de sistemas	A.14	
Requisitos de seguridad en sistemas de información	A.14.1	• Definición de requisitos de seguridad desde la fase de análisis y diseño. • Inclusión de criterios de seguridad en contratos con terceros (proveedores, desarrolladores, cloud). • Verificación de que las adquisiciones tecnológicas cumplan con las políticas de seguridad.
Seguridad en los procesos de desarrollo y soporte	A.14.1.2	• Implementación de prácticas seguras de codificación (ej. OWASP, revisiones de código, pruebas de seguridad). • Separación de ambientes de desarrollo, pruebas y producción. • Uso de controles de acceso en herramientas de desarrollo y repositorios de código. • Pruebas de seguridad (vulnerabilidades, penetración, revisiones estáticas/dinámicas). • Definición de procedimientos para gestión de cambios y control de versiones.
Datos de prueba y entornos de prueba	A.14.1.3	• Uso de datos ficticios o enmascarados en pruebas para evitar exposición de información sensible. • Controles de acceso y limpieza de datos de prueba una vez finalizado el proceso.

Tabla 11 - Adquisición, desarrollo y mantenimientos de sistemas

16. POLÍTICA DE RELACIÓN CON PROVEEDORES, TERCERAS PARTES Y/O CONTRATISTAS

El objetivo de esta política será proteger los activos de información de la EMAAF E.S.P., que puedan ser accesibles a los proveedores.

LA EMAAF E.S.P., vigilará que todo proveedor que pueda llegar a tener acceso a información pública clasificada y/o publica reservada de la empresa, cumpla con las políticas, normas y procedimientos de seguridad de la información. Además, establecerá mecanismos de control en sus relaciones con terceras partes y/o contratistas, con el objetivo de asegurar que la información a la que tengan acceso, esté debidamente protegida.

Entre los controles, se firmarán acuerdos de confidencialidad, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura de la Información según lo establecido en la Política General.

16.1. Seguridad en contratos de prestación de servicios

En los contratos de prestación de servicios suscritos con terceros, la EMAAF E.S.P., deberá incluir la seguridad de la información como parte integral del contrato y los interventores y/o supervisores deberán verificar su cumplimiento durante su desarrollo.

Para la firma del contrato, se documentarán los requisitos de seguridad de la información y los riesgos asociados al acceso del proveedor a los activos de información de la empresa. Se incluirán cláusulas que detallen los compromisos con el cuidado de los recursos de Información propiedad de la EMAAF E.S.P., y las sanciones en caso de incumplimiento. El acatamiento de estas cláusulas deberá verificarse y controlarse permanentemente por quienes ejerzan las funciones de supervisión de estos contratos.

Se presenta un modelo de cláusula para quienes adelantan los estudios precontractuales de tal forma que se garantice su difusión:

"*Los datos, los activos de información y los elementos entregados por parte de la EMAAF E.S.P., son de uso exclusivo para el cumplimiento de las funciones; permitiendo la manipulación y el acceso de esta información, únicamente durante el proceso de ejecución del contrato o servicio, controlando así que no se conserven copias o se altere la información sin el consentimiento explícito de la EMAAF E.S.P.*".

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Relación con los proveedores	A.15	
Seguridad de la información en las relaciones con proveedores	A.15.1	• Establecimiento de criterios de seguridad en la selección, contratación y gestión de proveedores. • Inclusión de cláusulas de confidencialidad, protección de datos, cumplimiento normativo y seguridad de la información en contratos. • Evaluaciones de seguridad en proveedores críticos antes y durante la relación contractual.
Gestión de cambios en la relación con proveedores	A.15.1.2	• Procedimientos para gestionar modificaciones en los servicios prestados por proveedores (ej. cambios en infraestructura, subcontratación, nuevas tecnologías). • Revisión y actualización de los acuerdos de nivel de servicio (SLA) cuando se produzcan cambios relevantes. • Supervisión continua para garantizar que los cambios no afecten la confidencialidad, integridad o disponibilidad de la información.

Tabla 12 - Relación con los proveedores

17. POLÍTICA GESTIÓN DE INCIDENTES DE SEGURIDAD

El objetivo de esta política es gestionar adecuadamente todos los incidentes de seguridad de la información reportados en la EMAAF E.S.P., dando cumplimiento a los procedimientos establecidos.

17.1. Reporte de incidentes de seguridad

La EMAAF E.S.P., establecerá los mecanismos para el reporte de cualquier evento de seguridad de la información que involucre la plataforma tecnológica, los sistemas de información y/o las personas y será reportado por la persona a l líder del proceso quien notificara a gestión TI por medio de la mesa de ayuda o de no ser posible lo hará de manera presencial.

La EMAAF E.S.P., promoverá entre los funcionarios y terceros vinculados, el reporte de cualquier evento de seguridad de la información. Quienes utilizan los sistemas y servicios de información deberán observar y reportar cualquier comportamiento sospechoso relacionado con esto.

El profesional de gestión TI con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces, definirán los eventos que puedan llegar a ser considerados como incidentes de seguridad, junto con sus respectivas alertas y registros, los cuales deberán ser generados, activados, vigilados, almacenados y revisados permanentemente.

Los registros y los medios que los generan y administran deberán ser protegidos para evitar modificaciones o accesos no autorizados, con el fin de preservar la integridad de las evidencias.
La responsabilidad y el procedimiento para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información estará en cabeza de Gestión TI, quien junto con el Oficial de Seguridad de la Información o quien haga sus veces, valorarán los eventos de seguridad de información y decidirán si cambiarán su estatus de evento de seguridad de la información a incidentes de seguridad de la información.

17.2. Sanciones por las violaciones a las políticas de seguridad de la información

Los empleados, y terceros vinculados deberán estar informados de las sanciones, incluidas procesos disciplinarios que se llevará a cabo en caso de incumplimiento de la **POLÍTICA GENERAL DE SEGURIDAD, PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS DE LA EMPRESA MUNICIPAL DE ACUEDUCTO, ALCANTARILLADO Y ASEO DE FUNZA EMAAF E.S.P.**, o alguno de los elementos que la soportan. En cualquier caso, se hará un seguimiento de acuerdo con el desarrollo de los procedimientos establecidos para el manejo de incidentes de seguridad.

Los incidentes de seguridad, resultantes del incumplimiento de las políticas y normas de seguridad de la información serán gestionados por el procedimiento de manejo de incidentes de seguridad, con el objetivo de realizar la respectiva investigación y entregar los resultados a los responsables de la información y al Comité Institucional de Gestión y Desempeño, quienes serán los encargados de tomar las acciones correctivas y preventivas del caso.

17.3. Proceso disciplinario

Se solicitará proceso disciplinario formal y comunicado en contra del talento humano que hayan cometido una violación de la seguridad de la información, y según corresponda la investigación será tramitada por el Proceso de Control Interno Disciplinario de la Entidad o por la Procuraduría General de la Nación.

17.4. Recopilación de evidencias

De manera proactiva, la EMAAF E.S.P., con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces, definirá y aplicará procedimientos para la identificación, recolección y conservación de información, que puede servir como evidencia en un caso de que sea necesaria la investigación detallada de un incidente de seguridad.

17.5. Aprendizaje de los incidentes de seguridad de la información

Los conocimientos adquiridos a partir del análisis y la resolución de incidentes de seguridad de información se deberán registrar en una base de datos. Esta información servirá para reducir la probabilidad y el impacto de nuevos incidentes en el futuro. Del mismo modo ayudarán para tomar las medidas necesarias y evitar su reincidencia.

- Documentar todos los incidentes de seguridad de la información reportados en la EMAAF E.S.P.
- Implementar una bitácora de los incidentes de seguridad de la información reportados y atendidos en la EMAAF E.S.P., por medio del aplicativo dispuesto para tal fin.

17.6. Comunicación a terceros de incidentes de seguridad

El Comité Institucional de Gestión y Desempeño o quien este delegue, serán los únicos autorizados para reportar incidentes de seguridad a las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante empresas externas.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Gestión de incidentes de seguridad de la información	A.16	
Gestión de incidentes y mejoras en la seguridad de la información	A.16.1	**Lineamiento**: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
Responsabilidad y procedimientos	A.16.1.1	**Control**: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
Reporte de eventos de seguridad de la información	A.16.1.2	**Control**: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
Reporte de debilidades de seguridad de la información	A.16.1.3	**Control**: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
Evaluación de eventos de seguridad de la información y decisiones sobre ellos	A.16.1.4	**Control**: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
Respuesta a incidentes de seguridad de la información	A.16.1.5	**Control**: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
Aprendizaje obtenido de los incidentes de seguridad de la información	A.16.1.6	**Control**: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

Tabla 13 - Gestión de incidentes de seguridad de la información.

18. POLÍTICA CONTINUIDAD DEL NEGOCIO

Continuidad de Negocio es la capacidad táctica y estratégica de planificar y responder a incidentes o interrupciones de negocio, continuando con las operaciones a un nivel aceptable definido. Se alcanza, mediante el diseño e implementación de un Plan de Continuidad de Negocio (PCN o BCP por sus siglas en ingles).

La EMAAF E.S.P., creará el Plan de Continuidad de Negocio y Recuperación ante Desastres, siguiendo la "Guía para la preparación de las TI para la continuidad del negocio", proporcionada por MinTIC y como parte del desarrollo del Modelo de Seguridad y Privacidad de la Información -MSPI-. El Plan estará alineado con los objetivos de negocio, formalmente documentado y con procedimientos perfectamente probados para asegurar la restauración de los procesos críticos del negocio, ante el evento de una contingencia.

Debido a la complejidad técnica, operativa y el cumplimiento de las buenas prácticas de la ISO para lo cual tiene una norma específica, el desarrollo e implementación del Plan de Continuidad del Negocio y Recuperación ante Desastres podrá ser contratada a una firma consultora especializada para garantizar la calidad del Plan y su implementación óptima.

Dando cumplimiento a la política de recuperación, la EMAAF E.S.P., podrá contar con sitios físicos, virtuales alternos o una combinación de ellos con capacidad de recuperación, que permitan recobrar inicialmente los procesos críticos y misionales y paulatinamente los demás, de manera que se mantenga la continuidad del negocio y/o se regrese a la normalidad en el menor tiempo admisible.

Se deberán realizar pruebas y simulacros programados para garantizar la efectividad del Plan de Continuidad de Negocio y de Recuperación.

El plan deberá actualizarse cada vez que se renueve la infraestructura física, tecnológica y/o de personal. También cada vez que se haga un simulacro, y se observen oportunidades de mejora. Todo lo anterior deberá estar documentado. La información actualizada y versionada del Plan se tendrá en varios sitios estratégicos, donde tengan acceso las personas designadas para activarlo, de forma que en un momento de crisis se pueda activar teniendo a la mano la documentación pertinente.

18.1. Análisis de riesgos y la continuidad de la seguridad de la información

Se realizará periódicamente un análisis de riesgos enfocado a valorar el impacto de incidentes que comprometen la continuidad del negocio. Se debe tener en cuenta que el impacto será mayor cuanto más dure la interrupción.

Para realizar el análisis de riesgos se tendrán en cuenta los procesos críticos de negocio; se identifican los eventos que pueden provocar interrupciones en los procesos de negocio como fallos de los equipos, errores humanos, robos, incendios, desastres naturales, sabotaje, actos terroristas, entre otros; se evaluarán los riesgos para determinar la probabilidad y el impacto de dichas interrupciones en cuanto a tiempo, escala de daños y periodo de recuperación; se Identificarán los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad de la información y se establecerán acciones de control y responsables de contribuir en la mitigación de los riesgos.

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Aspectos de seguridad de la información de la gestión de continuidad de negocio	A.17	
Planificación de la continuidad de la seguridad de la información	A.17.1	• Desarrollo de estrategias y planes de continuidad que incluyan aspectos de seguridad de la información. • Identificación de procesos críticos y sus dependencias tecnológicas. • Establecimiento de niveles de recuperación (RTO, RPO) para garantizar la disponibilidad de la información.
Implementación de la continuidad de la seguridad de la información	A.17.2	• Integración de los requisitos de seguridad en los planes de continuidad de negocio (BCP) y en los planes de recuperación ante desastres (DRP). • Ejecución de medidas técnicas y organizativas para mantener la confidencialidad, integridad y disponibilidad de la información durante interrupciones.
Verificación, revisión y evaluación	A.17.3	• Pruebas periódicas de los planes de continuidad y recuperación para asegurar su eficacia. • Revisión de resultados y actualización de planes tras cambios significativos o incidentes reales. • Inclusión de escenarios de ciberseguridad (ransomware, ataques DDoS, pérdida de servicios cloud).

Tabla 14 - Aspectos de seguridad de la información de la gestión de continuidad de negocio.

19. POLÍTICA DE CUMPLIMIENTO

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, de cualquier requisito de seguridad en la EMAAF E.S.P., y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al año o cuando se presente una actualización en la normatividad que afecte la seguridad de la información.

La EMAAF E.S.P., velará por la identificación, documentación y cumplimiento de las obligaciones legales estatutarias, de reglamentación y contractuales relacionadas con la seguridad de la información, como son: derechos de propiedad intelectual y el uso de software patentado, privacidad y protección de datos personales, transparencia y acceso a la información, el Modelo Integrado de Planeación y Gestión -MIPG- y el Modelo de Seguridad y Privacidad de la información -MSPI- emitido por el Ministerio de las Tecnologías y las Comunicaciones – MinTIC, y todas las que se soliciten.

Se realizará la verificación de cumplimiento normativo con el fin de identificar posibles falencias de seguridad y se optimizarán o implementarán controles aplicables a la operación, aspecto que será extendido a todos los proveedores de procesos misionales.

19.1. Cumplimiento de derecho de propiedad intelectual

Gestión TI vigilará que el software instalado y en uso en los recursos de la plataforma tecnológica de la EMAAF E.S.P., cumpla con el licenciamiento del fabricante.

Periódicamente, cuando se realice mantenimiento preventivo de los activos de información se verificará que el software instalado en las estaciones de trabajo, servidores, bases de datos, equipos de comunicaciones, entre otros, cumple con los derechos de propiedad intelectual.

19.2. Privacidad y protección de datos personales

En cumplimiento de la Ley 1581 de 2012 y el Decreto 1377 de 2013, la EMAAF E.S.P., protegerá los datos personales de los funcionarios y sus familias, contratistas, suscriptores, y demás terceros de los cuales reciba y administre información personal.

Se adoptarán las medidas administrativas, técnicas y de procesos para resguardar la privacidad y proteger los datos personales durante la captura, almacenamiento, procesamiento y transporte de esta información. Se establecerán las políticas de protección de datos personales de acuerdo con los lineamientos de la ley y se documentarán en la política de Tratamiento de Datos Personales, disponible en la sede electrónica institucional.

19.3. Cumplimiento de ley de transparencia

La EMAAF E.S.P., garantizará el derecho de acceso a la información pública a través de los canales habilitados por la empresa, excluyendo solo aquella que está sujeta a las excepciones constitucionales, legales y bajo el cumplimiento de los requisitos establecidos en Ley 1712 de 2014 "*Ley de trasparencia y acceso a la información pública*".

Resumen controles implementados del Anexo A del estándar ISO/IEC 27001:2013

Política / lineamiento	Control norma	Descripción
Cumplimiento	A.18	
Identificación de requisitos aplicables	A.18.1	• Identificación y actualización de leyes, normas y regulaciones aplicables (ej. protección de datos, comercio electrónico, propiedad intelectual, sectoriales). • Revisión periódica del cumplimiento normativo mediante auditorías internas o externas. • Documentación de responsabilidades legales de la organización y de terceros.
Derechos de propiedad intelectual y uso de activos	A.18..2	• Políticas para el uso legal de software, licencias, bases de datos, contenidos y tecnología. • Medidas para prevenir el uso indebido de activos protegidos por propiedad intelectual. • Supervisión del cumplimiento de licenciamiento en software y servicios en la nube.
Protección de registros	A.18.3	• Establecimiento de políticas de retención, custodia y eliminación de registros de acuerdo con normativa aplicable. • Implementación de controles de integridad, confidencialidad y disponibilidad en los registros físicos y digitales. • Procedimientos para acceso autorizado y trazabilidad de registros críticos.
Privacidad y protección de datos personales	A.18.4	• Cumplimiento de leyes y regulaciones sobre protección de datos personales (ej. GDPR, Leyes de Habeas Data, Ley 1581/2012 en Colombia).

		• Definición de procedimientos para la recolección, tratamiento, almacenamiento y eliminación de datos personales. • Consentimiento informado, derechos de los titulares y mecanismos de atención a incidentes de privacidad.

Tabla 15 - Cumplimiento

20. Referencias documentales relacionadas

- ISO 27001: 2013 Gestión de Seguridad de la Información.
- ISO/IEC 27001:2022 – Tecnología de la información – Seguridad, ciberseguridad y protección de la privacidad – Sistemas de gestión de la seguridad de la información – Requisitos.
- Plan Estratégico de Tecnología de la Información y las Comunicaciones de la EMAAF ESP.
- Anexo 1 Modelo de Seguridad y Privacidad de la Información Ministerio de Tecnología de la Información y las Comunicaciones.

2. Control de Cambios

Versión	Fecha	Control de cambios
01	06 de agosto	La actualización del Manual de la Política General de Seguridad, Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios, se realiza con el fin de alinear la estructura jerárquica y las responsabilidades institucionales con lo dispuesto en el Acuerdo de Junta Directiva No. 016 de diciembre de 2023, fortaleciendo así la gestión organizacional en materia de seguridad y privacidad de la información. Asimismo, se actualizan los controles implementados conforme a la transición del Anexo A del estándar ISO/IEC 27001:2013 al Anexo A del estándar ISO/IEC 27001:2022, garantizando la conformidad con los requisitos normativos vigentes y las mejores prácticas internacionales en gestión de la seguridad de la información, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad.

Aprobó:	María Camila Quintero Ojeda	Subgerente Administrativo	
Proyectó	Orlando González Pinto	Profesional Universitario	